COMPUTER

NETWORK

(3)

Date:

INTRODUCTION

→ **PHYSICAL ADDRESS :**

→ The system address of a computer ie MAC address is called as physical address.

→ Physical address points to main memory.

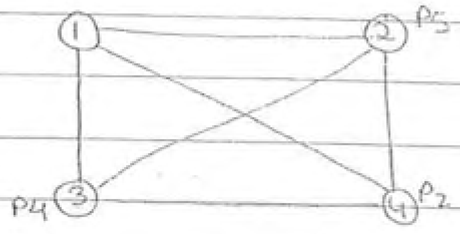
Physical address size = 48 bits.

$\left.\begin{array}{l}\text{MAC address} \\ \text{Physical address} \\ \text{NIC / LAN Card address} \\ \text{Ethernet address}\end{array}\right\}$ All are equivalent

→ In internet environment, computers can't communicate with each other through physical address. because different manufacturer manufactures different ~~diff~~ computers. So, physical address may be differ and may be they are same.

→ **COMPUTER NETWORKS :**

It is a collection of autonomous computers for transfering the data through communication links.



→ Each ~~processor~~ system having different processors.

→ **LOGICAL ADDRESSING ;**

Communication is done with logical address.

→ Logical addresses are also known as IP address

2 Types

- IPV4 → 32-bit address
- IPV6 → 128-bit address

→ IP addresses ~~have~~ range (0 — 255)

↑ Minimum ↑ Maximum

Date:

→ IP addressing is done by 3 methods :

1) Classful addressing

2) Subnetting

3) Supernetting

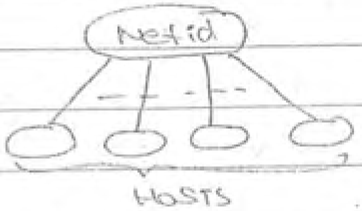
1) CLASSFUL ADDRESSING :

It divides IP addresses into 5 classes ie. A, B, C, D and E.

→ It has 2 parts : 1) Net id

2) Hosts

→ It supports 2-level of hierarchy.



→ It supports 2 notations for IP addresses :

1) Binary (consist of 0's and 1's)

eg: 10010011 1111111 0000000 111111

2) Dotted decimal :

eg:- 255 . 255 . 255 . 19
↳ It seperates 2 octet bits

→ In classful addressing, IP address have 32 bits divided in 4 octet bits.

Unicasting, in this one system transfers the data to another system.

• Is supported by Class A, B and C.

MULTICASTING, in this one system sends or transfers the single same data to many systems simultaneously like group mails.

• Is supported by Class D.

→ Class E is for research and for future use.

→ Class A : } For Unicasting
Class B :
Class C :
Class D : → For multicasting
Class E : → For research.

•) CLASS A : Is identified by 1st bit of net id. ie if 1st bit of netid is 0, then those IP address belongs to Class A.

→ $\underbrace{\underline{0} \quad 2^7-2}_{\text{Net ID (8 bits)}} \quad \underbrace{2^{24}-2}_{\text{HOST ID (24 bits)}}$

→ IP address range is (0–127)

ie Min value → $\underline{0}0000000$ = 0 ie 0.0.0.0 → DHCP Client

Max value → $\underline{0}1111111$ = 127 ie 127.x.y.z → loop back.

But Class A does not use 0 and 127 becoz these are special IP addresses

So, Class A have IP address in range (1–126).

→ In class A, no. of possible networks are (2^7-2) ie 126 and has $2^{24}-2$ hosts for each network.

•) CLASS B : Is identified by 2nd and 1st bit of netid ie Netid must start by 10 in binary notation.

→ $\underbrace{\underline{10} \quad (2^{14}-2)}_{\text{Net id (16 bits)}} \quad \underbrace{2^{16}-2}_{\text{Host id (16 bits)}}$

→ Range of Class B is (128–191)

ie Min Value → $\underline{10}000000$ 128

Max Value → $\underline{10}111111$ 191

→ No. of possible networks are (2^{14}) and has $2^{16}-2$ hosts for each network.

Ques- If IP address of the system is 63.12.1.1 to which class does it belongs to ?

Sol: Class A becoz it has range (1–126) & 63 belongs to class A range.

Ques- If IP address of the system is 160.11.120.19, to which class does it belongs to ?

Sol: Class B becoz it has range (128–191).

Ques- If IP address of the system is 160.125.257.1, to which class does it belongs to ?

Sol: This IP address is not possible becoz range of IP addresses are (0–255).

•) CLASS C : Is identified by 3 bits ie if starting 3 bits of net id in binary notation is 110, then IP belongs to class C.

$\rightarrow \underbrace{\underline{110}\quad 2^{21}}_{\substack{\text{Netid}\\ (24\text{ bits})}}\quad \underbrace{2^{8}-2}_{\substack{\text{Host ID}\\ (8\text{ bits})}}$

→ Range of Class C is (192–223)

ie Min → <u>110</u> 00000 · 192

Max → <u>110</u> 11111 223

→ No. of possible networks are 2^{21} and hosts are 2^8-2 for each network.

•) CLASS D : Is identified by starting 4 bits ie 1110.

→ Range of Class D is (224–239)

Min → 1110 0000 224

Max → <u>1110</u> 1111 239

•) CLASS E : Is identified by 1111 bits of starting net-id.

Range is (240 – 255). <u>1111</u> 0000 → Min 240

<u>1111</u> 1111 → Max 255

Ques-

Sol:-

Date:

→ We can divide 32 bits into net id and host id for Classes A, B, C but we can't divide bits of class D, and Class E into host id and netid. Becaz of multicasting but we can identify class E and class D IP addresses.

→ Class C have minimum no. of hosts in each network and Class A has maximum no of hosts in each network.

NET MASK :

- Is only available for class A, B and C.
- It says make netid bits ~~into~~ all 0's and host id bits into all 1's.
- So Net Masks for classes are :

Class A : 255.0.0.0

Class B : 255.255.0.0

Class C : 255.255.255.0

How To CALCULATE NET-ID :

1) Identify the class of given IP address.
2) Calculate the network mask for that class.
3) Perform bitwise AND operation between IP address and net mask.

Ques- If IP address of a system is 24.31.13.16. Calculate the net-id.

Sol :- Class is A

Net Mask ⇒ 255.0.0.0

(AND) 24.31.13.16

$\boxed{24.0.0.0}$ → Net id.

→ If we perform AND operation of all 1's with any no., then that gives ~~result~~ same no. as a result.

ie 255 AND 24 = 24

24 AND 0 = 0

Date:

a) In above problem what will be address of 1^{st} host?

It will be 24.0.0.1 becoz 24.0.0.0 is already assigned for net-id

b) In above problem what will be address of last host?

It will be 24.255.255.254. becoz 24.255.255.255 is assigned for broadcasting purpose and called as Directed broadcast address.

→ Hence hostid don't use 2 address becoz one is assigned for net-id and other for directed broadcast.

→ For a net-id, host bits should be all zero's.

→ For a directed broadcast address, host bits will be all 1's.

Ques- If IP address of a system is 36.11.119.14. Find Net-id, directed broadcast address, 1^{st} host and last host address?

Net id : 36.0.0.0

D.B address : 36.255.255.255

1^{st} host : 36.0.0.1

last host : 36.255.255.254.

Ques- If IP address of a system is 141.119.89.63 Calculate net-id, directed broadcast address, 1^{st} host and last host.

Class - B

Net-id : 141.119.0.0

DB address : 141.119.255.255

1^{st} host : 141.119.0.1

last host : 141.119.255.254

Ques- If IP address is 199.83.44.12 Calculate net id, directed broadcast address, 1st host and last host address. and how many hosts are in a network

Class C.

Net-id : 199.83.44.0

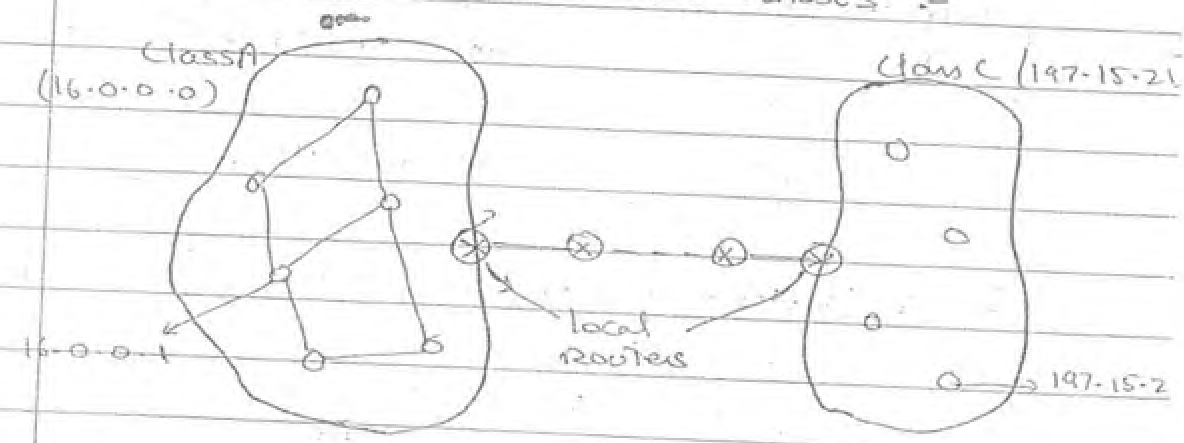
DB address : 199.83.44.255

1st host : 199.83.44.1.

last host : 199.83.44.254.

No. of hosts in a network = $2^8 - 2 = 254$

HOW DATA IS TRANSFERED BETWEEN TWO DIFFERENT LAN NETWORKS OF DIFFERENT CLASSES :-



→ Routers are devices which route the data packet on network and it has routing table containing information about source IP and destination IP.

→ In a LAN, computers are connected ~~with~~ through an topology and router is connected to topology.

→ Each LAN n/w has router which has Net-id.

→ When n/w wants to transfer data, it designs a packet.

- This packet contains data, source IP & dest.n IP. This pkt is transfered to local router.
- Local router routes this packet to dest.n systems local router.

Date:

- Whether to transfer data to one system or to broadcast the data, it is identified by dest.^{n} router.

 ie if des.^{n} IP is Directed broadcast address then pkt is broadcasted.

- While broadcasting only single packet is send by source router to dest.^{n} router. becoz seperate pkt for all systems will cause congestion in a network.

Examples :

1) If we want to transfer data from 16.0.0.1 to other system in a n/w bo of IP address 197.15.21.16

The packet will be,

Data	16.0.0.1	197.15.21.16
	SIP	DIP

Ques

2) If data transfered to every system of 197.15.21

then packet will be

Data	16.0.0.1	197.15.21.255
	SIP	DIP

HOW DATA IS TRANSFERD WITHIN THE SAME LAN NETWORK :

Ques.

→ Let LAN n/w is of Class A having net id 16.

→ If source IP and dest.^{n} IP ~~not~~ have same net id, then router will filter the packet ie it will not allow packet to go outside.

Eg:-

1) If 16 want to transfer data to ~~64 network~~ every system in network IP 64 then,

Data	16.0.0.1	64.255.255.255

Date:

LIMITED BROADCAST ADDRESS : In this address all bits a 1's and is used for broadcasting to every system in the same network.

- It is available to all classes for broadcasting in the same network.

To identify host on a particular network, just make network bits ie net bits as all zeros.

Ques- If IP address of a system is 131.86.17.18. Calculate the host on this network.

Host will be 0.0.17.18

Ques- Design a packet if the source IP is 197.15.21.16 and dest.^{n} IP is 197.15.21.31 on this network.

	SIP	DIP
Data	0.0.0.16	0.0.0.31

(OR)

Data	197.15.21.16	197.15.21.31

both are same.

Ques- Identify whether the packet design are correct or not.

a)	Data	16.0.0.1	255.255.255.255	✓
b)	Data	16.255.255.255	18.0.0.2	X
c)	Data	255.255.255.255	191.16.1.1	X
d)	Data	16.1.1.1	120.17.2.3	✓
e)	Data	16.1.2.3	141.16.255.255	✓

a) : Means one system of 16 is broadcasting msg within same n/w using limited broadcast address

b) : Means all system of 16 n/w is sending same data to one system of 18 n/w. ie False

c) : Means all system of one n/w sending data to one sys of same n/w ie within same n/w. Not possible So False

d) : System of 16 sending data to a system of 120.

Date:

→ Directed broadcast address and limited broadcast address will always be used as a destination IP.

→ To identifying a system in a internet world is done with the help of logical address

IANA OR ICANN (Internet Corporation for Assigned Names & no.'s)
↓
Internet Assigned Names Authority

→ IANA assigns a IP or gives internet facility to customers. ie it provides internet

→ Mediator's have bulk of IP addresses to provide internet to users. So users contact to these mediators instead of IANA. These mediators are like airtell, idea, reliance etc.

→ These mediators provide public IP for internet to users.

→ Mediators are ISP's. So for public IP user have to communicate with ISP and have to pay some amount for internet to ISP's.

→ There are some private IP's for which user don't need to pay any money.

Range of Private IP addresses are :

Class A : 10.0.0.0 to 10.255.255.255 : 1 n/w provided
Class B : 172.16.0.0 to 172.31.255.255 : 16 n/w provided
Class C : 192.168.0.0 to 192.168.255.255 : 255 n/w provided.
↳ used to communicate within LAN

Date:

HOW PRIVATE IP ACCESSES OR COMMUNICATES WITH PUBLIC IP IN INTERNET WORLD :

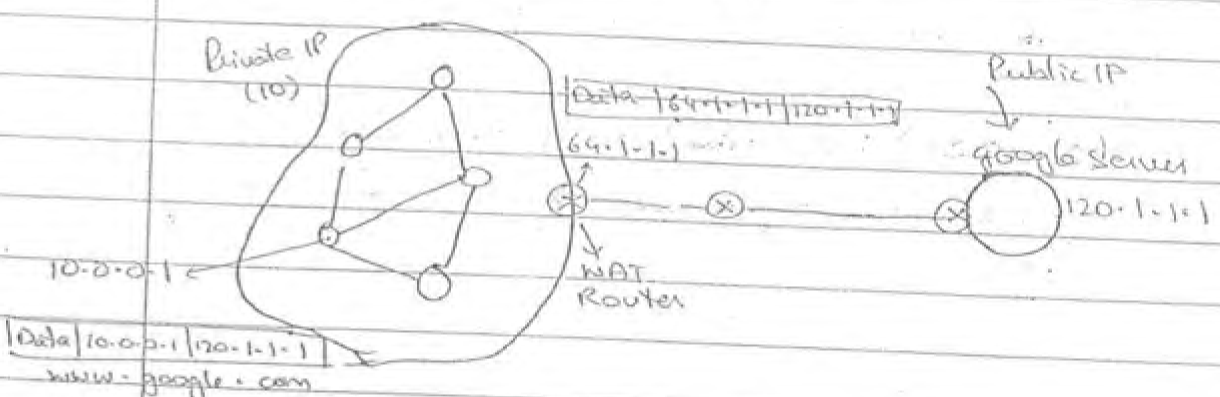
Suppose private IP 10.0.0.0 is assigned to a college lab. Administrator on server in that college assigns a private IP address to each system. College network must be having a router. All systems are connected through LAN.

→ ~~Always~~ Only through private IP these systems can't be able to access ~~net~~ internet.

→ So, router will have one public IP by paying some amount to ISP's.

→ This router is also known as NAT router because it converts private IP to public IP when pkt going outside the n/w and converts public IP to private when pkt coming or moving inside the n/w

→ Now, all systems of college lab can access internet by using 1 p same public IP.



Let 10.0.0.1 private IP writes www.google.com. to access. Where google server have public IP ie 120.1.1.1

- Now it forms a packet and send to NAT router.
- NAT router convert private IP to public IP and forms new packet.
- Now, this new packet is transmitted to public IP of google server.
- Response of google is send to NAT router & router sends that data to private IP system.

Date:

As google server understands and communicate with public IP., private IP is converted by NAT:

→ So, communication takes place b/w public IP to public IP in internet network.

logical address only helps to locate the system in internet network.

To identify processing in a network environment service addressing system is required.

SERVICE ADDRESSING SYSTEM :

↳ Is also known as port address.

→ Is also provided by IANA.

→ Port address has 16 bits.

ie 2^{16} = (0 to 65,535) port no's

→ These ports are logical ports.

(0–1023) : Predefined ports or universal ports.

• Are used for predefined services like http., SMTP, FTP etc.

Http – 80

SMPT – 20, 21

~~TU~~ FTP – 25

(1024 – 49,151) : Registered Ports.

Suppose any medium company launches a software and that software requires specific port for all, then that company will ask IANA for port.

IANA will provide port from these range not from predefined ports.

So, these ports are assigned to s/w developed by some Companies.

Date:

(49,152 — 65,535) : Dynamic ports ; Ephemeral ports.
Whenever a client requests a service from a server, the client is assigned a port no. that is dynamic port by TCP/IP software.

- Like google has 1 public IP but have multiple dynamic ports.

HOW IP ADDRESSES ARE ASSIGNED BY SERVER OR ADMINISTRATOR WITHIN LAN SYSTEMS :

Suppose Server has private IP ie 192.168.1.1 and have DHCP installation.

- Server 1st broadcast or send dummy packet to all systems
- No system is having IP address. So Now all systems know Server IP address.
- Each system will use default IP to response to server and along with default address MAC address are also send so that it will help Server to distinguish different clients in the LAN.

SIP	DIP
0.0.0.0	192.168.1.1

- Now acc. to their MAC address, server will assign IP addr to each system in LAN

→ DHCP Client is used as Sender IP, when client does not have their IP or don't know their IP addresses, then they use default address for communicating with server.

DISADVANTAGE OF CLASSFUL ADDRESSING :

1) In class A and Class B, most no. of IP addresses are wasted.
2) In class C, IP addresses are not sufficient to the required level.

→ To overcome these problems we are going for SUBNETTING

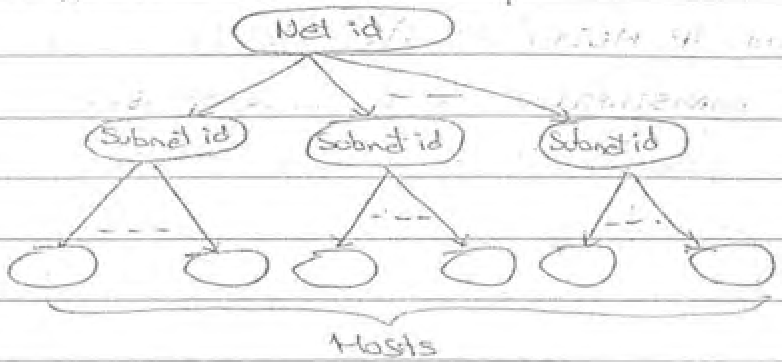
Date:

2) SUBNETTING :

→ It is efficient technique compared to classful addressing becoz IP addresses are utilized efficiently.

→ Security is also high in subnetting becoz data has to pass from 2 levels whereas in classful 1 level only data has to pass.

→ It supports 3-level hierarchy.



→ It borrows bits from host not from netid

→ If we are given subnet mask then we can calculate no. of subnets and no. of hosts in each subnet.

(Subnet-id = IP address (AND) Subnet Mask)

Ques- If subnet mask of class B is 255.255.240.0. Calculate no. of subnets and no. of hosts in each subnet.

Default mask = 255.255.0.0

Subnet bits are no. of bits having 1's in host bits in mask

$$\text{Subnet mask} = \underbrace{255.255}_{\text{Net id}}.\underbrace{240}_{\text{Subnet}}.\underbrace{0}_{\text{host}}$$

So, No. of subnets $= 2^4 - 2 = 14$ subnets.

$$\text{Mask} = 11111111.11111111.\underbrace{1111}_{\text{subnet bits}}0000.00000000$$

No. of hosts in each subnet $= 2^{12} - 2 = 4094$ hosts

Ques- If subnet mask of class C is 255.255.255.224. Calculate no. of subnets and no. of hosts in each subnet.

$$\text{Mask} = \underbrace{11111111.11111111.11111111}_{\text{Netid}}.\underbrace{111}_{\text{Subnet bits}}\underbrace{00000}_{\text{host}}$$

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

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

Ques. 4 subnet mask of A is 255.255.192.0. Calculate no. of subnets & ho

Mask = $\underbrace{11111111}_{\text{Netid}} . \underbrace{11111111 . 11}_{\text{Subnet}}000000 . \underbrace{00000000}_{\text{host}}$

No. of Subnet $= 2^{\text{\#of subnet bits}} - 2 = 2^{10} - 2$

No. of host $= 2^{14} - 2$

Ques- IP address is 197.111.121.199 & subnet mask is 255.255.255.240. Calculate subnet id.

197.111.121.199	11000111 - 199
(AND) 255.255.255.240	11110000 - 240
197.111.121.192	11000000 - 192

last Subnet id = 197.111.121.224 $\quad \underbrace{1110}0000$

1^{st} Subnet id = 197.111.121.16 $\quad \underbrace{0001}$

2^{nd} Subnet id = 197.111.121.32 $\quad \underbrace{0010}$

last host of last subnet = 197.111.121.238 $\quad \underbrace{1110}\underbrace{1110}$

Date:

Ques- IP = 203.112.111.117 and Subnet Mask = 255.255.255.224
Find Subnet-id, no. of subnets & subnet no. to which this IP belong.

IP : 203.112.111.117 117 → 01110101
255.255.255.224 224 → 11100000
01100000
Subnet bits

Subnet id ⇒ 203.112.111.96

Subnet bits = 3, No. of subnet = $2^3 - 2 = 6$

Subnet no. of IP = 3rd subnet

1) 3rd host of 3rd Subnet

011 00011

203.11

2) 3rd host of 4th subnet

3) 4th host of 4th Subnet

4) 4th host of 3rd subnet

203.112.

Ques- In above problem calculate the directed broadcast address of 4th subnet, last subnet.

4th subnet : ~~203.~~ 100 11111
159

203.112.111.159

last subnet : 110 11111
223

So, 203.112.111.223.

Date:

Ques- If IP address of a system is 61.119.189.176 and the subnet mask is 255.255.192.0.

a) Calculate the directed broadcast address of the 1st subnet

b) Calculate last host of last subnet.

$192 = \underbrace{11}_{\text{Subnet id bits}}000000$

2	192	
2	96	0
2	48	0
2	24	0
2	12	0
2	6	0
2	3	0
	1	1

Subnet id $= \underbrace{11111111\ 11}_{\text{bits}}000000\ 00000000$

a) Directed broadcast address of 1st subnet will be (:

00000000 | 11111111111111

61.0.127.255

b) last host of last subnet is,

$\underbrace{11111111.10}_{\text{last subnet}}111111.11111110$

61.255.191.254

Ques- If the IP address of system S_1 is 194.112.116.67 and IP address of S_2 is 194.112.116.84. Subnet mask is 255.255.255.240

a) Identify whether the two hosts of ~~two~~ belong to a same subnet or not.

b) If they don't belong to the same subnet id then mention their subnet id no.'s.

S_1 belongs to Class C and S_2 also belongs to Class C.

S_1 : 194.112.116.67 — 01001101

(AND) 255.255.255.240 — Subnet id bits ← (111)0000

194.112.116.64 — 01000000 — 4th subnet

2	67	
2	33	1
2	16	1
2	8	0
2	4	0
2	2	0
	1	0

2	240	
2	120	0
2	60	0
2	30	0
2	15	0
	7	

S_2 : 194.112.116.84 — 01010100

255.255.255.240 — 11110000

194.112.116.80 — 01010000 — 5th subnet

Thus they don't belong to same subnet id.

Date:

Subnet id bits = 1111 0000

$S_1 = 4^{th}$

$S_2 = 5^{th}$

Que- IF IP address of S_1 is 210.116.112.37 and IP of S_2 is 210.116.112.48. ~~Subn~~ IP of S_3 210.116.112.86, IP of S_4 is 210.116.112.113, IP of S_5 210.116.112.131 and Subnet mask is 255.255.255.240.

a) Identify which of the systems belong to same subnet id.

S_1 : 210.116.112.37 | 00100101
255.255.255.240 | 11110000
210.116.112.37 → 2 | 00100000

S_2 : 210.116.112.48 → directly its a subnetid | 00110000
255.255.255.240 | 11110000
210.116.112.48 → 3^{th} | 00110000

S_3 : 210.116.112.86 | 01010110
255.255.255.240 | 11110000
210.116.112.80 → 5^{th} | 01010000

S_4 : 210.116.112.113 | 01110001
255.255.255.240 | 11110000
210.116.112.112 → 5^{th} | 01110000

S_5 : 210.116.112.131 | 10000011
255.255.255.240 | 11110000
210.116.112.128 → 8^{th} | 10000000

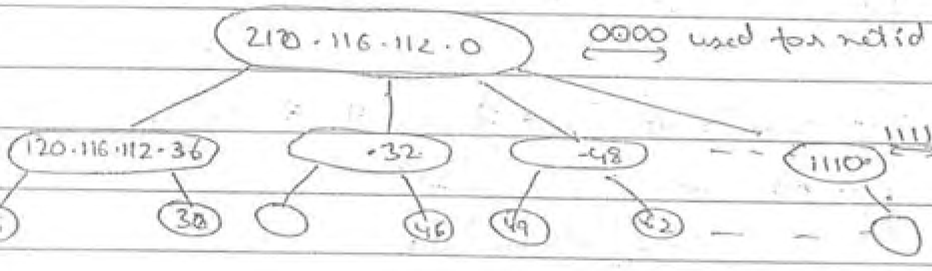
Hence, all hosts belong to different different subnets becoz no one's subnet id is same.

Que

Date:

Netid = 210·116·112·0

1^{st} subnet = 210·116·112·16
2^{nd} Subnet = 210·116·112·32 } difference is 16.



0000 used for netid

1111 not used because it is for directed broadcast to all subnets.

→ If mask is 255·255·255·197. and IP address is 213·111·110·116. Then Calculate 1^{st} host of 1^{st} subnet.

197 : 11000101

are subnet bits

11---1-1

1^{st} host 1^{st} Subnet = 00000011

= 3

1^{st} host - 0001
1^{st} subnet - 0001
adjust these in that

Above mask is not practically occur becoz we can't get consecutive subnet ids. and also their host differs.

2^{nd} host of 1^{st} subnet = 00001001

= 9

→ If mask is not continuous then, that will be not applied practically.

Ques- IF IP address of system is S_1 = 193·116·86·44 & subnet mask is 255·255·255·52. Calculate 1^{st} host of last subnet and 1^{st} host of 1^{st} Subnet.

3 subnet bits
00110100

1^{st} Subnet : _ _00_1_ _

1^{st} host of 1^{st} subnet = 00000101

= 5

ie 193·116·86·5

Date:

last subnet : _ _ 11 _ 0 _ _

1^{st} host of last subnet : 00110001

: 49

ie 193.116.86.49

Ques- IP address of S_2 = 196.171.112.89 , S_1 = 193.116.86.44

Subnet mask 255.255.255.57

57 : 00111001

89 : 01011001

00011001 = 25

Subnet id = 193.116.86.25

a) Identify the subnet id no.

57 : 00111001

Mask bits = 4

0111 → 7

→ Generally, Subnet mask will have continuous 1's and that can be applied practically. Subnet mask can also support non-contigious one's but it is theoritical.

b) In above problem, calculate the directed broadcast address of that subnet.

Subnet no. = 7

~~DBA~~ 11 0 11 111 → replace all host bits by 1's.

Ques- If a ip address of system is 199.16.14.221 and Subnet mask 255.255.255.39. Calculate subnet id.

221 : 11011100

Mask → 39 : 00100111

00000100

Subnet position

Subnet id value = 0101 = 5

Date:

Q) In above problem Calculate last host of 5^{th} subnet.

_ _ 0 _ _ 001

last host = 01110

So, 11010101 = 213

= 199.16.14.213

CLASSLESS ADDRESSING :

→ It consists of only blocks.

- If block has 1000 ids the 2 are not used.
- In this we give IP address and parallely we have mask.

→ In Classless addressing, there are no classes, only blocks are present.

Restrictions on Classless Addressing :

1) The 1^{st} address of a block should be exactly divisible by no. of addresses in a block.
2) Every address in a block must always be a power of 2,
3) The addresses must be contagious.

Ques- One of the addresses in a block is 167.199.170.82 / 27. Find the no. of addresses, 1^{st} address and the last address.

Notation known as Slash notation or CIDR

Mask : 27 → 11111111 . 11111111 . 11111111 . 111 00000 (5)

27 no. of 1's . 255 . 255 . 255 . 224. hosts or IP address.

this block consists of 2^5 = 32 addresses

No. of addresses in a block in identified by subnet mask.

1^{st} address :

82 → 010 10010 replaced by 0's

010 00000 = 64

1^{st} address will be all zero's

Date:

2^{nd} address :

010 00001 = 65

last address :

010 11111 = 95

Here 1^{st} address is used at Net id and last address used as directed broadcast.

Ques- One of the address in a block is 17.63.110.114/24. Find the no. of address, 1^{st} address, last address in the block.

24 : 1111111 1111111 1111111 0000000 ie $32-24 = 8$

No. of addresses = 2^8

1^{st} address :

114 → 01110010

all zero's

00000000

ie 17.63.110.0

last address :

1111111 = 255

17.63.110.255

Ques. One of the addresses in a block is 110.23.120.14/20 Find the no. of address, 1^{st} address, last address in the block.

No. of address = $2^{32-20} = 2^{12} = 4096$

1^{st} address :

Mask = 255.255.240.0   11110000

110.23.120.14   01111000

~~255.255.112.0~~   01110000

110.23.112.0 → Subnet id.

So, 1^{st} address is 110.23.112.0

110.23.112.0 —— 110.23.112.255 → 256

110.23.113.0 —— 110.23.113.255 → 256

110.23.127.0 —— 110.23.127.255 last address.

$256 \times 16 = 4096$

ie $2^8 \times 2^4 = 2^{12}$

To get 4096 address we have to

Ques. An org.^{n} is granted a block of address with the beginning address 14.24.74.0/24 The org.^{n} needs to have 3 sub-blocks of addresses to use in its 3 subnets. as follows :

1) One sub-block of 120 address
2) Another " " 60 address
3) " " " 10 address

nearest round figure of 120 addresses are 128. ie 2^7

Ist Subblock :

14.24.74.0/25 —— 14.24.74.127/25

To get 2^7 we have $2^{32-25} = 2^7 = 128$.

Yes we can accomodate 128 addresses in this block but we require 120 address.

So, some addresses are wasted, ie 8 wasted

IInd Sub-block :

nearest $= 64 = 2^6$

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

14.24.74.128/26 —— 14.24.74.191/26

Out of 64 we can accomodate 60 addresses.

4 addresses are wasted.

3rd Sub-block :

nearest $= 16 = 2^4$

$2^{32-28} = 2^4$

14.24.74.192/28 —— 14.24.74.207/28

Out of 16 we can accomodate 10 addresses.

6 addresses are wasted.

Total address the org.

Left over address after assigning $= 2^8 - (2^7 + 2^6 + 2^4)$

$= 256 - 208$

$= 48$ are left over which can be assigned to others

Date:

Ques. An ISP is granted a block of addresses has 190.100.0.0/16. Design the blocks in which 1st group has 64 customers and each customer requires 256 IP address. $\rightarrow 2^8$ mask

2nd group has 128 customers & each customer requires 128 IP address.

3rd group has 128 customers and each customer requires 64 IP addresses.

Total IP addresses = 2^{16}

1st group :

1st cust. → 190.100.0.0/24 — 190.100.0.255/24

2nd cust. → 190.100.1.0/24 — 190.100.1.255/24

64th cust. → 190.100.63.0/24 — 190.100.63.255/24

2nd Group :

1st cust. → 190.100.64.0/25 — 190.100.64.128/25

2nd cust. → 190.100.64.128/25 — 190.100.64.255/25

last before 128 cust.n → 190.100.127.0/25 — 190.100.127.127/25

last cust.n → 190.100.127.128/25 — 190.100.127.255/25

As 64 is shared by 2 cust.m So we have to add 64 which give 128 but we take 127 becoz extremes are also counted.

3rd Group :

1st Cust. → 190.100.128.0/26 — 190.100.128.63/26

2nd Cust. → 190.100.128.64/26 — 190.100.128.127/26

3rd Cust. → 190.100.128.128/26 — 190.100.128.191/26

4th Cust. → 190.100.128.192/26 — 190.100.128.255/26

$\frac{128}{4} = 32$ → no. of customer

So we have to add 31 value.

last before → 190.100.159.128/26 — 190.100.159.191/26 last add. → 190.100.159.192/26 — 190.100.159.255/26

Que- In above problem how many IP addresses are still left over.

$$2^{16} - (64 \times 256 + 128 \times 128 + 128 \times 64)$$

=

Ques- Given the n/w address of 112.44.0.0, Where Station1 ie S_1 has 112.44.22.19/16 & S_2 has 112.44.23.2/16 a) Identify whether these 2 hosts belong to same n/w or not.
b) Calculate the last address of that network if both host belongs to same network.

16 indicates mask ie 255.255.0.0

$2^{32-16} = 2^{16} = 65,536$ n/w address

1st address : 112.44.0.0/16

last address : 112.44.255.255/16

→ 0.0 to 0.255 → 256 getting

→ 1.0 to 1.255 → 256 getting.

!

22.0

!

23.0

!

255.0

So, these 2 hosts belong to same network.

OR

112.44.22.19
AND 255.255.0.0
112.44.0.0 → 1st address.

Ques- Stations with address S_1 = 172.16.22.1/22 S_2 = 172.16.23.9/2
What does these 2 stations network id. Is it same or not.
Then Calculate the broadcast address.

Date:

Mask = 255.255.252.0 11111100

S_1 : 172.16.22.1 00010110

172.16.20.0 00010100

S_2 : 172.16.23.9 11111100

255.255.252.0 00010111

172.16.20.0 00010100

S_1 and S_2 belong to same network.

Broadcast address :-

172.16.~~20~~ 23.255/22 host bits = 10

$2^{32-22} = 2^{10} = 1024$ IP required.

20 : → 20.0 — 20.255 → 256

21.0 — 21.255 → 256

22.0 — 22.255 → 256

23.0 — 23.255 → 256

1024

Ques - Which of the following devices share the same n/w.

A 192.168.78.25/29

B 192.168.78.23/29

C 192.168.78.33/29

D 192.168.78.38/29

E 192.168.78.41/29

Mask = 255.255.255.248

A= ~~25~~

AND ~~248~~

$2^{32-29} = 2^3 = 8$ IP required by each.

00000 000 → 0

00001 000 → 8

00010 000 → 16 ... N/w's

host bits.

(0 - 7)

(8 - 15)

(16 - 23) → 23 available

(24 - 31) → 25 available

(32 - 39) → 33 available, → 38 available.

C and D share same network

Ques- Which of the following would support best point-to-point link?

A → 255.255.255.258

B → 255.255.255.0

C → 255.255.255.128

D → 255.255.255.252

E → 255.255.252.0

Point to point link require only 2 addresses.

$2^2 - 2 = 2$

No. of host bits = 2 ie 2 bit must be 0

A → 1 left bit

B → 8 bits left → 256 hosts

C → 128 host

D → 2 bits left → 2 hosts possible

E → 2^{10} left → 1024 hosts possible.

Ques- Which address should not be advertised to the internet.

A 172.12.0.1 (Public IP)

B 192.168.0.23 (Private IP)

C 10.0.78.2 (Private IP)

D 112.56.22.5 (Public IP)

E 127.0.0.1 (loop back address ie Special address) used for testing whether system getting IP pkt from remote system

On internet we can advertise only public IP. ie we can't advertise private IP & special IPs.

→ loop back address is used to check whether the connection is correct or not. or cable is connected correctly or not.

It will never enter into the internet.

Characteristics of loop back:

1) Always used as DIP

2) It is also used for interprocess comm.^{n} within the same host becoz it is not going to other system it just comes back from the port of other system.

Ques- What is the broadcast address and n/w address?

192.168.99.77 /19

Mask = 255.255.224.0

$2^{32-19} = 2^{13}$

Host ⇒ 192.168.99.77

255.255.224.0

192.168.96.0 → n/w address.

Broadcast address :

$\underbrace{0110\,0000}_{}\cdot\underbrace{00000000}_{Host}$

$0 1 1\,11111 \cdot 11111111$

255

192.168.127.255

Ques- What is the zero sub-net address for a system

164.20.227.6 /19

Asking net-id.

164.20.227.6	1110 0011
255.255.224.0	1110 0000
164.20.224.0	1110 0000

→ Subnet id.

Net-id = 164.20.0.0. (zero subnet)

Ques- In above problem calculate the broadcast subnet.

164.20.224.0

all 1's in subnet bits.

→ broadcast subnet

000 → zero subnet

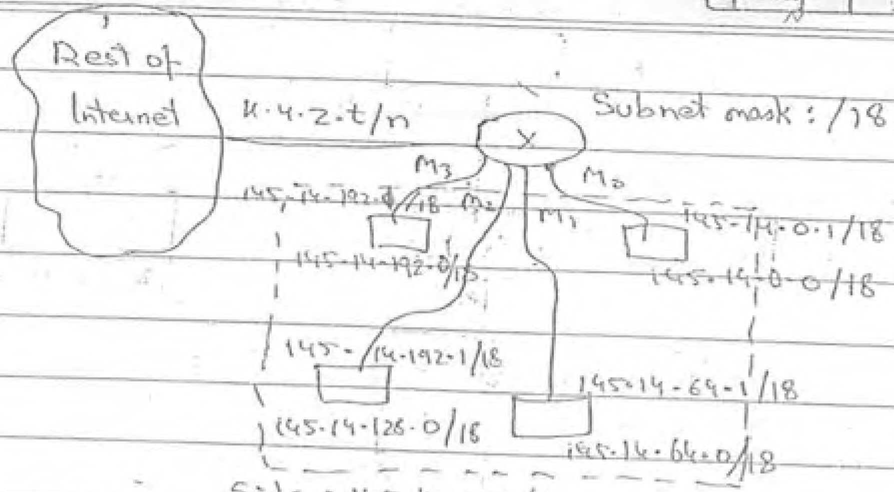
001

010

⋮

111 → broadcast subnet.

Ques-1-



Site = 145.14.0.0/16

Diagram is of multipart device.

The router receives the pkt with the dest.ⁿ address 145.14.32.78. Show how the packet is forwarded.

Subnet address	Next hop address	Internet Interface no.
145.14.0.0	-----	m0
145.14.64.0	-----	m1
145.14.128.0	----	m2
145.14.192.0	----	m3
0.0.0.0	Default router.	m4

Qn. A host in n/w 145.14.0.0 has a packet to send to the host with the address 7.22.67.91. Show how the packet is routed.

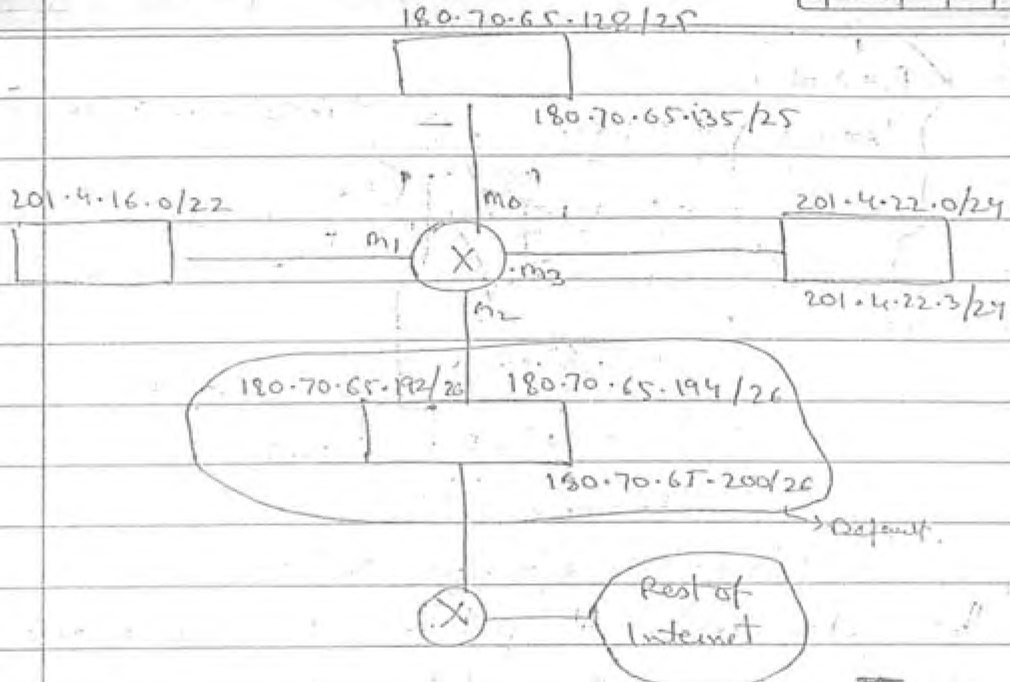
Sol: 1:

145.14.32.78
255.255.192.0
145.14. ~~32~~ 0 .0

11000000
00100000
00000000

It will route from m0 Interface.

Ques -



a) Calculate Routing table for R_1?

MASK	N/w Address	Next hop	Interface.
/26	180.70.65.192	---	m_2
/25	180.70.65.128	---	m_0
/24	201.4.22.0	---	m_3
/22	201.4.16.0	---	m_1
Default	Default	180.70.65.200	m_2

b) Show the forwarding process if a pkt arrives at R_1 with destn address 180.70.65.140.

180.70.65.140
255.255.255.192
180.70.65.128

11000000
10001100
10000000

Packet is process through m_0

180.70.65.140
255.255.255.128
180.70.65.128

10000000
10001100
128

So packet will go through m_0

c) Show forwarding process if pkt arrives as R_1 with destn address 201.4.22.35

201.4.22.35
255.255.255.0
201.4.22.0 Through m_3

11

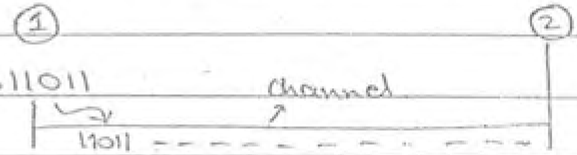
Date:

→ At sender we add headers, but at receiver we removes header.

→ This architecture is known as Protocol stack architecture becoz like stack 1st header added is removed at the ~~end~~ or the last header is added at the sender side is the 1st header removed at receiver side.

eg:-

Time taken to generate data is Processing Time



- Processing time depends on the clock of CPU and the memory capabilities.

→ Time taken to generate the data is called processing time.

Time taken to place the data on the channel is known as Transmission time.

⇓

Depends on msg size and bandwidth.

Qus- If the msg size is 1KB, bandwidth is 1 mega bits/s. Calculate the transmission time.

$$\text{Transmission Time} = \frac{1 \times 10^3 \text{ Bytes}}{10^6 \text{ bits/sec}}$$

$$= \frac{8 \times 10^3}{10^6 \text{ bits/sec}} = 8 \times 10^{-3} \text{ sec}$$

$$= 8 \text{ millisec}$$

$$\boxed{\text{Transmission Time} = \frac{\cancel{\text{Bandwidth}}\ \text{Msg size}}{\text{Bandwidth}}}$$

Data has to be propagated to reach the destination

Date:

this time is known as propagation Time
⇓
depends on Distance & velocity

$$\text{Propagation Time} = \frac{\text{Distance}}{\text{Velocity}}$$

Ques- If distance b/w sender & receiver is 3 km & velocity is 2×10^8 m/sec. Calculate the propagation time.

$$\text{Propagation time} = \frac{\text{Distance}}{\text{Velocity}}$$

$$= \frac{3\times10^3 \text{ m}}{2\times10^8 \text{ m/sec}}$$

$$= 1.5\times10^{-5} \text{ sec}$$

$$= 15\ \mu\text{sec}$$

→ Acknowledgment size is small which is given by receiver.

$$\text{Transmission Time}_{ack} = \frac{\text{Ackn. Size}}{\text{Bandwidth}}$$

• $T.T_{ack}$ is small as Ack. size is small so, we can neglect this $T.T_{ack}$.

$$\text{Propagation Time}_{ack} = \frac{\text{Distance}}{\text{Velocity}}$$

$$\text{Total Time} = T.T_{data} + P.T_{data} + P.T_{ack}$$
$$= T.T + 2.P.T$$

→ Sender has only utilized transmission time after transmission, sender is only waiting for acknowledgment.

$$\text{Link Utilization of Sender} = \frac{T.T}{T.T + 2\times P.T}$$

Page No. ______
Date:

→ Two times of propagation is called as round trip time.

$$\boxed{R.T.T = 2 \times P.T}$$

→ P.T to transmit data to receiver
→ P.T to transmit ack to sender.

Qus- If the link utilization is to be 50%, P.T is 10 millisec. Calculate the Transmission time.

$$\frac{50}{100} = \frac{T.T}{T.T + 2 \cdot 10}$$

$$\frac{1}{2} = \frac{T.T}{TT + 2 \cdot 10}$$

$$T.T + 2P.T = 2T.T$$

$$TT = 2 \cdot P.T$$

$$= 2 \times 10 \text{ millisec}$$

$$= 20 \text{ millisec}$$

Qus- If the link utilization is 75% and round trip time is 10 millisec. Calculate the transmission time.

$$L.U = \frac{T.T}{T.T + R.T.T}$$

$$\frac{3}{4} = \frac{T.T}{T.T + RTT}$$

$$3T.T + 3R.TT = 4.TT$$

$$TT = 3 \times RTT$$

$$= 3 \times 10$$

$$= 30 \text{ millisec}$$

Qus- If the message size is L and B is bandwidth and R is the Round Trip Time. Calculate the link utilization of the sender.

$$L.U = \frac{T.T}{T.T + 2 \cdot P.T}$$

Date:

$$L.U = \frac{L/B}{L/B + R}$$

$$\boxed{L.U = \frac{L}{L+BR}}$$

$$\eta = \frac{L}{L+BR}$$

→ If $L = BR$, $\eta = 50\%$.
If $L > BR$, $\eta > 50\%$.
If $L >>> BR$, $\eta = 100\%$
If $L < BR$, $\eta < 50\%$.
If $L << BR$, $\eta \simeq 0\%$

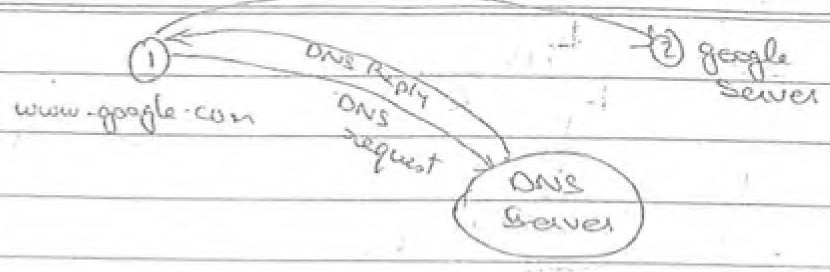
→ Physical address points Datalink layer → Bridge
logical address points network layer → Router
Port address points to Transport layer. → ~~Gateway~~ Gateway.

Application layer : Provides services like HTTP, FTP, NTP, SMTP, DNS, SNMP, NNTP, encryption.
↳ N/W news Transport Protocol used for news

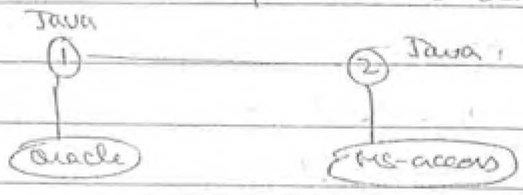
- Http provides
- NTP provides service in which time is converted according to requirement (N/W Time Protocol)
- SNMP provides services for

Layers	Devices
Application	Gateway
Presentation	Gateway
Session	Gateway
Transport	Gateway
Network	Router
Data link	Bridge
Physical	Repeater, Web.

Date:



Presentation layer : Provides services dealing with syntaxs and semantics of data.



→ Data is taken in MS-access format and present.^{n} layer converts this format into oracle format.

ie

All format conversion done by Presentation layer.

Session layer : It provides session between systems, dialog control and token mgmt.

- It decides transmission type.

1 ⟶ 2 : Simplex

1 ⇠ - - - - ⇢ 2 : Half duplex (In both sides but one after another)

1 ⟷ 2 : Full duplex (Transmission is 2 way, xchang Simultaneously)

→ In the practical model ie in TCP/IP, the services of presentation and session layer are included into the appl.^{n} layer becoz both have simple services.

So, TCP/IP has 5 layers.

Datalink layer : It provides flow of control within LAN only
• Error Control by CRC

① 8086 → It transmits data slowly → becoz it should have slow transfer rate.

② Pentium → It will take data very fastly. → ∴ have fast transfer rate.

So, No sychronisation in b/w two systems.

① CPU → Flipflops

Cache M/M → Flip-flops → Provide Synchronization

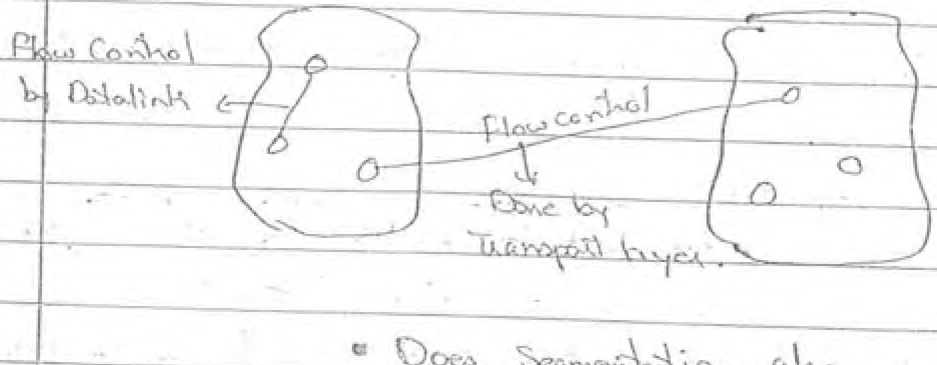
② M/m → Semi-conductors + comb^n circuits.

Is local : Flow Control within LAN : Datalink layer.
Is Global : Flow Control outside LAN : Transport layer.

→ Flow control at datalink layer is only link to link ie within the LAN.

→ Whereas aflow control at transport layer is end to-end. and does error control by checksum.

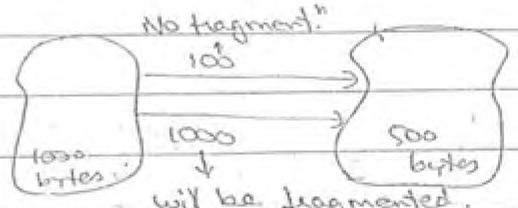
Transport layer : Provides flow of Control from end to end which is known as Global flow of control.
• Perform error control by checksum from end-to-end.



• Does Segmentation also.

Date:

Network layer : Performs Routing, fragmentation and Traffic Shaping.



→ If the upper layer data is greater than the data of the MSS (maximum segment size), than it is divided into segments.

→ When a packet is approaching to a LAN network, if size of the packet is greater than the maximum transferable unit (MTU) of the LAN, then the packet is fragmented.

type of cable

PHYSICAL LAYER : Deals about the physical, electrical and mechanical characteristics of cable).

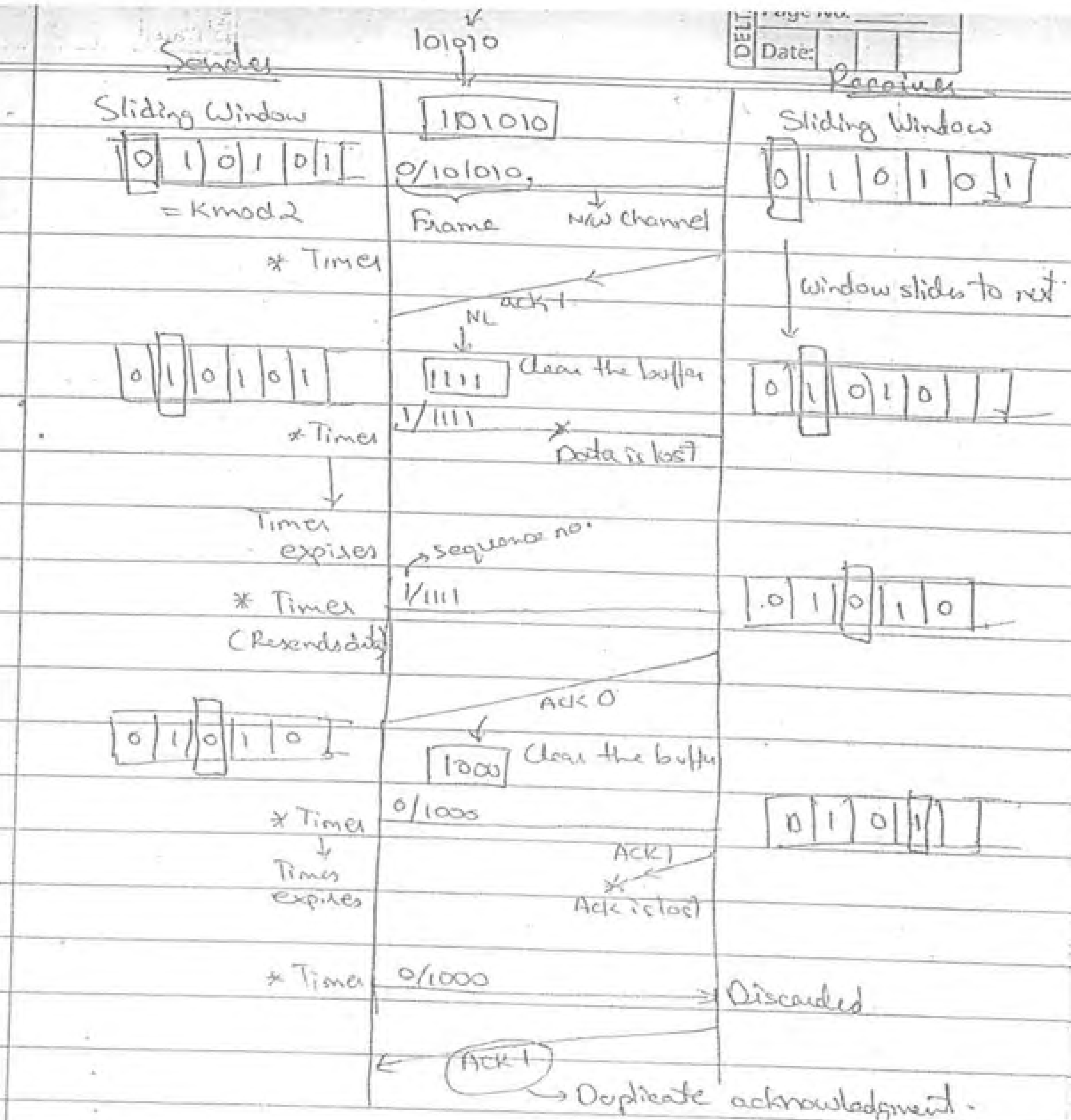
How 0/1 are Triggering

0 → 0V → -5V
→ -9V

1 → 5V → +9V
→ +12V

→ FLOW CONTROL AT DATA LINK LAYER :

- It accepts data in packet form from Network layer.
- DLL has buffer & it maintains 2 windows ie
  1) Sender Sliding window
  2) Receiver Sliding window.
- It add extra bit to packet and now it is known as frame. ('0 is extra bit added)
- ACK no. is expected sequence no. of next frame required.



CASE 1 : Copy of buffer data put on channel.

↓

Add sequence no. to data called frames now is send.

↓

Receiver checks sequence no., if sequence no. matches with window sequence no., data is accepted by receiver

↓

After accepting data window will slide to next sequence no.

Date:

Qus-

→ The sender window size and receiver window size and in ~~stop and wait~~ ARQ is one.

⇓

15 Protocol

→ Window size always determines the no. of frames ~~transf~~ transmitted.

→ In a round trip time, the no. of frames transmitted in a Stop & wait ARQ are 1.

→ Sender Window size + Window Size at receiver is ~~equal to~~ will always be equal to distinct sequence no. in that protocol.

Date:

→ Stop and Wait ARQ supports individual frames and individual acknowledgment.

→ When cumulative frames are transmitted then we are having pipeline. ⇒ when more than 1 frame is transmitted in 1RTT

→ In Stop and wait ARQ, there is no pipeline.

→ The ack no. will always be the sequence no. of the next expected frame.

Qus- If the bandwidth is 1Mbps and frame size is 100 bits How many frames are transmitted in a Round Trip time of 100 millisec.

Conversion of BW:

$$1 \text{ sec} \longrightarrow 10^6 \text{ bits}$$

$$100 \text{ millsec} \longrightarrow 100 \times 10^6 = 10^8 \times 10^{-3} \text{ bits}$$

$$\Rightarrow 10^5 \text{ bits.}$$

So, 10^5 bits can be transmitted in ~~RR~~ RTT.

$$\text{No. of frames} = \frac{10^5 \text{ bits}}{10^2}$$

$$= 1000 \text{ frames.}$$

Q) In above problem calculate the efficiency of Stop and wait ARQ.

$$\eta = \frac{100}{10^5} \times 100$$

~~In Stop & wait in RTT we can transmit~~ 1 frame ~~as~~ frame size = 100.

In Round trip time we can transmit 10^5 bits.

$$= 0.1\ \%$$

→ Efficiency is less in Stop and wait ARQ.

→ To improve efficiency, send more frames in a Round Trip time.

Date:

Ques- The R.T.T is 200 msec and bandwidth is 10 Mbps. Calculate the no. of bits to be transmitted in a R.T.T

$1 sec \longrightarrow 10 \times 10^6$ bits

In 200 msec $\longrightarrow \frac{200 \times 10^{-3} \times 10^7}{10}$ bits

$= 2 \times 10^6$ bits

= 2 megabits.

Ques- In above problem if frame size is 1000 bits. Calculate the window size.

Window size = No. of Frames in R.T.T

$= \frac{\underbrace{2 \times 10^6}_{\text{bits transfer in R.T.T}} \text{ bits}}{\underbrace{10^3}_{\text{Frame size}} \text{ bits}}$

= 2000 frames

Ques. In above problem if stop and wait is used then what is the efficiency

R.T.T = 1, we are transferring 1 frame in RTT

But channel accomodate 2000 frames in 1 R.T.T

$\eta = \frac{1}{2000} \times 100$

$= 0.05\%$

Ques-

$\eta = \frac{\text{1 in RTT}}{\text{Total frames channel can accomodate}} \times 100$

Ques- If the distance is 5 Km and velocity = 2×10^8 m/sec B.W = 10 Mbps. Calculate no. of bits in RTT.

$P.T = \frac{\text{Distance}}{\text{Velocity}} = \frac{5 \times 10^3 \text{ Km}}{2 \times 10^8 \text{ m/sec}}$

$= \frac{5 \times 10^3 \text{ m}}{2 \times 10^8 \text{ m/sec}} = 2.5 \times 10^{-5}$ sec

$= 25\ \mu sec$

Date:

R·TT = 2 × P·T

= 2 × 25 μsec

= 50 μsec.

B·W : 1 sec ⟶ 10^7 bits

50 μsec ⟶ $50 \times 10^{-6} \times 10^7$ (μ to sec conversion.)

= 500 bits.

No. of bits in R·TT = 500 bits

Qus. In above problem if frame size is 100 bits. What is the time taken to send 500 bits in Stop and wait ARQ.

Window Size = $\frac{500}{100}$ = 5

In Stop & wait ARQ, R·TT = 1

50 μsec ⟶ one frames.

frame size = 100 bits

50 μsec ⟹ 100 bits

In 250 μsec ⟸ 500 bits

Qus. If transmission time, T·T = 50 millisec, frame size = 1000 bits. R·TT = 100 μsec Calculate the no. of bits that are transmitted in RTT.

$$T \cdot T = \frac{\text{frame size}}{B \cdot W}$$

$$50 \times 10^{-3} \text{ sec} = \frac{1000}{BW}$$

$$BW = \frac{1000}{50 \times 10^{-3}}$$

μ - 10^{-6}

$$= 20 \times 10^3$$

= 20 kilo bits per sec.

1 sec ⟹ 20×10^3 bit.

R·TT ⟹ 100 μsec ⟶ $20 \times 10^3 \times 100 \times 10^{-6}$ = 2000×10^{-3}

= 2 bits

Date:

Ques- If velocity of data is 2×10^8 m/s ; B.W = 10 Mbps
Calculate 1 bit delay in terms of meters of cable.
(1 bit delay means Time for 1bit)

Sol: BW: 1 sec $\longrightarrow 10^7$ bits

$\frac{1}{10^7}$ sec $\longleftarrow$ 1 bit

0.1 μsec $\longleftarrow$ 1bit

Velocity: 1 sec $\longrightarrow 2 \times 10^8$ m

1bit delay (0.1 μsec) $\longrightarrow 0.1 \times 2 \times 10^8 \times 10^{-6}$

= 20 metres of cable

Ques- Between two systems we have 3 interfaces and each interface has 2 bit delay, BW of channel is 10 Mbps
Calculate the delay introduced by the interfaces in seconds.

1 sec $\longrightarrow 10^7$ bits.

2 bit delay $\longrightarrow \frac{1}{10^7} \times 2$

$= 2 \times 10^{-7}$

~~Total delay~~ = 0.6

1 bit $\longrightarrow \frac{1}{10^7}$ bits

6 bit delay $\longrightarrow \frac{6}{10^7}$

= 0.6 μ sec

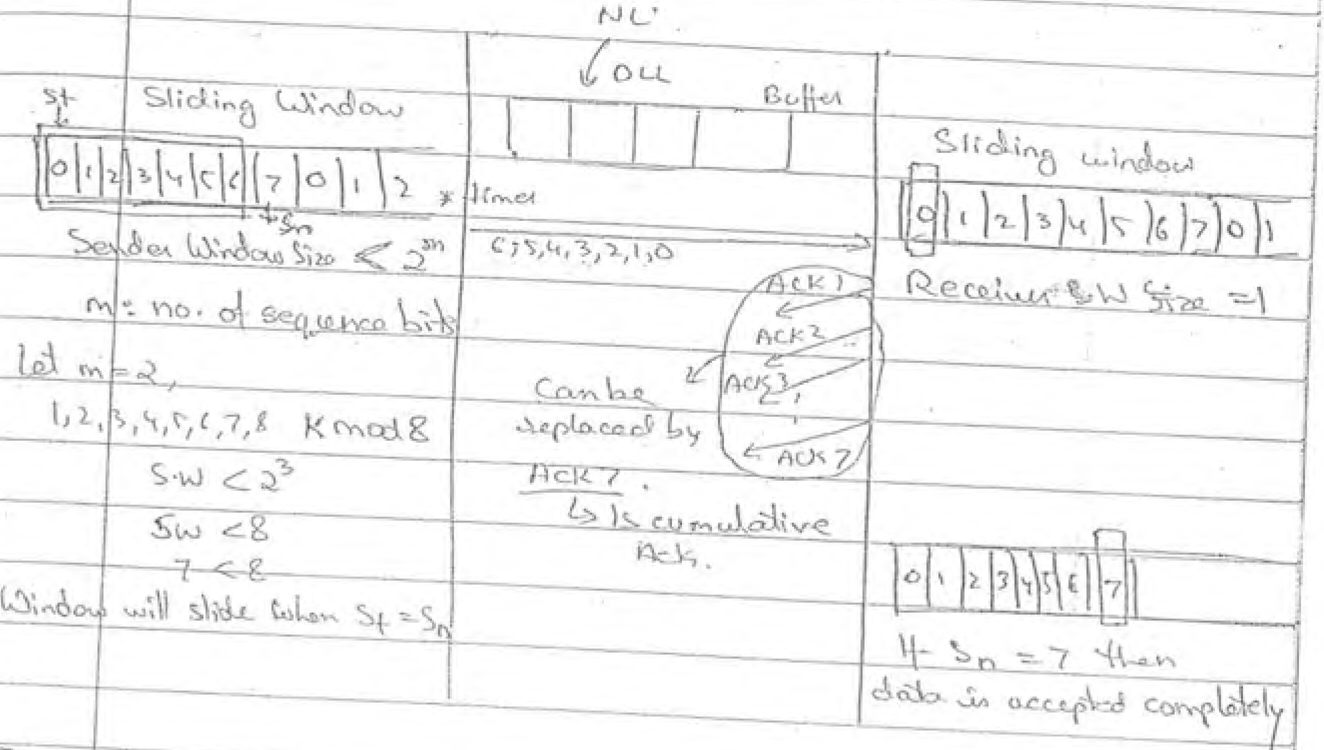
3 interfaces will have 6 bit delay total.

GO BACK N ARQ :

→ Used to improve efficiency
→ To transmit more than 1 frame in 1 RTT
→ Stores more no. of packet in a buffer.

Date:

→ In Go Back N ARQ the buffer requirement is larger compared to the buffer requirement in Stop and Wait ARQ.



Que. In Go back N ARQ if sequence bits are taken as 5, then what is the sender window size & receiver's window size.

$2^5 = 32$

Sender window size = 31

Receiver " " = 1

Que. In above problem if sequence bits 6, What is SWS and RWS.

SWS ↓ Sender Window Size

$2^6 = 64$

SWS = 63

RWS = 1

If window size is n, then we can transmit n frame in R.TT at a time

Date:

→ Go back N ARQ supports cummulative frames.

⇓

It supports both individual & cumulative Ack.

⇓

is better choise becoz efficient use of B.W.

→ Cumulative ack. is better choice compared to individual acks becoz n/w Traffic will be less.

→ In Go back N ARQ, if frame is lost, the lost frame as well as the frames following the lost frame are also to be re-transmit.

→ If channel has more no. of errors or error rate is high, the efficiency is going to decrease in Go Back N ARQ.

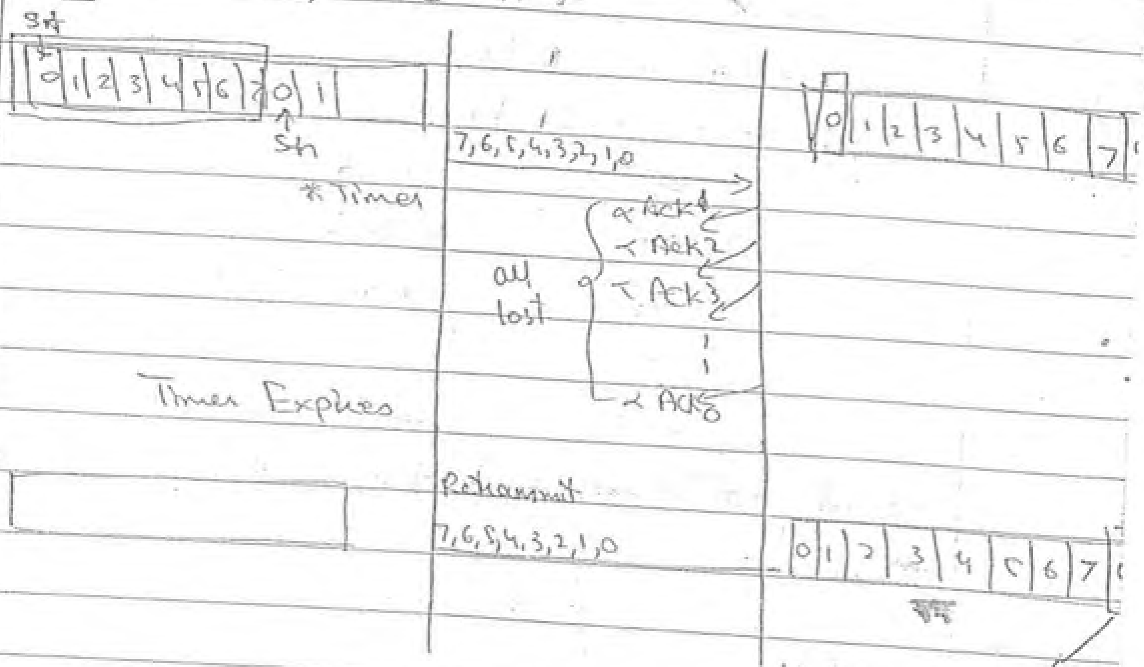
Disadvantage of GO Back ARQ is we have to resend all frames ~~follow~~ which are followed by damaged frame.

To improve efficiency, transmit only damaged frame

→ Why Window Size $< 2^m$ in Go Back N ARQ

Date:

1) If $S.W = 2^m$; $m = 3$



It is expecting next frame but it will get same frame ie previous

It fails, So,

2) If $S.W < 2^m$, $m = 3$

When all ack lost then $S_n \neq S_f$ so ie $0 \neq 7$ so it receiver will not except that frame and discard those retransmitted frames.

Qus- What will be the sequence no. of 30^{th} frame if 3 bits sequence no. is used in go back N ARQ.

(0 – 7) → 7 frame

(7 – 5) → 7 frame

(6 – 4) → 7 frame

(5 – 3) → 7 frames

28^{th} frame → Sequence no. 3

29^{th} frame → s. 4

30^{th} frame → 5 sequence no.

Qus- If 5 bit sequence no. is used, what will be the sequence no. after sending 100 frames.

(0 — 30) → 31 frame

(31 — 29) → 31 frame

(30 — 28) → 31 frame

~~93th frame → 28~~

~~94th → 30~~

~~98th → 31~~

~~99th → 32~~

~~100th → 0~~

~~So, after 100th frame sent then we have 0th sequence~~ no.

93th → 28

94th → 29

95th → 30

96 → 31

97 → 0

98 → 1

99 → 2

100 → 3

After 100th frame 4 sequence no.

Ques. If M is max. sequence no. in sliding window of Go back N ARQ. Calculate the no. of frames that can be transmitted in a R.T.T of Go back N ARQ.

Take eg:-

3 bit sequence no.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

Max. M = 6 M = 7

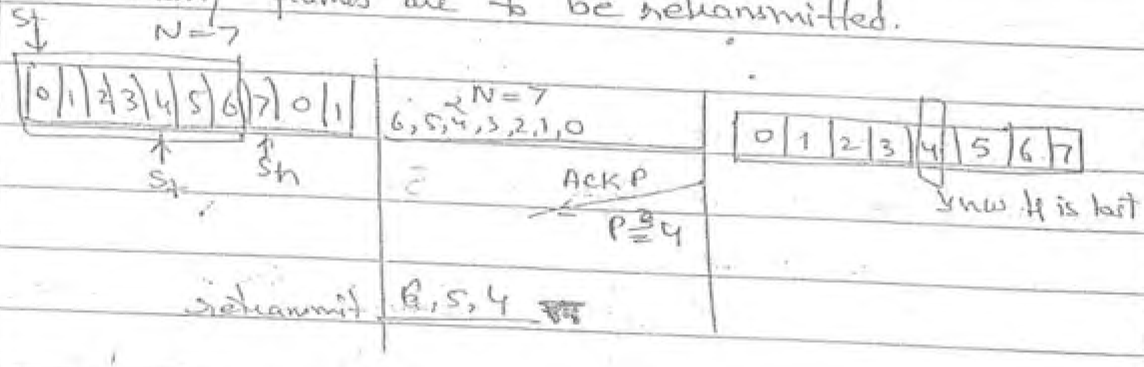
So M = 7

So, We are transmitting 7 frames.

So, N no. of frames can be transmitted.

Date:

Qus- If the size of the window is N and N frames are transmitted. It is supporting cumulative ACK. The ACK no. that is transmitted by the receiver is ACK P. Then
a) Calculate the how many frames are received to the receiver
b) How many frames are to be retransmitted.



a) P frames are received.
b) (7-4) = 3 so N-P frames are to be retransmitted.

Ques- If K is the sequence bits that are used and L is the cumulative Ack.
a) How many frames are reached to dest^n
b) How many frames are to be retransmitted.

Sol: a) L
b) $(2^K - 1) - L$

window size

Qus- If senders window size in Go Back N ARQ is 'Q'. Calculate the no. of sequence bits taken.

$\log_2 (Q+1)$

$0-6$ = window size = $7 \rightarrow Q$

$\log_2 (8) = 3$ ie 3 sequence bits.

Qun- B.W = 10 Mbps , R.T.T = 100 μsec , Frame Size = 50 bits
Go back N ARQ is used. Calculate window size, no. of Sequence bits.

Date:

$1\,sec \longrightarrow 10^7$ bits.

$100\,\mu sec \longrightarrow 100 \times 10^7$

$= 10^9 \times 10^{-6}$

$= 1000$ bits.

No. of frames $= \frac{1000}{50}$

$= 20$,

Window size $= 20$.

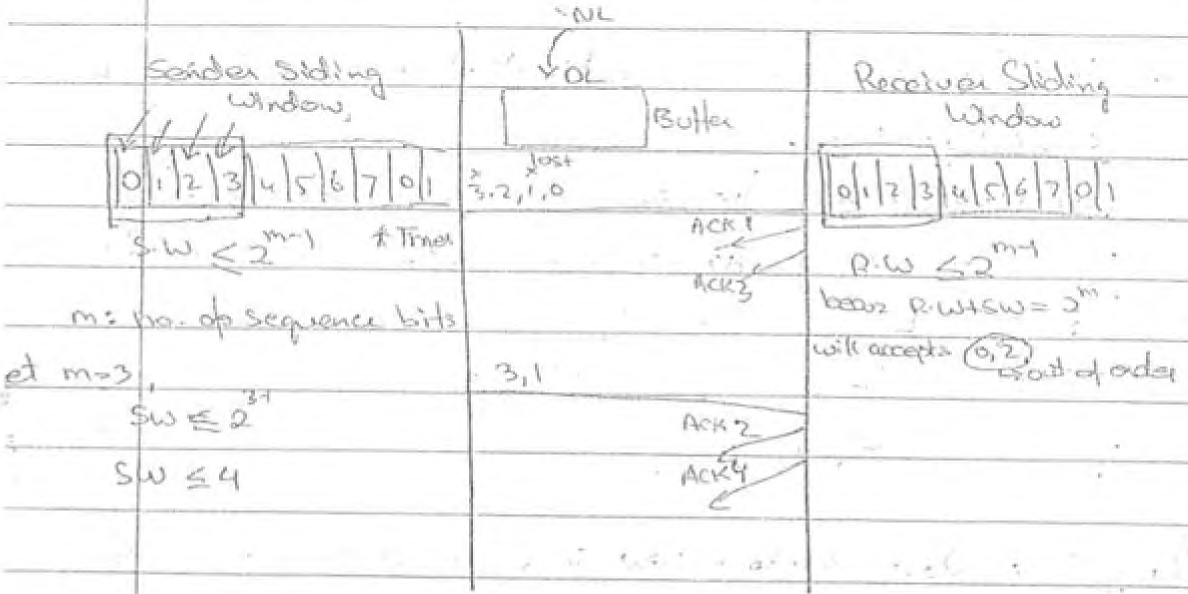
~~Seq~~ No. of Sequences $= 5$

becoz if $n = 5$

we can transmit $2^5 = 32$, less than 31

ie we can transmit 20 frames in 32 ~~bit~~

→ SELECTIVE REPEAT / REJECT ARQ :



→ Stop and wait & Go back N ARQ accepts only in-order frames.

→ Selective Repeat / reject ARQ accepts out-of-order frames.

→ Sender will have ~~select~~ searching logic and receiver will have sorting logic.

Date:

→ Receiver will apply sorting logic when 4 frames it got, then only otherwise it will not apply sorting logic.

→ This ARQ supports individual Ack becoz it is accepting out-of-order frames.

When ACK1 reached to sender, then it will search 0 frame and when ACK3 reach, sender again apply search to search 2nd frames. MeanWhile, timer will expire.

⇓

Now, frames which are not searched are retransmitted to ~~send~~.

⇓

~~When~~ Now receiver got 4 frames, so it will apply sorting and slide the window.

→ Sorting logic is required becoz receiver accepting out-of-order frame and network layer will accept frames in in-order.

→ Sender should have searching logic. It is an indication that frames are reached to the destⁿ

- Once all frames are searched the sender window slide.
- Once the no. of frames = count value of sorting logic, sorting algo will be applied and sorted frames are given to the N/W layer at the receiver side.

→ Complexity is high in selective repeat / reject ARQ becoz we are retransmitting only the damaged frame.

Ques- If N is size of the window in Selective repeat ARQ calculate the no. of sequence bits used.

$N = 2^{m-1}$

$\log N = (m-1)\log 2$

$\log N = m-1$

$m = \log N + 1$

(OR) $= \log 2N$

$= \log_2 2 + \log N$

$= 1 + \log N$

Ques- If 5 is no. of sequence bits used. Calculate the size of senders of window & receivers window in selective Repeat ARQ, go Back N ARQ

In Selective Repeat :

$S.W = 2^{5-1}$

$= 2^4 = 16$

$R.W = 2^{5-1}$

$= 2^4 = 16$

In Go Back ARQ :

$S.W < 2^{5-1}$

< 32

$SW = 31$

$R.W = 1$

Ques- If B.W = 10 Mbps & R.T.T = 1000 μS, Frame Size = 100 bits Calculate the no. of sequence bits used in Selective Repeat ARQ to transmit the data in R.T.T

$1 \text{ sec} \longrightarrow 10^7 \text{ bits}$

$1000\ \mu s \longrightarrow 10^7 \times 1000 \times 10^{-6} \text{ sec bits}$

10^4 bits

In R.T.T no. of frames $= \frac{10000}{100} = 100$ frames

Date:

In Go back ARQ ;

$2^7 = 128$ So we can transmit 100 frames.

In Selective Repeat ;

$2^8 \rightarrow \frac{2^8}{2} = 2^7 = 128.$

→ becoz S.W & R.W have 1/2, 1/2 frames

So, no. of sequence bits = 8

Ques. If M is the maximum sequence no. in Selective Repeat ARQ. What is the size of the Window in Selective Repeat ARQ.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

3 7

M = 7

and S.W = 4

ie Window Size = $\frac{M+1}{2}$

Ques. If N is the total sequence no. used what is the size of the window in Selective Repeat ARQ.

Window Size = $\frac{N}{2}$

Let above example, then N = 8 So, we have to S.W = 4

So, S.W.S = $\frac{8}{2}$ = 4 = $\frac{N}{2}$

→ ERROR CONTROL :- (AT DATA LINK LAYER)

→ To control error, we have to add extra bit to data

⇓

called as Redundant bits.

→ Data + Extra bit = Code Word

To add extra bit we follow parity Rule.

bits = 2 bit = 3

even Parity

Sender	Codeword
00	000
01	011
10	101
11	110

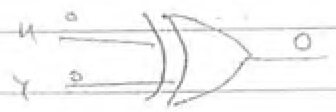
Codewords which are generated from the data are known as Valid Codewords.

As codeword size = 3 bit, so we got 8 combinations in which 4 codewords are valid and 4 are invalid codeword.

Parity Generator :

x	y	0
0	0	0
0	1	1
1	0	1
1	1	0

Codeword generated inside System



At receiver side also system generate codeword by using parity generator.

example :

Codeword

~~00~~ 011 - - - - → 111 } 1 bit error.
010
001 → Receiver will not accept the data

modified by noise in channel

Parity Scheme

↓

is scheme detect only bit error.

1 bit modified

110 - - → 111 → Not matching
detect 1 bit error only

→ To make statement all possible errors must be detected

Date:

Qn. Why does this scheme detect only one bit error?
When 2 valid Codewords are exor then the result is hamming distance.

ie 000
011

011]→ 2 1's then So 2 is the hamming distance

If different hamming distances are present then take the minimum hamming distance.

Condition
→ To detect d errors, Minimum hamming distance d+1
→ To detect 1 error, " " " 2.

This scheme is called the parity Scheme.

DISADVANTAGE :

- Parity Scheme is only valid for detecting odd bit errors. or odd no. of errors. based on above condition ie It is not good for detecting even no. of errors. becoz minimum hamming distance is d+1 in this scheme.

Qus. How many bit error is detected :

Sender	Receiver
00001111	00001111
00000000	00000000
11110000	11110000
11111111	11111111

4, 4, 8, 8

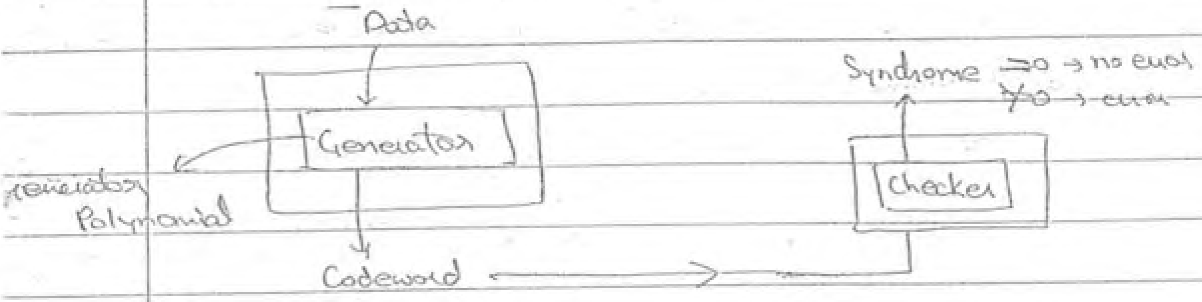
00001111
(+) 00000000

00001111 ⇒ 4

00000000 → 00001111 Not detect
→ 01010101 Detect
} 4 bit, 2 bit

→ 01010100
→ 00000111
→ 11100000
} 3 bit error all are detected.

CRC (Cyclic Redundancy Code) :



→ If Syndrome = 0 , then no error in data
If Syndrome ≠ 0 ; then error in the data.

$\Downarrow$

Is the remainder generated by checker.

G(x) ⇒ Generated by generator.
M(x) ⇒ which we have to transmit.

To perform CRC operation we require :

1) Ex-or
2) Shift register.

} performed by generator, internally.

If no. of bits are N on generator then we have to take N-1 paddy bits..

If MSB is either 1,1 or 0,0 then don't touch those MSB bits.

ie 11010 → Indirectly these are shifted by shift register so we are not touching those 2 bits.
10011
not Touched 0001

Pg-106

Ques 20-

$G(x) = x^4 + x + 1$

$M(x) = x^7 + x^6 + x^4 + x^2 + x$

$G(x) = 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1 \cdot x^0$

$= 10011$

$M(x) = 1\cdot x^7 + 1\cdot x^6 + 0\cdot x^5 + 1\cdot x^4 + 0\cdot x^3 + 1\cdot x^2 + 0\cdot x^1 + 0\cdot x^0$

$= 11010110$

```
10011 ) 110101100000 ( 11000010
        10011
         10011
         10011
          00001
          00000
           00010
           00000
            00100
            00000
             01000
             00000
              10000
              10011
               00110
               00000
                0110
```

$\boxed{0110}$ ~~Sepnds~~

Replace padding bits by this

Now, Codeword = ~~1001~~ 110101100110

$T(x) = x^{11} + x^{10} + x^8 + x^6 + x^5 + x^2 + x^1$

Pg-106

Qus 21- Received = 101110001111

Transmitted = 110101100110 (Ex-or)

011011101001

7 bits are 1's, So 7 bits are defered.

Pg-197

Qus 34 $G(x) =$ ~~0001~~ 1011

$M(x) =$ ~~01111011110 1110~~ 1101011001

1011 | 1101011001000 | 1111010110

1011
1100
1011
1111
1011
1001
1011
0100
0000
1000
1011
0111
0000
1110
1011
1010
1011
0010
0000

$\boxed{010}$

Codeword = 1101011001010

$= x^{13} + x^{12} + x^{10} + x^{8} + x^{7} + x^{4} + x^{2}$

Pg-105
Ques 15

$T.T = \frac{1}{b}$

$R.R = R$

$U = \frac{TT}{TT + 2PT}$

$= \frac{1/b}{1/b + R}$

(c) ✓

Date:

Pg-104

Ques 10

B.W :- 1 Sec ——— 155×10^6

60 ms ——— $155 \times 10^6 \times 60 \times 10^{-3}$

$= 930 \times 10^4$

$= 93 \times 10^5$

No. of frames $= \frac{93 \times 10^5 \text{ bits}}{53 \times 8 \text{ bits}}$ = Window size

$= 21900$

$2^{16} = 65,536$

$2^{15} = 32, \ldots$

$2^{14} = 16, \ldots$

For Go back N ARQ, no. of sequence bits are 15 bits.

Pg-104

Ques 11

Throughput $= \frac{\text{Total data}}{T.T + 2 \times PT}$

$T.T = \frac{5000}{9000} = 0.55 = \frac{5}{9}$ sec.

$P.T = \frac{2000}{200,000} = 0.001 = \frac{1}{100}$ sec.

Throughput $= \frac{5000}{0.55 + 0.001}$ → In stop & wait, we transmit 1 frame and 1 frame = 5000 bits

$= \frac{5000}{0.551}$

$= 8687.25$ bits/sec

$= 8.687$ Kbits/sec.

Pg 106

Ques-22

R.T.T = 80 ms.

B.W = 128 Kbps.

Frame = 32 bytes.

$K = 10^3$

milli $= 10^{-3}$

1 sec ⟶ 128×10^3

80 ms ⟶ $128 \times 10^3 \times 10^{-3} \times 80$

$= 128 \times 80$

Window size $= \frac{128 \times 80}{32 \times 8} = 40$

Pg-108

Qus 27

$BW = 4 Kbps$

$P.T = 20\ ms$

$\eta = 50\%$

$$\eta = \frac{T.T}{T.T + 2P.T}$$

$$\frac{1}{2} = \frac{T.T}{T.T + 2\times20}$$

$$\frac{1}{2} = \frac{F/4\times10^3}{F/4\times10^3 + 40\times10^{-3}}$$

(OR)

$P.T = 20\ ms$

$TT = 2\times PT$

$= 2\times 20\ ms = 40\ msec$

$$\frac{\text{Frame Size}}{B.W} = 40\ msec$$

$$\frac{K}{4\times10^3} = 40\times10^{-3}$$

$K = 160$ bits.

Qus 32

$N = 63$

Sequence no. = 62 in 1 window

Then, Range = 0 – 63.

Sequence no. used = 63

ie Window Size = 62.

Date:

→ FRAMING :

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

To detect the errors easily at the data-link layer transmitting a small size data is a better approach.

1000 → 1001 (1 bit change) ⇒ $^4C_1 = 4$

1000 → 1011 ⇒ $^4C_2 = 6$ (2 bit change.)

100 bit ⇒ $^{100}C_2$

N.L → 0110 11011011 0111 11

D.L → 0110 ~~1t~~ 1101 1t 1011 1t 01111

↳ size of data is small.

- Sender maintaining 8 bit space in-between ~~thinks~~ with aim that constant 8 bit space.
- But it is not possible, if noise modified the space then it is not detected by receiver.

→ If the spaces are maintained b/w the data and the same space is maintained through-out the journey, both sender and receiver are synchronized.

→ If noise has modified into the gap, the gap may decrease or increase, then both sender and receiver are out of synchronisation.

1) Character Count :

In this technique, DLL will add characters ~~in~~ count value.

NL : 463478532589 6

DLL : | 4 | 4 | 6 | 3 | 4 | 3 | 7 | 8 | 5 | 6 | 3 | 2 | 5 | 8 | 9 | 6 |

Frame 1   Frame 2   Frame 3

Date:

→ If frame1 is modified by noise then it is easily to protect data by error controls on small data.

Problem : In character count technique, if the count value is modified by noise, then both sender and receiver are out of synchronisation.

→ In this technique, the count value is added to indicate size of the frame.

→ If noise modifies data, then error detection schemes are there to protect the data.

2) CHARACTER STUFFING :

N.L ← ABCKP

D.LL → FLAG ABCKP FLAG → transmitted online → DLL → FLAG ABCKP FLAG → N.L

FLAG ↓ is 1 character ↓ It indicates data started

FLAG → indicates data is ended.

FLAG ... FLAG Removed at receiver side

Flag ⇒ 01111110 } flag pattern
↳ is of 1 character

eg:- NL ← ABCFLAGKP

DLL → FLAG $\underbrace{\text{ABCFLAGKP}}_{\text{data}}$ FLAG ⟶ DLL

DLL ↓ FLAG ABC FLAG KP FLAG ↑ here DLL understand ending of data

↓ send ABC only NLL ABC

So Now it send wrong data to NLL.

Flag patterns are used only for the synchronization of the data.

Date:

→ A character is stuffed when there is a ~~fes~~ data pattern that is equal to the flag pattern.

Now, In above eg:-,

NL ← ABCFLAGKP

DLL → FLAG ABC ESC FLAG KP FLAG
escape

D.LL Receiver
It will understand that ESC is stuffed character

↓

FLAG ABC ~~ESC~~ FLAG KP FLAG
↳ De-stuffed.

↓

NL:- ABC FLAGKP

→ Now, Receiver DLL will remove 1st flag and send ABC to N.L, when it encounter ESC then DLL will understand that next is also data, so it will transfer FLAGKP to NL and at last FLAG it remove this.

Ques- If the data is generated at N.L is KLMFLAGESCGP What is the data is transmitted in the D.LL by using character stuffing?

DLL → FLAG KLM ESC FLAG ESC ESCGP FLAG

Ques- If data is available at the receiver datalink layer is FLAG MOQ ESC ESC ESC FLAG ESC ESC PQR FLAG. Then what data is given to N.L after character de-stuffing.

N.L → MOQ ESC FLAG ESC PQR.

Problem : If more data & flag pattern matches then more character stuffing to apply which will result in large or increase size of data to be transmitted.

Date:

3) BIT STUFFING :

NL1 → ABFLAGC

↳ 01000001 01000010 01111110 01000011

↳ FLAG AB FLAG C FLAG

DLL

↳ 01111110 01000001 01000010 0111110 01000011

0

01111110

bit stuffed to distinguish data flag with Flag pattern.

- In character stuffing, we are stuffing 8 bits, but Now in bit stuffing, we are only stuffing 1 bits So, Here overload size is less.

→ Bit stuffing is a technique in which a zero '0' is stuffed to distinguish b/w the data and flag patterns.

Ques. If FLAG = 01110 and data that is transmitted is 011101110011110 Then calculate the data that is transmitted after bit stuffing.

01110 0111011100111110 01110 ✗

Logic : Stuff 0 after every 3 consecutive 1's.

01110 01110011101001110111 00 01110

becoz it may not be equal to flag pattern but that may be equal to some other pattern.
So, stuff 0 after every 3 consecutive 1's to distinguish all patterns.

Pg-109

Ques 33 Flag = 01111

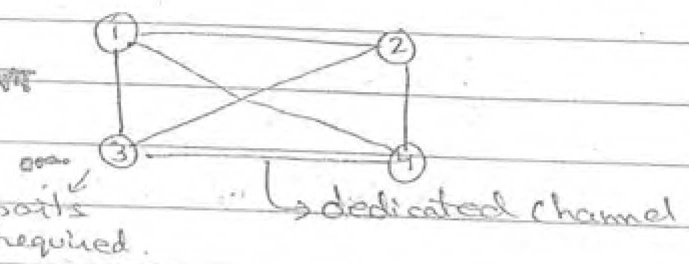
0111 011101101110011010 0111

(9-1-?)
Q26 Flag = 0111
0110101100

TOPOLOGIES

1) ~~STAR~~ MESH TOPOLOGY :

→ Every system is connected to every system by a dedicated link or dedicated channel.



→ If N devices are connected in Mesh topology, then the no. of ports that are required by each device is N-1.

→ If N devices are in mesh topology, then total no. of cables required are $\frac{N*(N-1)}{2}$
ie

for 4 devices, 6 cables.

ie $\frac{4\times(4-1)}{2} = 6$ cables.

for 100 devices; $\frac{100\times 99}{2} = 5000$ cables.

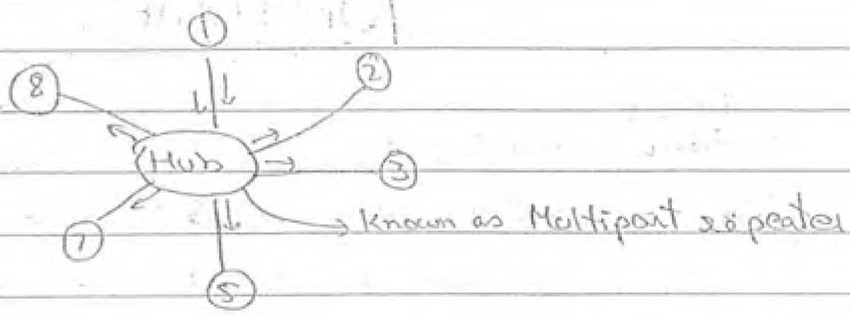
Problem : 1) Cost of cables are high
2) Cost of maintainence also high.
3) As no. of system ↑, cable requirement ↑ exponentially

→ So, it is only suitable for less no. of systems.

Date:

Advantage : 1) Security is high. } due to dedicated
2) Data is reliable } channel.

2) STAR TOPOLOGY :

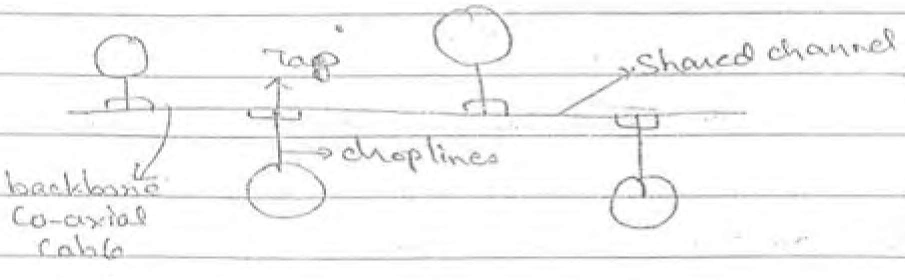


Hub can be → Passive (Hub is not intelligent)
So called broadcasting device.
→ Active (Hub is intelligent)

Advantage :
→ If N devices are connected in star topology, the no. of cables required are N,
→ Each device require 1 port only ie for hub

Disadvantage : 1) If hub fails, then whole system will crash.
→ Hub is replaced by switch ie intelligent device, in small companies.

3) BUS TOPOLOGY :

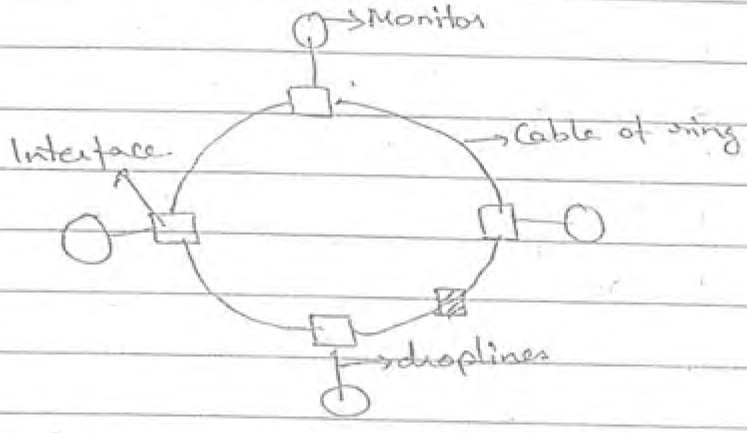


Problems : 1) Increases Collisions, to avoid this we apply some protocols. ie 1) Pure ALOHA
2) Slotted ALOHA
3) CSMA
4) CSMA(A)
} All in MAC Layer

Date:

→ In bus topology, N droplines and 1 backbone cable is required.

4) RING TOPOLOGY :



→ One system is called monitor which take responsibity to perform proper operation. It put token on ring also

→ When no station is transmitting data then token will be circulating in ring.

→ To transmit data system has to hold the token, and when transmission completed token is to be released for other systems.

→ Early token release is when if token is released just after transmitting the data.

→ ~~Late~~ Delayed token release is when token is released after receiving acknowlegment.

→ There is no possiblety of collisions, in general.

Hybrid topology is a combination of the above topologies

Date:

NETWORKING DEVICES

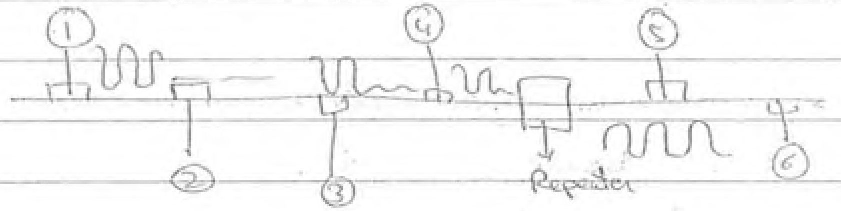
1) Repeater
2) Passive hub
3) Simple switch
4) Bridge
5) Router
6) BRouter
7) Gateway

1) REPEATER :

↳ Known as regenerative device.

⇓

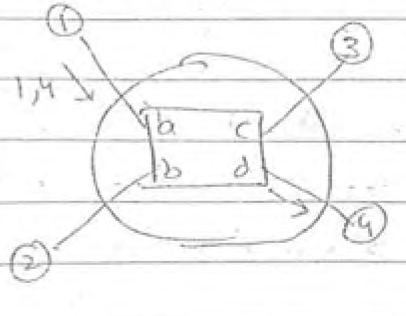
means, it while transferring strength of signal may decrease, then repeater maintains same original strength i.e regenerate actual strength.



→ Is a passive device.

→ Is used for digital signals and amplifier used for analog signals.

3) SIMPLE SWITCH :



lookup Table :

a	1
b	3
c	2
d	4

Date:

for forwarding the frames.

→ It maintains a lookup table, and connected to devices.

→ It looks up dest.ⁿ route by looking in lookup table. and forward that particular packet to dest.ⁿ.

4) BRIDGE :

→ Bridge is a LAN device and its operation is based on physical addressing system.

→ Operations of bridges are :

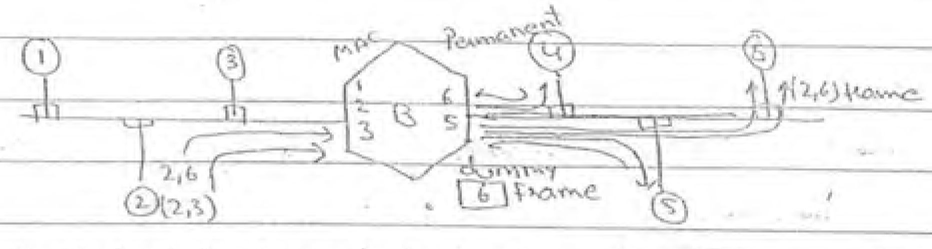
1) Filtering
2) Forwarding
3) Learning

→ It has bridge table and this table is prepared by learning.

→ If frame is generated, the source MAC address is placed permanent and dest.ⁿ MAC address is placed temporarily.

• When reply comes from any system, the dest.ⁿ MAC address is placed permanent and frame is forwarded

• If the reply doesn't come from any system, the bridge removes the temporary address and it will block the frame. This is known as Filtering.



Let (2,3) packet is send to bridge, bridge now broadcast a dummy packet to 4, 5, 6. When any reply comes back to bridge, then bridge will forward the frame to dest.ⁿ.

→ It works in a network environment i.e. within LAN but not in internet environment becoz its operation are based on MAC address.

Date:

5) BROUTER :

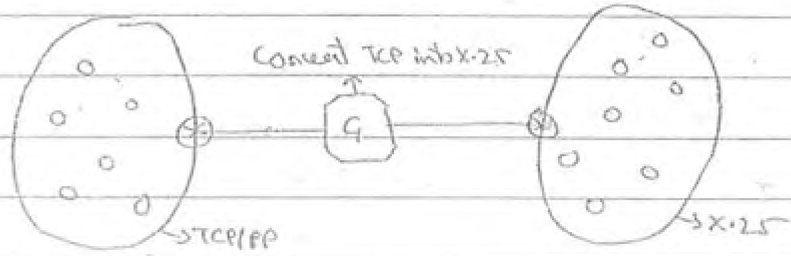
It is a device which is a combination of bridge and the router.

So, it performs operations of both router and bridge

6) GATEWAY :

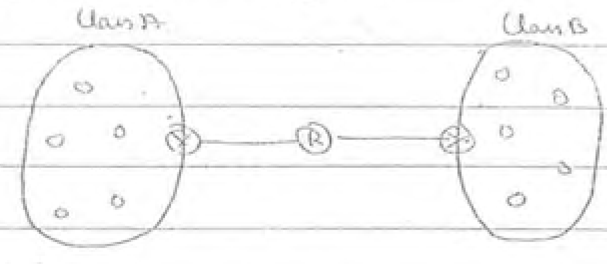
→ Gateway is a multi-protocol converter.

→ It is used to connect different types of networks ie one n/w can be TCP/IP and other network can be X.25 network



7) ROUTER :

→ Is a WAN device and its operation is based on logical addressing system.



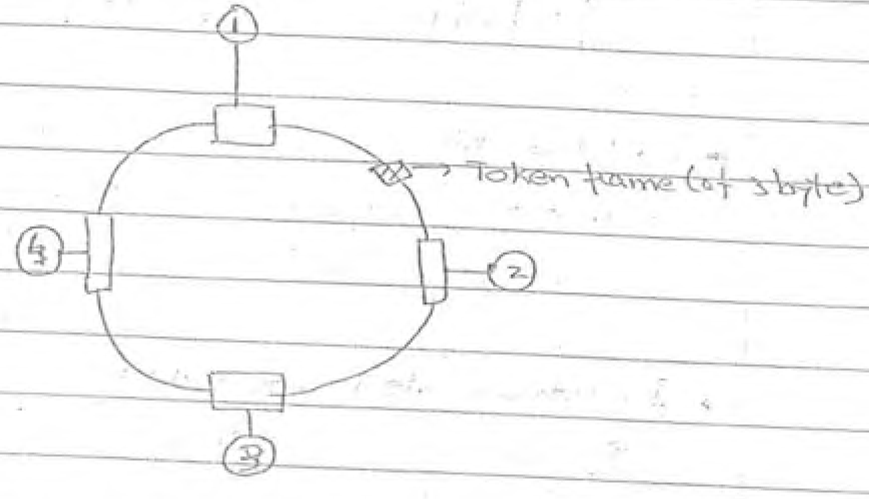
→ It can route packets b/w different classes but of same ~~network~~ similar network. ie if one n/w is X.25 and then other n/w also should be X.25.

→ Is a Sophisticated device.

→ Cost of router is in terms of lacs and crores of rupees.

→ It does not act as a multi-protocol converter ie if one n/w is TCP/IP & other is X.25, then it will not route the packet ie it will not convert packets

→ IEEE 802.5 (TOKEN RING) :



→ It understands differential Manchester encoding only.

⇓

If (1→0) then transition ie change otherwise no transition.

- In Manchester Encoding, 1 indicates high to low ie 1̅0 & 0 indicates low to high ie 0̲1

TOKEN FRAME :

← 3 byte. →

SD	AC	ED
1byte	1byte	1byte

SD : Starting Delimiter

J	K	0	J	K	0	0	0

→ J and K are replaced by differential manchester encoding scheme of both SD & ED fields.

Date:

ED : Ending Delimiter

J	K	1	J	K	1	I	E

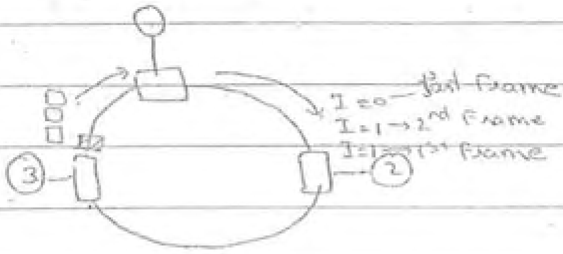
→ E : Error bits.

If E = 1 , modified
E = 0 , not modified
} Available for only SD and ED

→ I : Intermediate Frame Indicator

For all intermediate frames , I = 1

For last frame , I = 0



AC : Access Control

P	P	P	T	M	R	R	R

Priority (P P P) Reserve bits (R R R)

→ T : Token bit

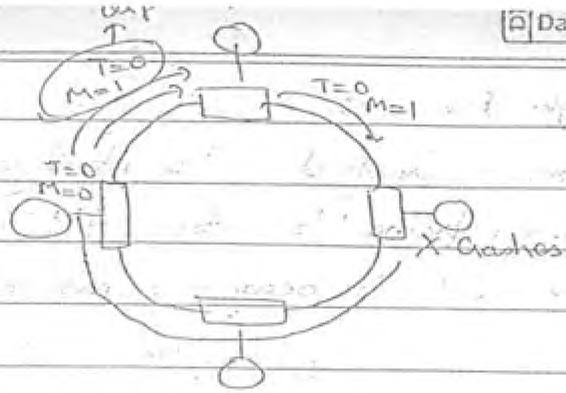
If T = 1 , then frame is token frame
T = 0 , then frame is Data frame

→ M : Monitor bit.

M = 0 , then new frame reached

M = 1 , then orphan frame reached

- For a data frame, when T = 0 & M = 0 is transmitted
- Once this frame reaches to monitor , monitor modifies , M = 1



- In the meanwhile, if dest.ⁿ system is not taking the data then this frame will again come to the monitor with T=0 & M=1
- Then, monitor indicates that it is a orphan frame and removes this frame from the ring becoz this is the responsibility of a monitor.
  Monitor inform this problem to source.

For token frame, T=1 and their is no significance for the M field. in the token frame becoz token is placed on ring by monitor only.

DATA FRAME :

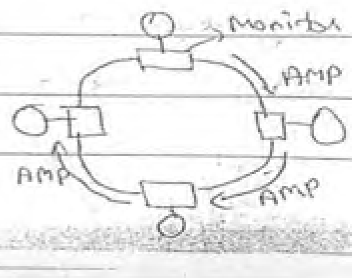
SD	AC	FC	DA	SA	DATA	CRC	ED.	FS
1B	1B	1B	6B	6B	>0	4B	1B	1B

SD, ED, AC } are also in token frame and are explained above.

FC : Frame Control.

Monitor has responsibility to inform other systems that it is a monitor.

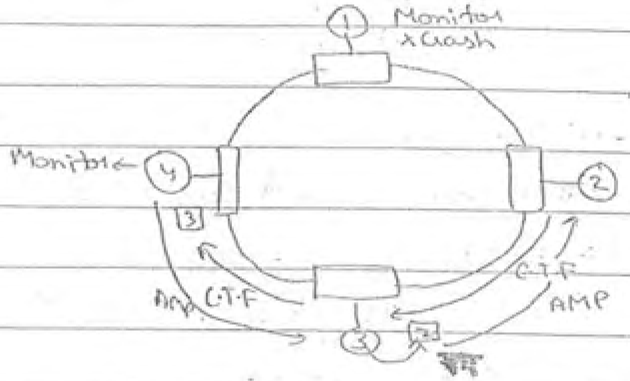
AMP Frame : Monitor sends AMP frame periodically many times to inform to others in the n/w that it is a monitor.



Date:

Claim Token Frame :

If monitor crashed, who identifies this, sends a claim token frame to inform the remaining stations that he want to become a monitor.

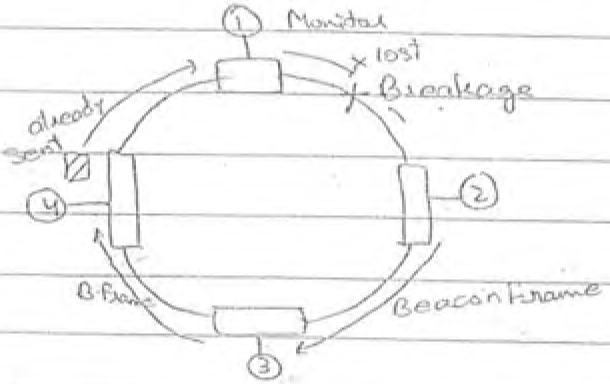


Suppose other higher priority station want to become monitor, then that will replace that ~~token~~ token frame by its no. and transmit to next station.

- It will work so, on.
- Finally, a station with highest priority becomes a monitor.

BEACON FRAME :

When there is a breakage in the ring, a station who identifies it, sends a beacon frame to alert all other stations in the ring that there is a breakage



Now station 3 is alert and will not send data before ring repaired. But meanwhile station 4 already sent data. Then ~~he~~ it will get to know that data is lost.

Date:

- During a breakage any system may transmit data if he has a token but this data will not reach to the dest.^{n} becoz of the breakage.
- When ring is repaired monitor sends the Purge frame to clean the ring
- Then monitors sends the AMP frame

STANDBY MONITOR FRAME :

Monitor sends a standby monitor frame to declare that a particular system will be monitor if present monitor crashes in future.

DAT FRAME :

Monitor sends a DAT frame to resolve MAC address conflict ie no two stations have same MAC address but there are some tools due to which one station get to know other stations MAC address and sometimes uses that MAC address So, DAT frame resolves this conflict.

- If there is a MAC address conflict in ring then monitor will not work.
- DAT Frame is forwarded before ring operation. by the monitor.

DA : Destination Address.

As it uses MAC address for communication, D.A is of 6 bytes becoz MAC is 48 bits.

SA : Source Address

Must mention source address ie from where data frame is send by.

CRC : Cyclic Redundancy Code

Is used for error control on data link layer.

FS : Frame Status

Status of a frame is always placed by receiver whether data received or not etc.

A	C	x	x	A	C	x	x

A → Address Recognized bit

C → Frame Copied bit

x → Don't Care

If A = 0 , C = 0 Dest.^{n} system is crashed

A = 1 , C = 0 Address recognized bt data not copied ie System is busy

A = 1 , C = 1 Data is received.

A = 0 , C = 1 Can't possible.

$$\text{RING LATENCY} = \text{Propagation Delay of ring} + \text{Interface Delay}$$

Ques- If the B.W of the ring is 4 Mbps. Calculate the transmission time of the token frame.

$$\text{Transmision time} = \frac{\text{Frame or Token frame}}{\text{Bandwidth}}$$

$$= \frac{3 \times 8 \text{ bits}}{4 \times 10^6 \text{ bits}}$$

$$= 6\ \mu sec$$

Ques- If BW = 10 Mbps , no. of stations in the ring are 500. Each station has 1 bit delay and length of the ring is 1km with velocity 2×10^8 m/sec. Calculate the ring latency.

$$P.T = \frac{1 \times 10^3}{2 \times 10^8} = 5 \times 10^{-6} \text{ m/sec}$$

$$= 5\ \mu Sec$$

1 Sec $\longrightarrow$ 10^7 bits

$\frac{1}{10^7}$ $\longleftarrow$ 1 bits

50 μsec $\longleftarrow$ 500 bits

Ring latency = 50 μsec + 5 μsec

= 55 μsec.

Qu- What is the longest frame that can be transmitted if the BW = 4 Mbps of ring and token holding time is 4 millisec.

1 sec $\longrightarrow$ 4×10^6 bits

4 millisec $\longrightarrow$ $4\times10^6 \times 4\times10^{-3}$

$= 16\times10^3$

= 16 Kbits.

Pg-112

Qu-9 - Token Size = 3 bytes

BW = 4 Mbps

Token holding Time = Ring latency.

So,

Token holding Time = $\frac{3\times8}{4\times10^6}$ sec.

length of ring = 46N

Propagation delay of ring = $\frac{46N}{2.3\times10^8}$

1 sec $\longrightarrow$ $10^6\times4$ bits

$\frac{1}{4\times10^6}$ sec $\longleftarrow$ 1 bit

$\frac{N+15}{4\times10^6}$ sec $\longleftarrow$ (N+15) bits

Interface delay

For proper operation monitor added extra bits, ∴ So, N+15 bit delay

$$\frac{24}{4\times10^6} = \frac{46N}{2.3\times10^8} + \frac{N+15}{4\times10^6}$$

$$6 = \frac{0.2N}{10^2} + \frac{N+15}{4}$$

N = 5

Date:

3) CSMA : → Channel is shared.

→ In CSMA station is ready then it first sense the channel.

→ Channel has 3 types of energy :

1) Energy low → channel idle
2) Energy normal
3) Energy abnormal.

→ In CSMA when a station is ready with the data it senses the channel.

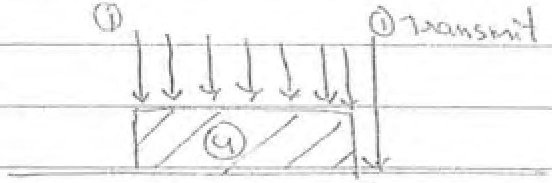
- If the channel is idle, that station can transmit immediately.

→ If the energy is normal or abnormal, the station has to wait a random amount of time.

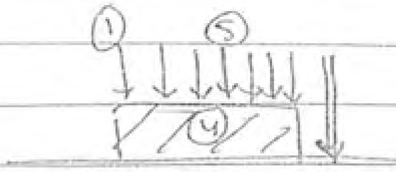
TYPES OF CSMA :

1) 1-PERSISTENT CSMA : In this, station continuously senses the channel if channel is busy until it got free channel.

- When it find channel idle, it transmits with probability one ie definitely it is transmitting.



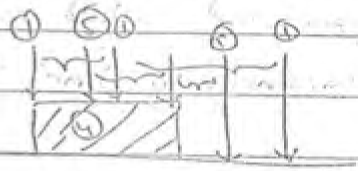
PROBLEM : If more than one station ~~senses~~ find the channel is idle, then these two stations may transmit immediately, possibly leads to collisions



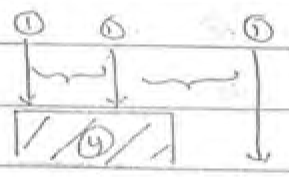
Date:

2) NON-PERSISTENT CSMA : If channel is busy, then station senses the channel once, then wait for some random amt. of time (and again senses the channel). So, here waiting time differs everytime and waiting time is different for different channel stations.

→ Finding the channel idleness, is different at different places. So the possibilities of collisions is less in case of non-persistent CSMA.



3) P-PERSISTENT CSMA :



→ In P-persistent CSMA, if the channel is idle a station may transmit with probablity "p" or it may not transmit with probablity "(1-p)"

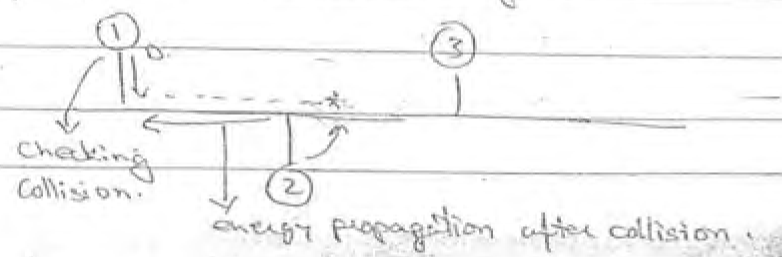
• So no. of collision reduces much more.

→ In above techniques we focus on issue that collision will not occur.

4) CSMA/CD :

→ It is used to provide remedy if collision occurs after transmission.

In this station is transmitting data ie data is in travelling position and parallely station is checking whether collision is occuring or not.



Date:

- In this vulnerable time depends on propagation time such that station can know collision occurence.

→ In CSMA/CD network any station has to transmit a minimum time of 2×P.T So that collision occuring at any point in the network can be detected.

Whereas in pure and slotted aloha Vulnerable time depends on transmission time so efficiency of them are very much less.

JAMMING SIGNAL : If a collision is detected, ~~at~~ any station that has not heard of collisions then a jamming signal is transmitted so that all stations will know about the collisions.

- If any station already send data then jamming signal will stop that data in the n/w.

Qus- If the distance b/w sender and receiver is 4km. velocity = 2×10^8 m/sec, B.W = 10 Mbps. Find the minimum frame size that can be transmitted on CSMA/CD Network

$$P.T = \frac{4 \times 10^3}{2 \times 10^8}$$

$$= 2 \times 10^{-5}$$

$$T.T = 2 \times PT$$

$$= 4 \times 10^{-5}$$

$$= .4 \mu s.$$

$$\frac{\text{Frame Size}}{10 \times 10^6} = 4 \times 10^{-5}$$

$$\text{Frame Size} = 40 \times 10^{-5} \times 10^6$$

$$= 400 \text{ bits}$$

→ IP PROTOCOL :

↳ Talking about n/w layer.

Packet → | Header | Data | ← Transport layer.

Header ↓ ~~is added to provide functionality of a n/w layer.~~

⇓

~~size = 65,535 bytes.~~

Header	Data
(20–60) bytes	

$\underbrace{\text{Header} \mid \text{Data}}_{65,535 \text{ bytes.}}$

IP HEADER :

Deals about Fragmentation ←

<table>
<tr><td>VER (4 bits)</td><td>HLEN (4 bits)</td><td colspan="2">Service Type (8 bits)</td><td colspan="4">TOTAL LENGTH (16 bits)</td></tr>
<tr><td colspan="3">IDENTIFICATION No. (16 BITS)</td><td colspan="2">Don't Care X</td><td>D F</td><td>M F</td><td>FRAGMENTATION OFFSET (13 bits)</td></tr>
<tr><td>TTL FIELDS 8 bits</td><td colspan="2">PROTOCOL FIELD (8 bits)</td><td colspan="5">HEADER CHECKSUM (16 BITS)</td></tr>
<tr><td colspan="8">SOURCE IP ADDRESS (32 bits)</td></tr>
<tr><td colspan="8">DESTⁿ IP ADDRESS (32 bits)</td></tr>
<tr><td colspan="8">OPTIONS AND PADDING (40 BYTES)</td></tr>
</table>

VERSION : It provides the version of IP ie IPV4 or IPV6

0100 → IPV4

0110 → IPV6

4 bits are used so that to give possibility in future.

- It going to identify the type of the packet ie IPV4, or IPV6.

Header length :
0000 }
0001 } Don't Care
⋮ }
0100 }
0101 } → header consists of 5 rows. min. header = 20
0110
⋮
1111 } → max. header is 60

→ Hlen is going to indicate the size of the header that is added to the payload. or data.

SERVICE TYPE : It tells what type of service packet is provided to the packet ie via a high BW or a low BW, a low delay or a high delay, maximum no. of hops and minimum no. of hops.

$\Downarrow$

Distance or cable b/w two successive routers.

→ It considers various metrices and these metrices can be delay.

TOTAL LENGTH : It indicates length of the packet. or size of the packet.

ie $\underbrace{11111111\ 11111111}_{\text{all are 1's.}} \Rightarrow 16$ bits

→ If total length bits are 0000000011111111, size of the packet is 255 bytes.

Ques- If total length bits 0000000011111111, if minimum header is added What is the payload that is added.

Packet = 255 bytes.

Packet = Header + Payload

255 = 20 + x

x = 235

* If Only total length → size of packet
If only Hlen → size of header.
If both are given → size of packet, payload and size of header.

Ques- Total length = 0000000010101010, HLEN = 1110 Calculate size of packet, size of header & size of payload.

(Size of packet)
||
Total length

~~Size of packet~~ = ~~2+16+64+8~~ 2+8+32+128

(~~Size of header~~) HLEN = 170

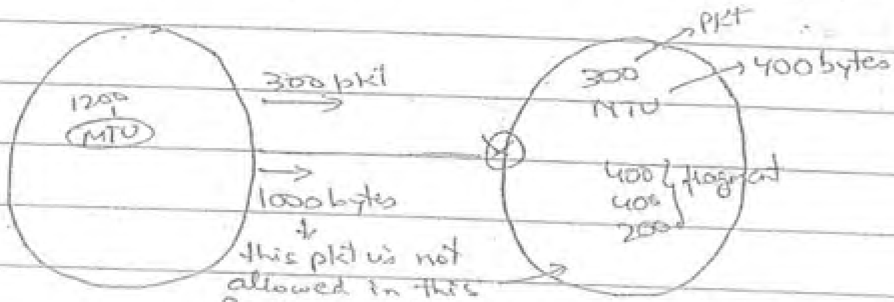
~~Size of header~~ = 8+4+2 = 14 × (4) = 56 bytes.
↳ bcoz each row is of 4 bytes.

Packet = Header + payload

170 = 56 + x

x = 114

MTU : Maximum Transferable Unit.



So it has to be ~~seg~~ fragmented by header.
fragments are : 400, 400, 200

- Fragments have to be recombined for further transmission. These fragments have to assign some no. ie known as identification ~~&~~ no. ie each fragment has same identification no.

IDENTIFICATION No. : Router provides identification no. ie
↓
16 bits.   ranging from (0 to   )

MF : (More Fragments) MF = 1 for all fragments, MF = 0 for last fragment.

- It indicates how many fragments have to be recombine to form as a packet.
- If MF = 1, it indicates that it is a intermediatory fragment.

Problem : If last fragment comes early than intermediate fragment.

DF : ~~Is used to resolve above problem~~. It indicates
↳ Don't fragment bit

whether it is a fragment or packet.

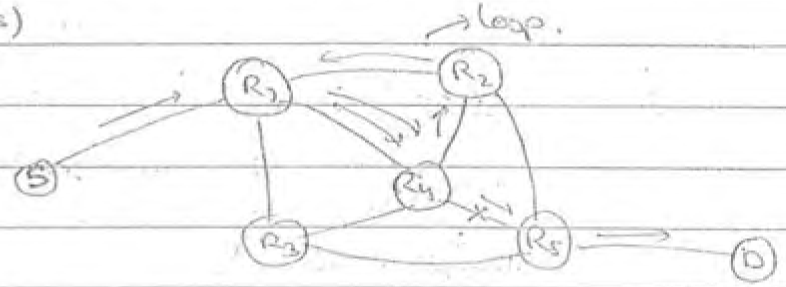
If DF = 1, it indicates it is a packet

If DF = 0, it indicates that it is a fragment.

Fragmentation Offset : Is used to solve above problem. It indicates the size of the fragment. Its size is (13 bits).

TTL FIELD : (Time-To-Live).

(8 bits)



Reason : All routers send

Due to breakage R4 is having wrong values and R2 also got wrong value and packet will travel in loop infinetly.

So we use TTL and its value is assigned by network. TTL value decreases while reaching router. Once TTL value becomes 0, IP packet has SIP & DIP so, ICMP protocol will be highlighted. and ~~take~~ ICMP take SIP from IP and report to sender about error.

ie ICMP reports error messages.

→ TTL field is going to indicate whether the packet is in the loop or not

→ Whenever there is a breakage of link the routers are filled with the wrong values so there may be a chance that pkt will be in the loop.

→ At one point of time, TTL becomes zero, then ICMP.

Date:

will take information from IP packet and informs to the Source that the packet is discarded.

PROTOCOL FIELD (8 bits) : It indicates type of upper layer protocol which to which this packet belongs to or which upper layer is using this packet. ie different no. are given to the different protocols in this IP header.

HEADER CHECKSUM (16 bits) : Provides error control for IP header only. Checksum for data is already present in above Transport layer. If header is not provided checksum then Router may route the packet to a ~~host~~ to different dest.^{n}.

→ Checksum is Only provided for header in n/w layer becoz checksum is already provided for the data from coming layer.

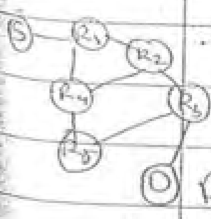
→ Since the header size is small, processing of the packets is done faster.

A SYSTEM CAN HAVE MORE THAN ONE IP ADDRESS BUT POSSIBLY ON DIFFERENT NETWORK

Qn- Does routing of the packets is always be done by the router or not.

Sol: No, Some other devices can also perform routing of packets like gateway.

→ Discovery packet can be send by source to know the path to reach the dest.^{n}. When source receives reply of the discovery packet it will get to know various path to reach dest.^{n}. So now sender can route the packets. This routing is called as Source routing.



Reply of discovery pkt : $\left[\begin{array}{l} R_1\ R_2\ R_3 \\ R_1\ R_4\ R_5\ R_3 \\ R_1\ R_2\ R_4\ R_5\ R_3 \end{array}\right\}$ → One path is decided by source.

Source Routing

Strict source — It visits only the path that is mentioned by source

loose source — It can visit other paths which sender not mentioned.

STRICT SOURCE ROUTING :

All the paths that are specified by the source must be visited, no other paths must be allowed.

LOOSE SOURCE ROUTING :

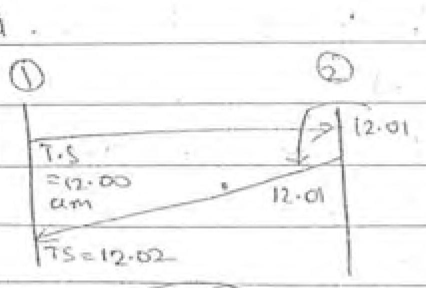
In loose source routing, along with the path specified by the source, some other paths can ~~be~~ also be visited.

RECORD ROUTE :

- It is used for debugging the network. ie it traces the n/w. which different router it has visited.
- It has all infor.^n about different routers that are visited in the n/w.

TIMESTAMP OPTION :

It is used to calculate the round trip time of the packet.

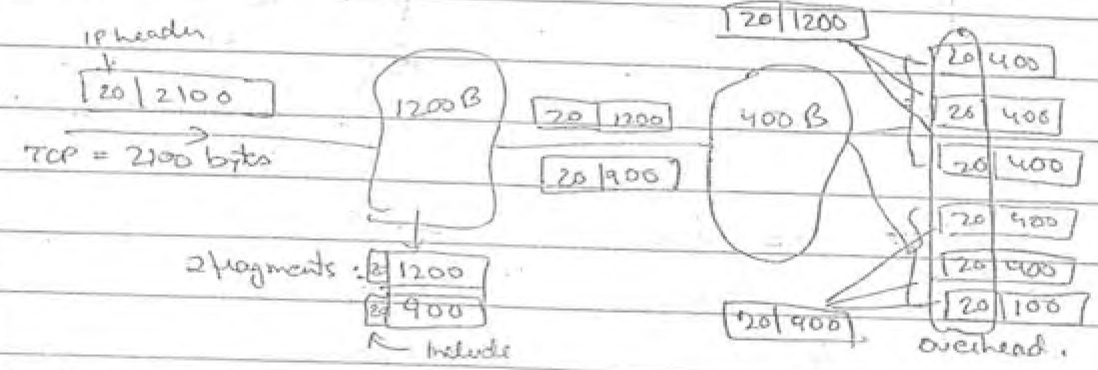


Difference (0.02) → is the R.T.T

ie it tells the time to put pkt on n/w and by what time ACK is received.

Ques 10 TCP message = 2100 bytes.

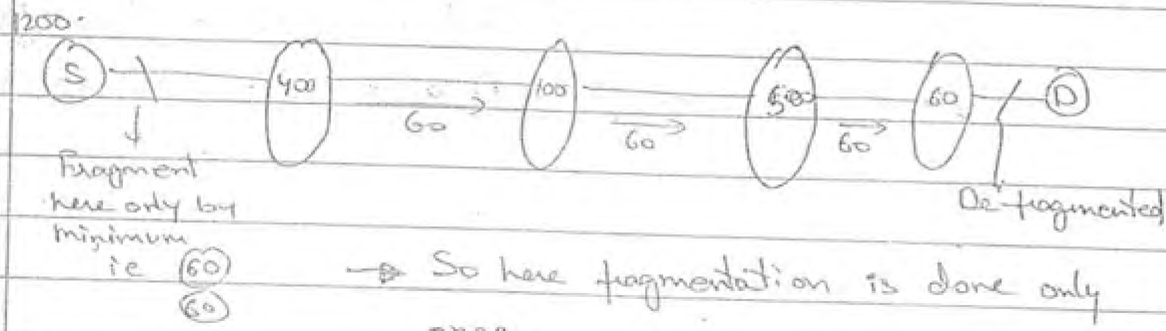
IP header = 20 bytes.



Total IP header overhead = 20×6

= 120 bytes.

In IPV6 :



→ So here fragmentation is done only once.

TCP HEADER :

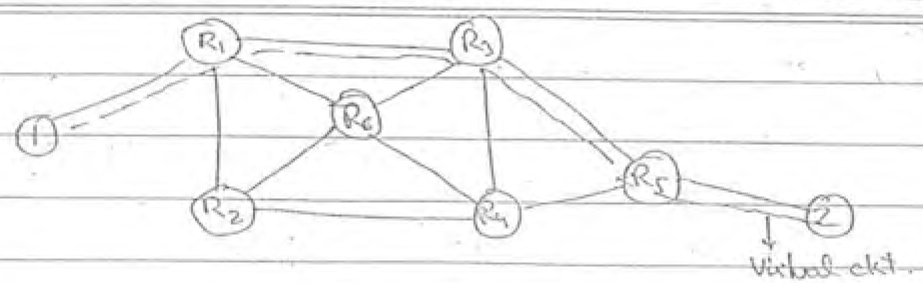
↳ Related to Transport layer

TL → | Header | Payload |

(20-60) B ; AL ; ← 65,535 Bytes →

AL → TL → TCP → Segment

- In TCP data is in Segments.
  ⇓
  Is a group of bytes
- In TCP, before sending data a virtual connection is established.
- After transmitting data connection is released.



→ Three steps in TCP are :

1) Connection establishment
2) Data Transmission
3) Connection released

CONTROL SEGMENTS : During connection establishment control segments are transmitted. Also, for connection released control segments are transmitted.

- For data transfer, Data Segments are transmitted.

→ In ~~n/w~~ Transport layer, port address is used to identify the services.

Each row is 4 bytes

SOURCE PORT (16 bit)						DESTINATION PORT (16 bit)
SEQUENCE NO. (32 bit)						
ACKNOWLEDGE NO. (32 bit)						
HLEN 4 bits	X X X	S Y N	A C K	F I N	U R G	WINDOW SIZE (16 bit)
CHECKSUM (16 bits)						URG POINTER (16 BITS)
OPTIONS & PADDING (40 BYTES)						

- In this layer, we add sequence no. for bytes that are in segment.

→ Sequence no. for 1^{st} bytes is randomly choosen ~~and~~ from range $(0 \text{ to } 2^{32}-1)$

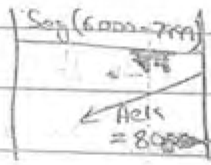
ie Random no. generator generates a ~~sec~~ ~~random~~ initial sequence no. ~~from~~ in range $(0 \text{ to } 2^{32}-1)$

eg:- If segment is of 1000 bytes and initial sequence no. is 5000, then 5000 is sequence no. for 1st byte of that segment.

→ The ack no. will always be the sequence no. of the next expected data. So it doesn't require any random no. generator.

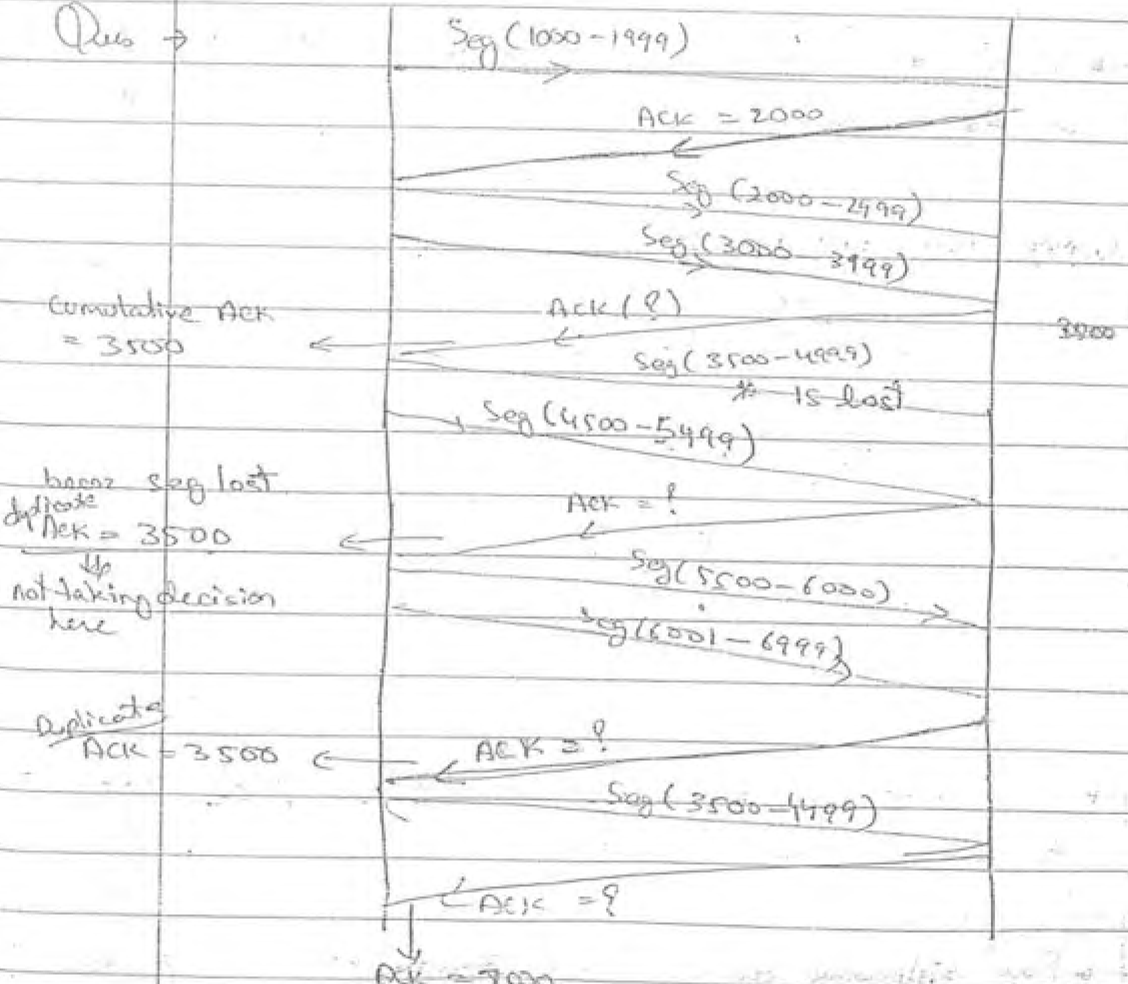
Qus. Segment is (6000 – 7999). Calculate the size of segment and ack no. of

Sol. Size of Segment = 2000 Bytes
Ack no. = 8000.

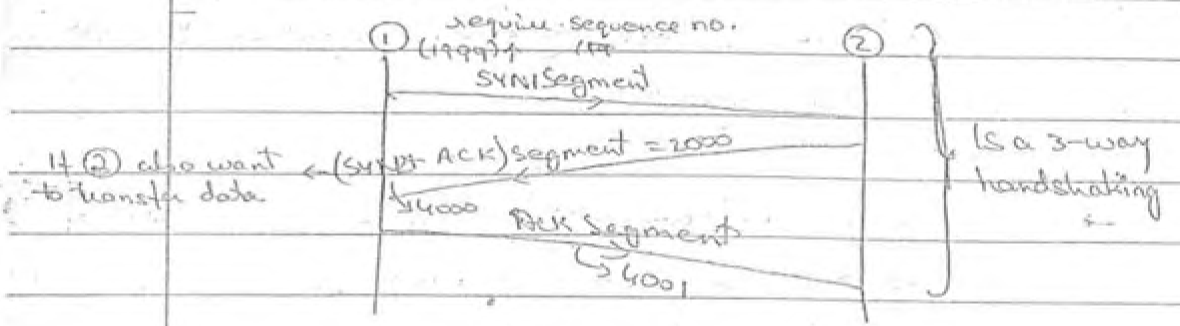


→ TCP Supports FULL DUPLEX OPERATION. It can accept out-of-order segments but always sends in-order ACK.

Ques →



Visual path establishment :



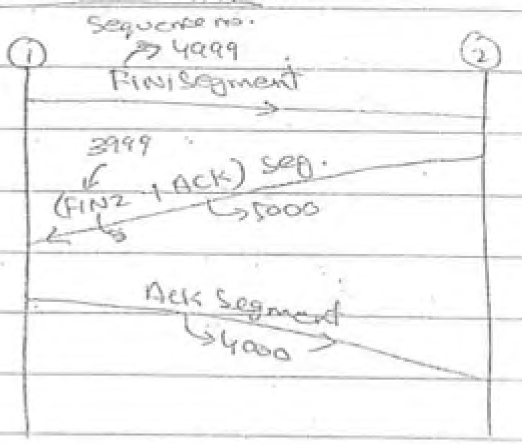
→ A SYN segment carries no data but consumes one sequence no.

→ If ACK = 1 , segment is ACK send by receiver to sender.

→ A system can accept request for connection and can parallely send request for connection in one single signal.

→ When 3-way handshakes are completed, then connection is established.

Connection Termination :



→ FIN. segment indicate data is transmitted so require to release the connection.

→ For releasing or termination, 3-way handshaking is required

RST SEGMENT :

It is transmitted at the point where data is lost. ie If the data is lost in the network an RST segment can be send for transmitting data from that point at which the data is lost.

- No need of establishing a new connection.
- It resets the connection.

RST = 1 , data lost so retransmit.

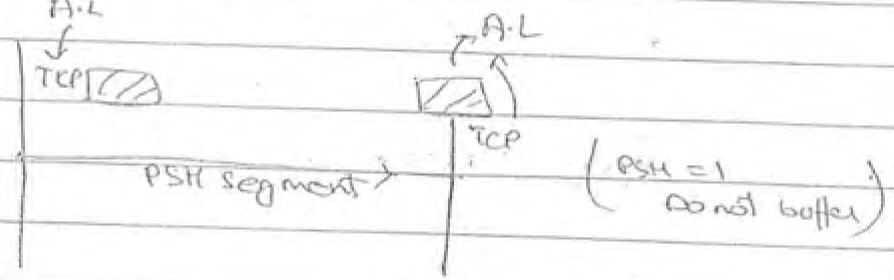
RST = 0 , No need to retransmit.

Interactive Applications, when input is given, then immediately output is send so there is no delay. It requires faster response. ie data should not be buffered.

PSH SEGMENT :

It does not buffer the data.

- For interactive applications, the response should be faster So TCP uses PSH segment.
- TCP sends PSH segment so that data will not be buffer at the receiver TCP, it will be given directly to the application layer.
- When sending the interactive data, resources are provided to the data such a way that the data will not be lost in the network.



URGENT DATA :

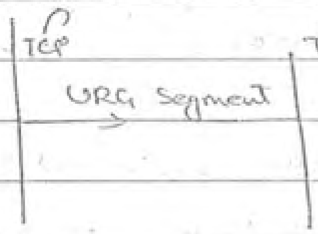
↳ It starts the processing ie it is required to start processing.

Eg:- Urgent data = 400

then before getting 400 processing will not start. So we require to send urgent data to first.

URGENT POINTER :

Urgent pointer holds the address of the urgent data.



URG = 1 → for Urgent data

URG = 0 → for non-urgent data.

HLEN :

It has 4 bits. and have don't care condition.

WINDOW SIZE :

→ It indicates sender about expecting data by receiver.

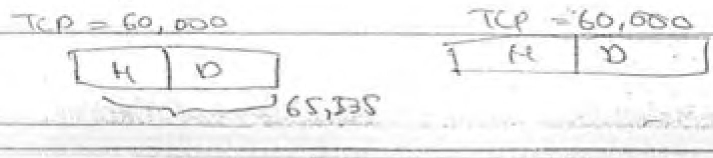
OPTIONS & PADDING :

By placing scaling factor in this field we can increase the size of segment.

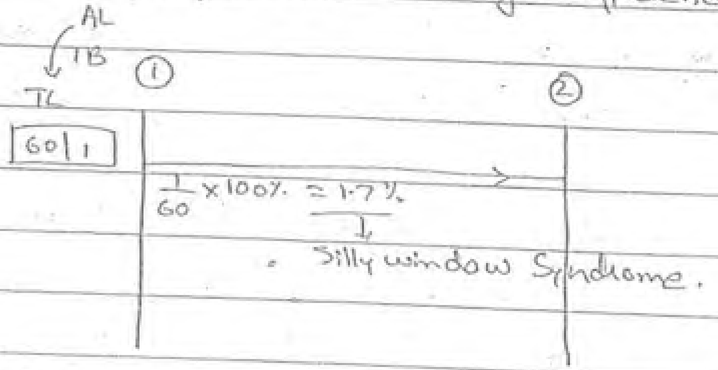
Seg → 65,535 bytes ✗ It increased then,

then, TCP = 1,20,0000 bytes.

Scaling factor = 2

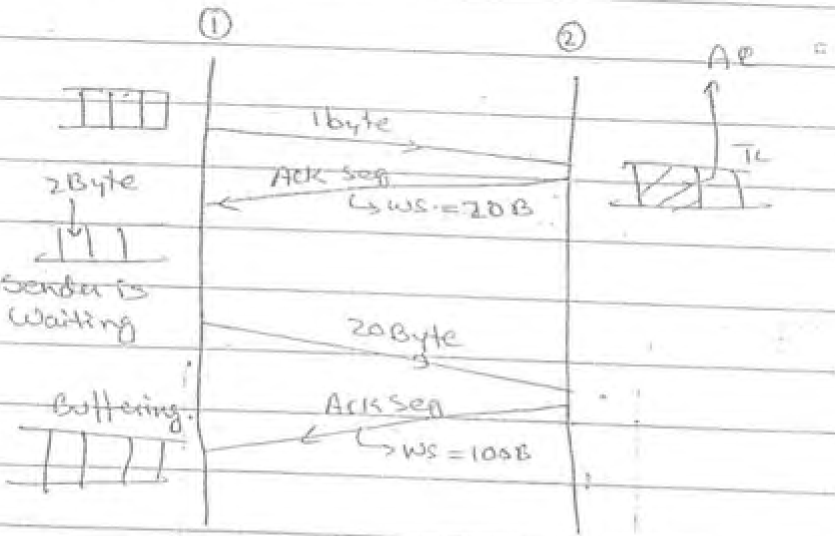


→ There are some applications, which if sends less or small data like 1 byte then we get efficiency very less.



SILLY WINDOW SYNDROME : When the A.L is generating small amount of data, then the efficiency at the transport layer will be small. This is known as Silly Window Syndrome.

To overcome this problem, Nagle solved this problem at sender side.



Initially, sender is sending small data to receiver.

→ Nagle suggested that if the appln is generating the data byte by byte, send the 1st byte as it is. and buffer the next coming data.

⇓

→ Once the ACK reaches to the sender, the buffer data is compared with the receivers window size.

⇓

→ If the buffer data is less than the window size then the sender waits for sometime.

⇓

→ During this process initially the efficiency may be low. but after sometimes efficiency increases.

→ Senders waiting time gives time to receiver to empty or to clean the buffer and increase the expecting data amount. ie window size is increasing.

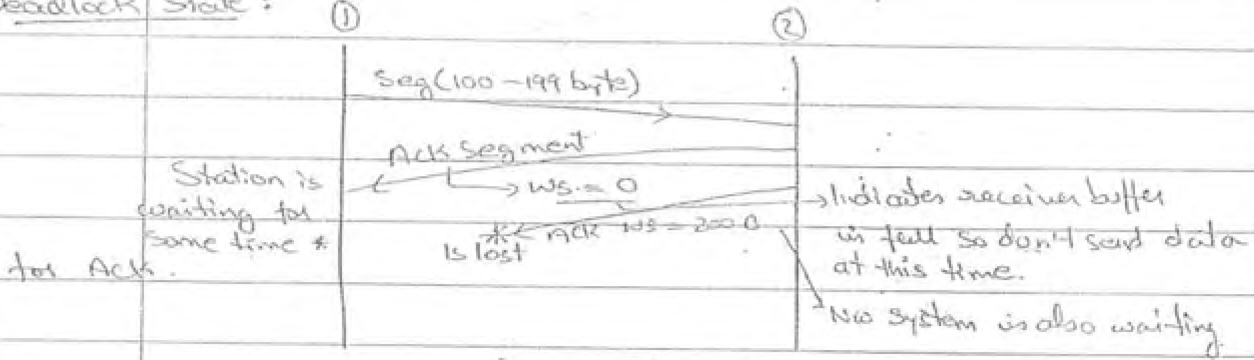
CLARKE SUGGESTION :

- Clarke Suggested that if the ACK is delayed then cleaning of or clearing of data will take place at the receiver side so that window size increases.

- Parallely buffering of the data will takes place at the sender side.

So efficiency will be increased fastly. So silly window syndrome problem can be solved.

Deadlock State :



→ If the advertised window size is zero, then the sender will be in a waiting state.

- The sender is waiting for the next ACK from the receiver.

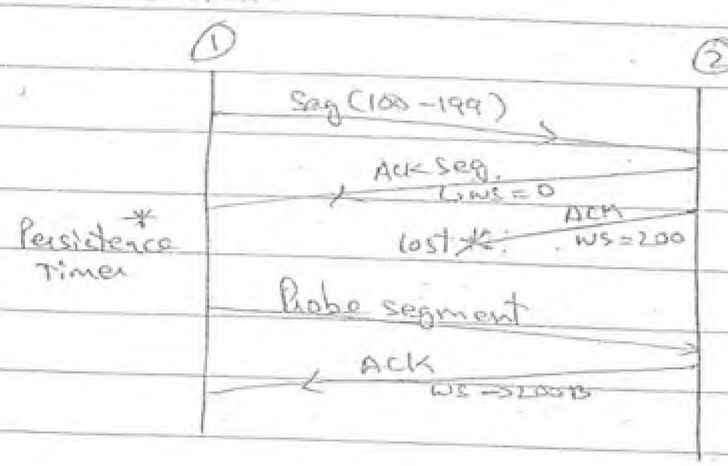
- If this ACK is lost both sender & receiver are in Deadlock.

- This problem can be solved by using a persistence timer.

Persistence Timer: This timer waits for fixed time for ACK. When ACK not received in that time then persistence timer will expire and so it is again set for waiting for to receive reply of control segment from receiver.

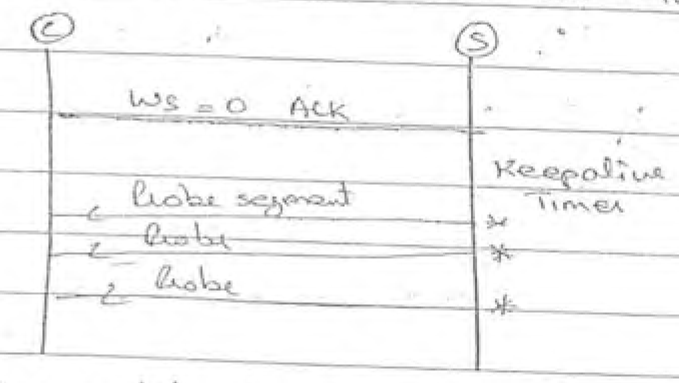
Persistence timer is used to overcome the deadlock between the systems that are transmitting segments.

- When persistence timer expires sender sends probe segment (ie control segment) to receiver.
- When receiver accepts probe segment, it will get to know that ACK is lost and it will retransmit the ACK.



KEEP ALIVE TIMER:

Is used at receiver when sender sends ACK with window size = 0



→ After transmitting a data for some time b/w client & the server, if the response is not coming from the client, the server does not know about the situation of the client.

⇓

→ After a period of time server will start a keep alive timer. ~~If~~

⇓

→ If the response doesn't come, the timer will expire and server is going to send the probe segments to the client.

⇓

→ Even if the response is not coming then server will voluntarily release the connection.

RTO TIMER :

↳ Retransmission After Time-Out

→ is given by Basic Algorithm.

in which,

I.R.T.T ← Initial RTT (Data Sent)

N.R.T.T ← New RTT (ACK)

α - is the scaling factor.

ERTT = $\alpha \times$ I.RTT + $(1-\alpha)$ NRTT
(estimated RTT)

RTO = $2 *$ E.R.T.T

Timers in D.L.L are static whereas the timers in Transport layer are dynamic becoz it deals with end to end connection.

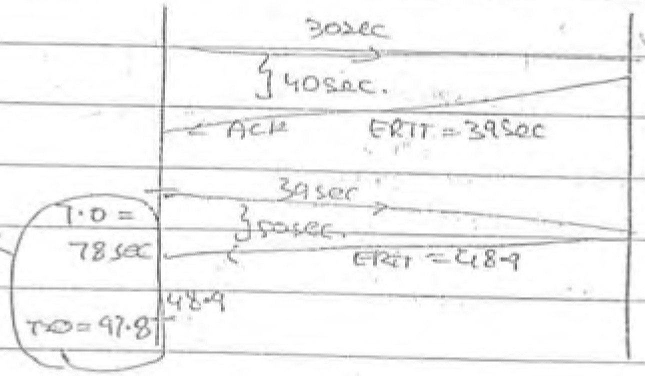
eg:-

I.R.T.T = 30 sec (expected or thinking time taken)

N.R.T.T = 40 sec (practically time taken)

$\alpha = 0.1$

Date:



Timer Changing So timer is dynamic.

→ $E.R.T.T = 0.1 \times 30 + (1-0.1)\,40$

$= 3 + 36$

$= 39\,sec.$] → It becomes new I.R.T.T

$RTO = 2 \times 39$

$= 78\,sec.$

→ $E.R.T.T = 0.1 \times 39 + (0.9)\,50$

$= 3.9 + 45$

$= 48.9$

$RTO =$ ~~87.8~~ ~~sec.~~ $97.8\,sec$

→ JACOBSON ALGORITHM :

$E.R.T.T = \alpha \times IRTT + (1-\alpha) \times N.R.T.T$

ie E.R.T.T is taken same as in basic algo.

→ It uses deviations.

$D_I = 5$ (Initial Deviation)

$D_N = 10 = |IRTT - NRTT|$ (New Deviation)

$D_E = \alpha \times D_I + (1-\alpha) \times D_N$

(estimated Deviation)

$D_E = 0.1 \times 5 + 0.9 \times 10$

$= 0.5 + 9$

$= 9.5$

$RTO = 4 \times D_E + E.R.T.T$

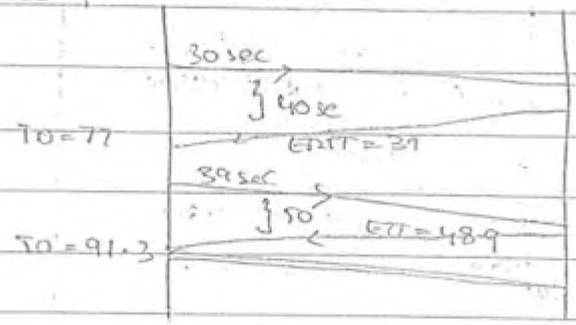
$= 4 \times 9.5 + 39$ → from previous ex.

$= 77\,Sec.$

IRTT = 30

NRTT = 40

In Jacobson,



→ $D_I = 9.5$

$D_N = |50-39| = 11$

$D_E = 0.1 \times 9.5 + (1-0.1)\times 11$

$= 0.95 + 9.9$

$= 10.85$

$RTO = 4 \times 10.85 + 48.9$

$= 91.3$.

→ In both algorithm E.R.T.T value doesnot change but time out value changes.

Conclusion: The time out value will be less in Jacobson algo compared to basic algorithm.

Qn- If IRTT = 10 sec, N.R.T.T = 19 sec, Calculate ERTT and RTO in basic algo. (Assume $\alpha = 0.1$)

$ERTT = 0.1 \times 10 + (1-0.1)19$

$= 1 + 0.9 \times 19$

$= 18.1$

$RTO = 2 \times 18.1$

$= 36.2$

Qn- Calculate the time out value in Jacobson algorithm if $D_I = 5$.

$D_N = 9$

$D_E = 0.1 \times 5 + (1-0.1)\times 9$

Date:

$= .5 + 8.1$

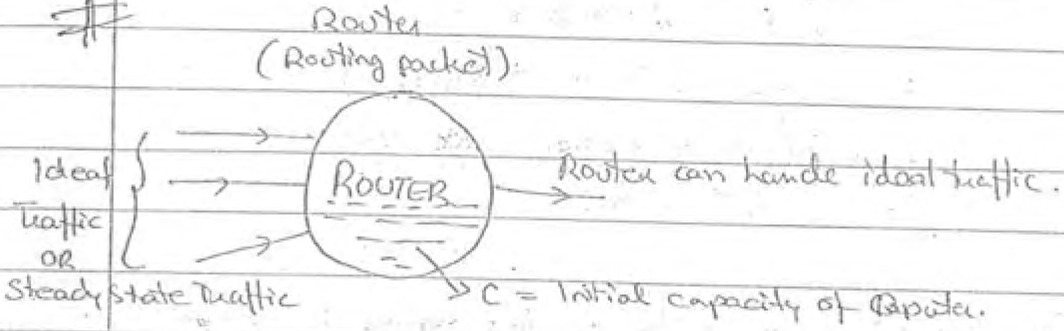
$= 8.6$

$\therefore RTO = 4 \times 8.6 + 18.1$

$= 34.4 + 18.1$

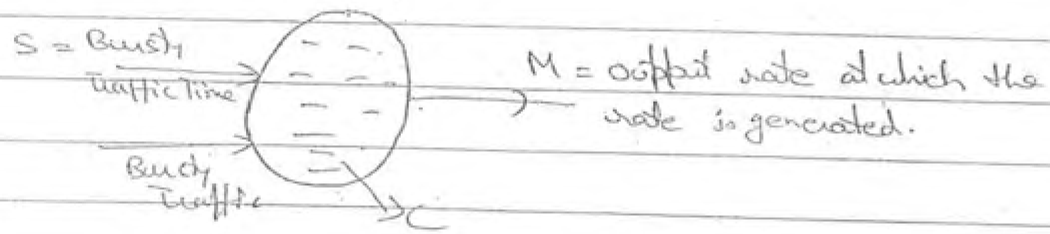
$= 52.5$ sec

#



BURSTY TRAFFIC : Sudden increase in steady state traffic is known as bursty traffic.

HOW TO HANDLE BURSTY TRAFFIC :



S = Time of bursty traffic

ρ = Token rate ie rate at which token are generated.
↳ helps to route.

→ If router is completely filled with packet ie capacity is full then token will not be generated. ie less no. of token were generated.

Date:

* If there is empty place in router, than more no. of token can be generated.

To handle this bursty traffic, condition is

$$C + \rho S = MS$$

where,

C : Capacity of that Router.

S : Time of bursty traffic.

ρ : Token generation rate

M : output rate

Qus. If the initial capacity of the router is 1Mbps and no. of tokens generated are 6 Mbps, output rate is maintained as 8 Mbps. Calculate the total time of the bursty traffic.

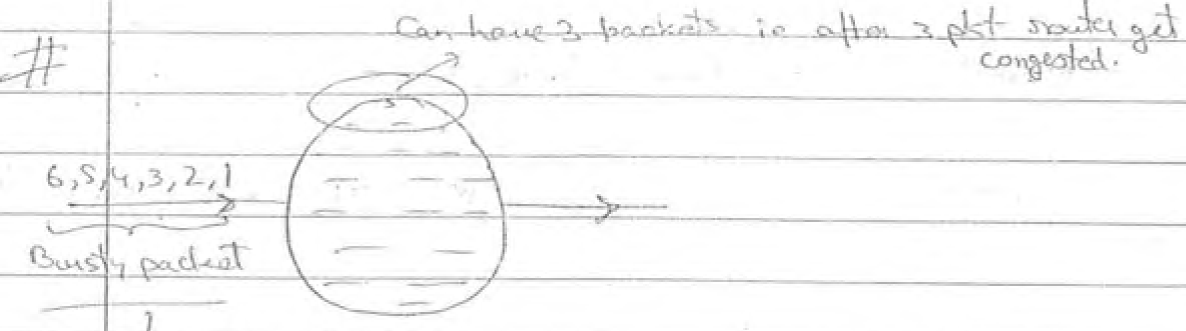
$$C + \rho S = MS$$

$$1 + 6 \times S = 8S$$

$$2S = 1$$

$$S = 0.5 \text{ sec}$$

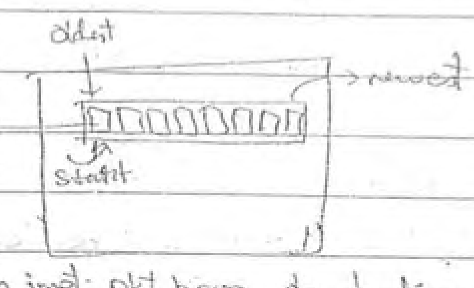
#



↳ packet selection depends on application which we use

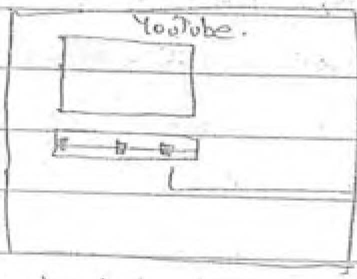
FTP   Multimedia.

We suppose FTP:



* Old packet is impt. pkt bcoz downloading starts from initial so, 1,2,3 are oldest & impt.

Suppose Multimedia :



new packets are most important.

→ So, for multimedia,

4, 5, 6 are most important packets. becos multimedia video can be watch or start from in-between also

LOAD SHEDDING :

When packets cannot be routed by the source, the router discards the packet.

→ Discarding of the packets is done based on the application. This is called load shedding.

→ Applications can be like :

1) FTP : Old pkts important, So old packets routed
2) Multimedia : New pkts are important, So new packets are routed.

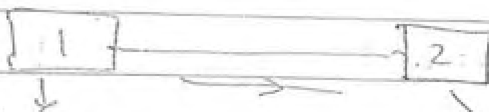
#

ie Data is transmitted serially

Serial Transmission Can be :

1) Synchronous
2) Asynchronous
3) Isochronous

SYNCHRONOUS S.T :



Send SYN characters with group of characters along with data only for synchronization.

It takes only data not accept SYN characters

Date:

Ques- a) In this, ~~8-bit~~ If 3-8 bit SYNC characters are included in 30-8 bit of information and the bit rate is 1200 bits/sec What is the rate at which data is taken by the destn.

Sol:

Sync + group of character = Information

1 sec ⟶ 1200 bits

27/1200 ⟵ 27 bits

3×8 ⇒ 24 sync bits included in 30 × 8 bit character

ie

24 sync bits ⟶ 240 Infor. bits.

1 sec ⟶ 1200 bits.

~~24×5 Sync bits ⟶ 240×5 Info.~~

120 Sync bits ⟶ 1200 bits.

Rate data is accepted = 1200 − 120

= 1080 bits/sec.

$= \frac{1080}{8}$

= 135 Characters/sec.

* In synchronous Serial transmission, the SYNC bits are removed at the receiver.

ASYNCHRONOUS S.T :

Sender		Receiver
Start bit + data + Parity + Stop bits	Send ⟶	Data + Start bit + Parity + Stop bits

Parity: for error detection

ie In this receiver will take start, stop & parity bit along with data.

REST OF INTERNET

ROUTING TABLE

Ques- In the problem, Calculate the rate at which data is accepted
is in asynchronous when $\boxed{1+8+1+1 = 12 \text{ bits}}$ per 1 character

bit rate = 1200 bits/sec

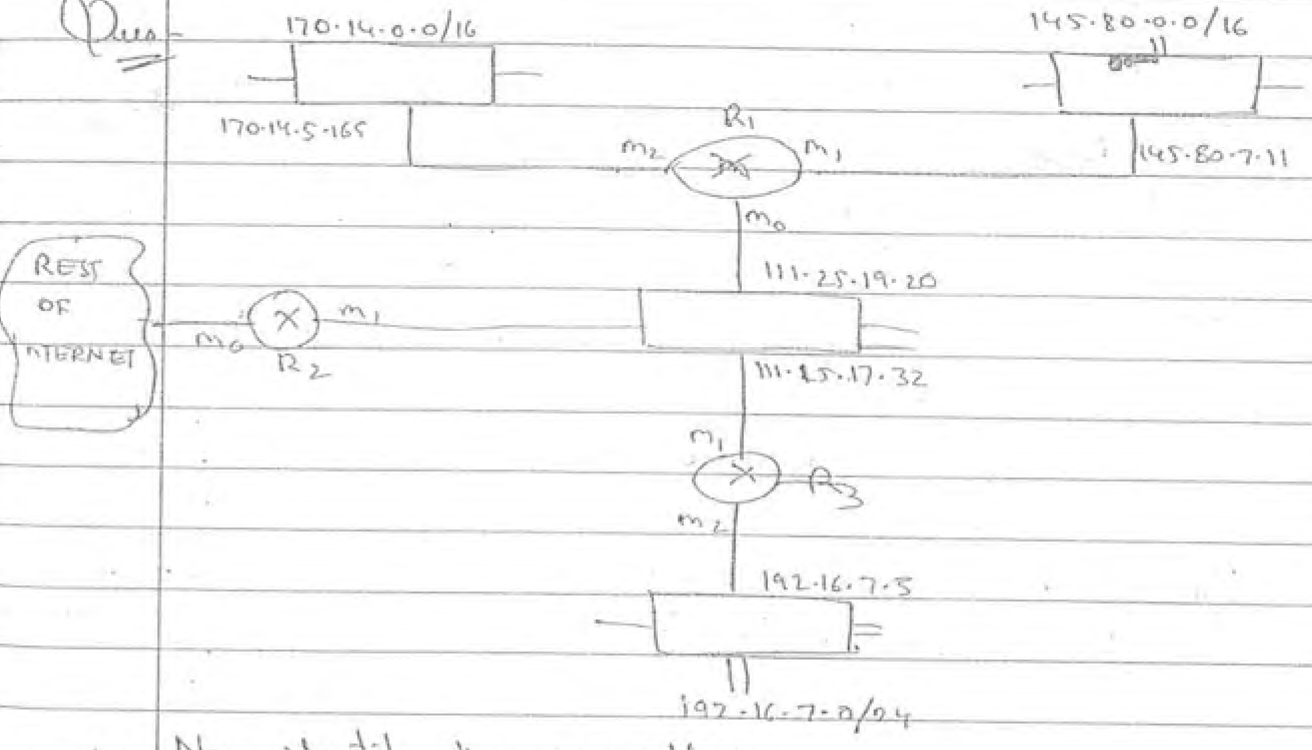
1 sec ⟶ 1200 bit

$\frac{1200}{12}$ = 100 characters/sec

ISOCHRONOUS S.T :

For transferring high bandwidth data Isochronous transfer is used.

Ques-



Sol :- Now identify the n/w address.

ROUTING TABLE

R1 : Class A

N/w Address	Nex-hop address	Interface
111.0.0.0	— — —	m0

Class B

N/w Address	Next hop.add	Interface
145.80.0.0	—	m1
170.14.0.0	—	m2

Class C

N/w Address	Next-hop add.	Interface
192.16.7.0	111.15.17.32	m0

Date:

N/w address	Next-hop	Interface
Default	111.30.31.18	m_0

Ques- Router R_1 receives a packet with destination address 167.24.160.5 Show how the packet is routed.

Class A :- 167.24.160.5

255.0.0.0

167.0.0.0 Doesn't match so not by m_1

Class B :

167.24.160.5

255.255.0.0

167.24.0.0 Doesn't match not by m_2

Default Class C :

167.24.160.5

255.255.255.0

167.24.160.0 Doesn't match.

So it will come from default route.

$m_0 \longrightarrow 111.30.31.18 \longrightarrow R_2$.

Ques- If R_1 receives a packet with 170.14.23.15 Via which Interface R's packet is Routed

170.14.23.15

255.255.0.0

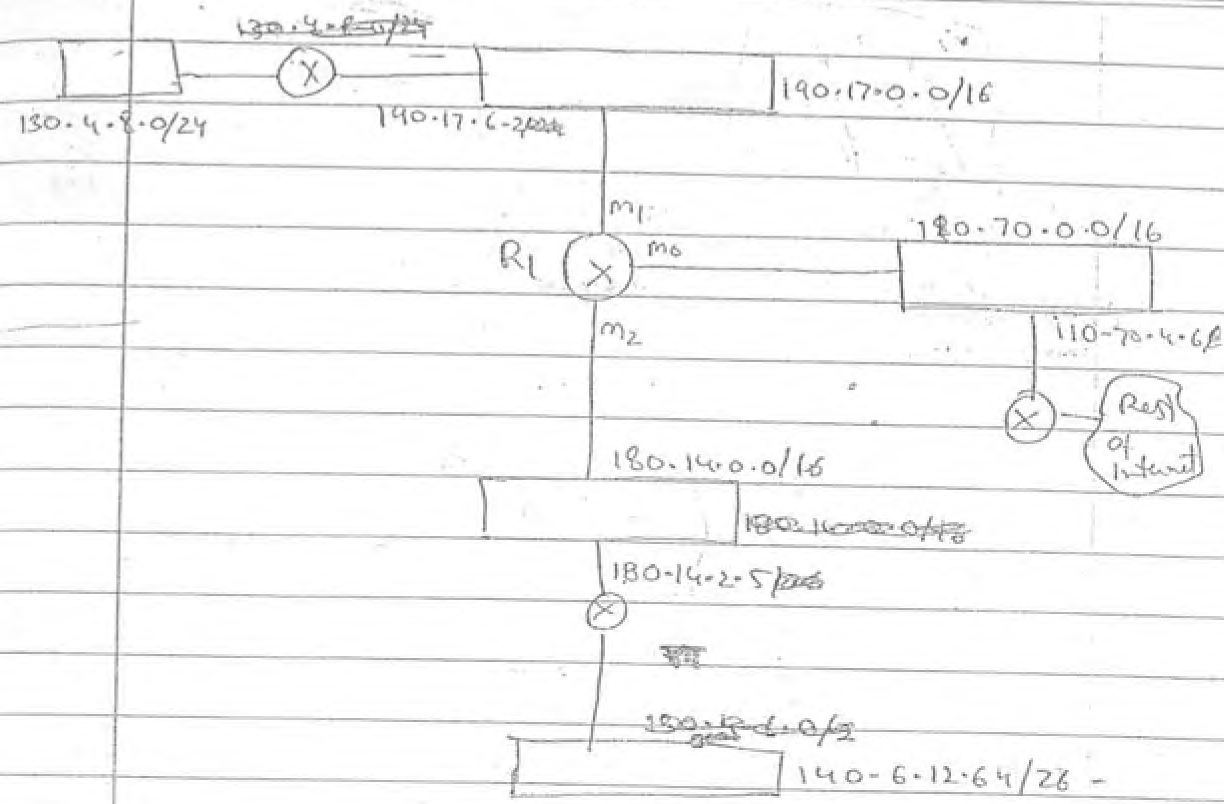
170.14.0.0 Matches with class B netid.

So, it is transferred via m_2 i/p interface

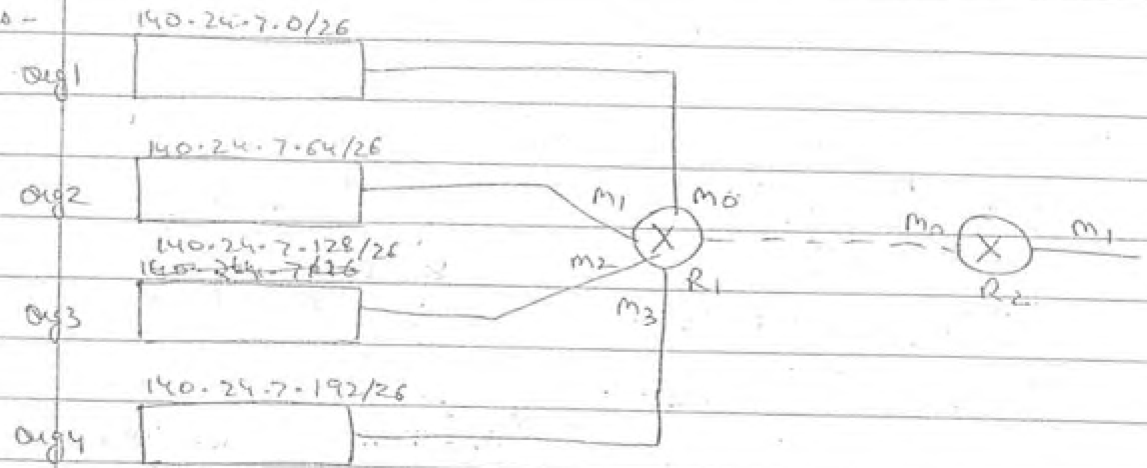
Ques- ROUTING TABLE :

MASK	N/w address	Next-hop	Interface
/26	140.6.12.64	180.14.2.5	m_2
/24	130.4.8.0	190.17.6.2	m_1
/16	110.70.0.0	- - -	m_0
/16	180.14.0.0	- - -	m_2
/16	190.17.0.0	- - -	m_1
Default	Default	110.70.4.6	m_0

→ Draw diagram from table given?



Ques -

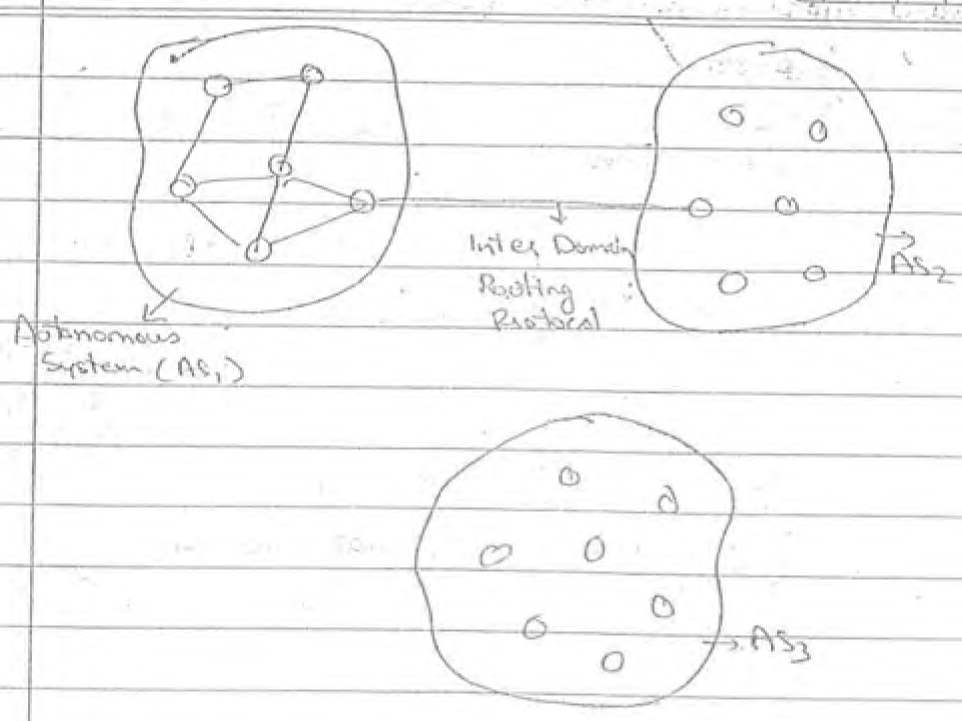


Write routing table for R_1?

Mask	N/w address	Next-hop add.	Interface
/26	140.24.7.192	-----	m3

Page No. ____
Date: 12/9/1

Routing Algorithms :-



- If the routing of the packet is done within the autonomous system or sub-domain, it is known as Intra Domain Routing Protocol.

eg:- RIP, OSPF

RIP → Routing Infor.ⁿ Protocol ⇓ It implement Distance vector Routing algo

OSPF → Open Shortest Path First. ⇓ Implement link State Routing algorithm

→ Are Dynamic algorithms

Routing Algo

Static Algo ⇓

- Doesn't take n/w load into consideration ie it behaves in same way always.
- (or) they don't adapt n/w load so also known as Non Adaptive algo.

eg: Flooding algo.

Dynamic Algo ⇓

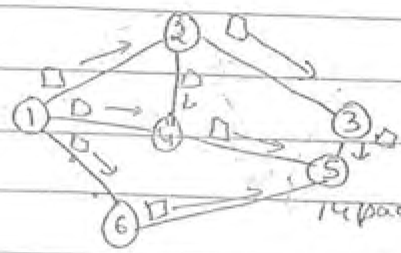
- Called as Adaptive algo bcoz they take n/w load into consideration.

12/9/11 Date:

1) FLOODING ALGO. :

It is a static algo. in which packet is routed in all direct^n except the path on which it is arrived.

⇒ 1 to 5



14 packets it got.

→ Metric is no. of hops

⇓

assume max. no. of hops = 3

3 - 1 - 2 - 3 - 5 ✓

2 - 1 - 4 - 5 ✓

2 - 1 - 6 - 5 ✓

3 - 1 - 2 - 4 - 5 ✓

Max. no. of hops = 3, then.

4 - 1 - 4 - 2 - 3 - 5 ✓ when max hop is 4. exactly.

14 - packets

Disadvantage: Redundant packets are created in the network.

→ It is used when we don't know the exact dest^n.

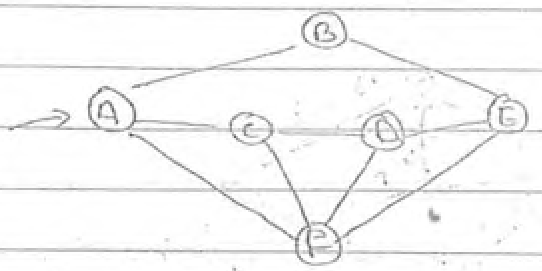
→ Flooding creates unnecessary packets which may leads to congestion at router in the n/w.

→ It is used in the military application.

It is called static becoz it is not taking care of other router and the links between the routers and even not care about buffers of other routers.

2) DISTANCE VECTOR ROUTING ALGO :

↳ It is a dynamic algorithm.



→ In distance vector routing, whenever a packet comes to a router, then the neighbouring routers will give their vector tables.

- Now a new vector table will be created for that node.

→ It is dynamic' becoz it takes help of next router for routing the packet.

Ques- Let B(1, 0, 1, 4, 3, 5)

C(2, 3, 0, 1, 2, 1)

F(1, 1, 4, 6, 1, 0)

The measure delays of B, C, F to A are (1, 2, 3)

Calculate the final vector table of A for a new packet.

A's table via B,

A	B	C	D	E	F
0	1	2	5	4	6

AA + AB = 1

AB + BC = 2

AB + BD = 1+4

AB + BE = 1+3

AB + BF = 1+5.

A's table via C,

A	B	C	D	E	F
0	5	2	3	4	3

~~CB~~ AC+CB

Date:

A's table via F

$$\begin{array}{cccccc} A & B & C & D & E & F \\ \end{array}$$
$$\left(\begin{array}{cccccc} 0 & 4 & 7 & 9 & 4 & 3 \end{array}\right)$$

→ Directly add A to C to C's table and add A to F to F's table directly.

So,

A's final table (0, 1, 2, 3, 4, 3)

(–, B, B,C ↓, C, {B,C,F}, {C,F})

any one can be chosen

Ques- If the packet come to A then it has to go F via which path it was choosen?

Via C or F to reach F.

Ques- If packet has come to A to reach to E via which path?

Via, B or C or F to reach E.

Ques- A new packet got to B and the vector table of E is (4, 5, 6, 8, 0, 9). The measured delays of E is 3 from B Calculate the final routing table for router B.

B's table via A

(1, 0, 3, 4, 5, 4)

B's table via E

(7, 0, 9, 11, 3, 12)

Final B's table:

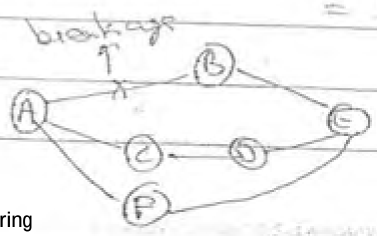
(1, 0, 3, 4, 3, 4)

(A, –, A, A, E, A).

Ques- If link b/w A to B is breakage, then Calculate the vector table for B?

B's final table = via E

= (7, 0, 9, 11, 3, 12)



Date:

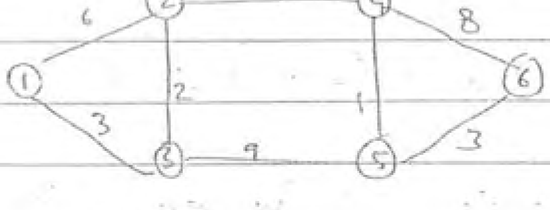
Suppose packet has to reach F from B. :
→ If link is not breaked than packet will go through A.
→ If breakage than packet will go via E ie
So due to breakage B got wrong vector table and it will route through wrong path.
ie B is completely depending on A's vector table.

Count to infinity problem :
Whenever there is a breakage, the adjacent routers are filled with the incorrect routing values.
- Later, remaining routers are also filled with the wrong values.
- Finally the n/w may collapse. This is known as Count to infinity problem.

Pg 120
Ques-10

Via A (8, 48, 22, 25, 29, 0, 32)
Via E (34, 37, 17, 30, 10, 0, 32)
D (32, 20, 42, 12, 26, 0, 34)
C (27, 30,
Final table,
(8, 20, 17, 12, 10, 0, 6)

Ques 25



R1		
R_2	5	R_3
R_3	3	—
R_4	12	3,2
R_5	12	3,5
R_6	15	3,5

Not utilized,
$R_1 \to R_2$ ✓
$R_4 \to R_5$
$R_4 \to R_6$ ✓

Date:

R_2	R_1	5	R_3	
	R_3	2	—	$R_1 \to R_2$ ✓
	R_4	7	—	$R_3 \to R_5$
	R_5	8	4,5	$R_4 \to R_6$ ✓
	R_6	11	4,5	

R_3	R_1	3	—	
	R_2	2	—	$R_1 \to R_2$ ✓
	R_4	9	2	~~$R_2 \to R_4$~~
	R_5	9	—	$R_4 \to R_5$
	R_6	18	5	$R_4 \to R_6$ ✓

R_4	R_1	12	2,3	
	R_2	7	—	$R_1 \to R_2$ ✓
	R_3	9	2	$R_3 \to R_5$
	R_5	1	—	$R_4 \to R_6$ ✓
	R_6	4	5	

R_5	R_1	12	3	
	R_2	8	4	$R_1 \to R_2$ ✓
	R_3	9	—	$R_4 \to R_6$ ✓
	R_4	1	—	$R_2 \to R_3$
	R_6	3	—	

R_6	R_1	15	5,3	$R_1 \to R_2$ ✓
	R_2	11	5,4	$R_2 \to R_3$
	R_3	12	5	$R_4 \to R_6$ ✓
	R_4	4	5	
	R_5	3	—	

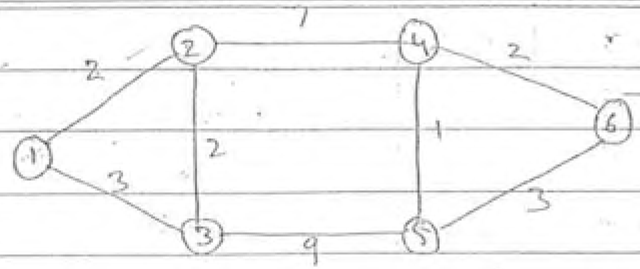
So,

$R_1 \leftrightarrow R_2$ & $R_4 \leftrightarrow R_6$ are not utilized.

So, 2 links are unutilized.

Pg-124

Qus 26



R_1

R_2	2	—
R_3	3	—
R_4	9	2
R_5	9	2,4
R_6	11	2,4

$R_2 \to R_3$
$R_4 \to R_5$
$R_5 \to R_6$

R_2

R_1	2	—
R_3	2	—
R_4	7	—
R_5	8	4
R_6	9	4

$R_1 \to R_3$
$R_3 \to R_5$
$R_5 \to R_6$

R_3

R_1	3	—
R_2	2	—
R_4	9	2
R_5	9	—
R_6	11	2,4

$R_1 \to R_2$
$R_4 \to R_5$
$R_5 \to R_6$

R_4

R_1	9	2
R_2	7	—
R_3	9	2
R_5	1	—
R_6	2	—

$R_5 \to R_6$
$R_1 \to R_3$

R_5

R_1	10	4,2
R_2	8	4
R_3	9	—
R_4	1	—
R_6	3	—

$R_4 \to R_6$
$R_3 \to R_2$

R_6	R_1	11	4,2
	R_2	9	4
	R_3	11	4,2
	R_4	2	—
	R_5	3	—

$R_1 \to R_3$

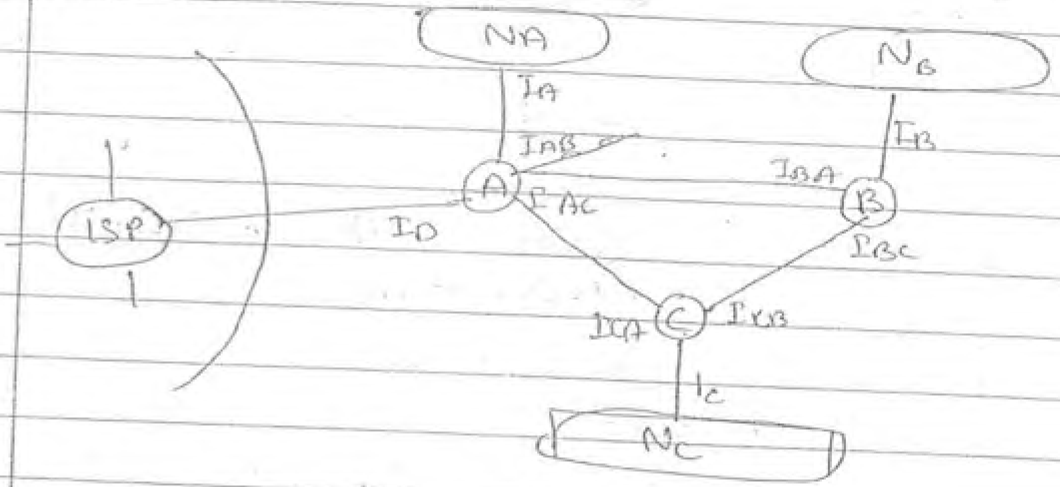
$R_4 \to R_5$

$R_3 \to R_5$

All edges are utilized.

So zero edges are unutilized ie (a)

Ques- A local network with 3 routers and 3 subnets is connected as shown in the figure. Assume that Class C range has been divide into four 64-IP subranges and assigned to subnets N_A, N_B and N_C. One sub-range has been left unused as spare. Connections b/w routers are done using 10.X.X.X IP numbers.



a) Which of the following is most likely incorrect:

1) In B : Default $\to I_{AB}$ ✗

2) In C : Default $\to I_{BC}$ ✗

3) In A : Default $\to I_{CA}$ ✗ but most likely this is crt.

4) In C : Default $\to I_{AC}$ ✗

5) In A : $N_B/26 \to I_{BA}$ ✓

Sol: Directly connecting is not default but indirect connection is default.

Date:

b) Which of the following is most likely incorrect ?

a) I_A = an IP from N_A Range

b) A host setting in N_C : GW = ISP, NM = 26 bits

c) a host setting in N_B : GW = I_B, NM = 26 bits

d) $I_D = I_{BC}$

e) NM of I_{AB} is 16 bits.

d) If from B pkt has to go to ISP then it can go through gateway I_{BC} or by I_D gateway.

c : GW = I_B,

NM = 26 bits ie hosts = 2^6 ∴ So from 64 IP address we can have 2^6 hosts.

b : GW = I_C but not ISP

NM = 26 bits

e : out of 2^{16} hosts or IP's we can have 16 hosts on network.

a : I_A is the IP address of N_A

c) Which of the following is most likely incorrect ?

a) in ISP : MyNet/24 → I_A

b) in B : N_C/27 → I_{CB}

c) in A : GW = I_{ISP}

d) I_{AB} : 10.0.0.1 and I_{BA} = 10.10.10.10

e) A host setting in N_C : NameServer = I_A

ISP directly can't see I_A. It know only I_D. So (a) is incorrect.

c : I_D can be replaced by ISP for other network to connect with N_A.

d : These are private IP's so we can use them

e : N_A and N_B can use N_A as name server like

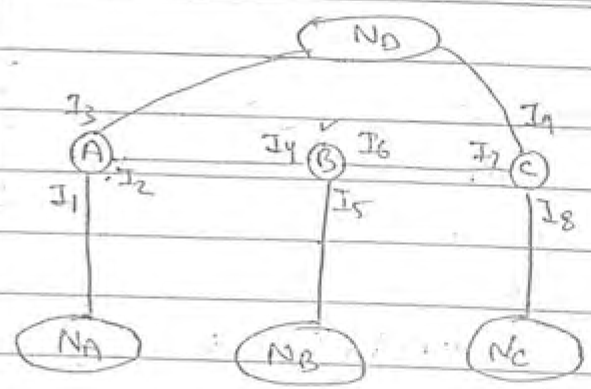
A @mail.com B @mail.com

Nameserver : mail (A) (B)

both can store their mail at name server.

Date:

Ques-



1) What are the routing table entries in B other than a possible default?

a) $N_B \to I_5$, $N_C \to I_6$, $N_A \to I_4$ ✗

b) $A \to I_2$, $C \to I_7$ ✗

c) $N_A \to I_2$, $N_C \to I_7$, $N_D \to I_7$ ✗

✓ d) $N_D \to I_3$, $N_A \to I_1$, $N_C \to I_8$

e) $N_D \to I_7$, $N_C \to I_8$, $N_A \to I_1$, $N_B \to I_5$ ✗

2) Which of the following is probably incorrect?

a) GW of a host in N_D is I_3

b) GW of a host in N_D is I_9

c) GW of a host in N_B is I_5

✓ d) I_3 and I_6 are same

e) Netmasks of $I_2 - I_4$ and $I_6 - I_7$ are same.

(becoz if these masks are not same then we can't connect them together in n/w.)

⇒ Gateway addresses can be different but their id's are same so netmasks must be same.

3) If N_A is the Sub-Class-C network which of the following is possible?

✓ a) $I_1 = 10.1.1.1$ ✓

✓ b) $I_1 = 220.140.141.4$ (more appropriate) ✓

c) Netmask of $N_A = 255.255.255.254$ ✗ becoz there will be no host.

d) A host IP in $N_A = 72.16.141.69$ ✗ → from Class A

e) A host in N_A has $GW = 190.16.128.1$?/✗ from Class B.

IEEE 802.3 :-

→ Datalink layer.
→ CSMA/CD support this particular LAN to overcome the collisions.
→ Called as ETHERNET FRAME

FRAME FORMAT :

Preamble	SFD	DA	SA	Type	Data	CRC
7B	1B	6B	6B	2B	↓ (46–1500)B	4B

$\underbrace{\text{7B} \quad \text{1B}}$ ~~not taken by receiver~~ side because its only for synchronization.

** In IEE 802.5 there is no specification for the payload.
But IEEE 802.3, the minimum payload is 46 Bytes and maximum payload is 1500 Bytes.

→ If the upper layer ie Network layer is generating data of 16 Bytes then 30 Bytes of padding are used to support minimum frame size.

→ Preamble and SFD added at sender but not taken by the receiver.
- It is added only for synchronization.
- To calculate the frame size we can't take those two fields.

→ Preamble (long bell) is 1010 1010 _ _ 10 & SFD (Short bell) is 10101011. When receiver get 2 consecutive 1's ie end of SFD is 11 then receiver get to know that next is dest^n address.

Purpose of Preamble & SFD :
- Used for synchronization of data b/w receiver & sender.

Why SFD also used ?

⇒ The last two bits of SFD indicates that after this the dest.ⁿ address is going to exist.

→ In CSMA/CD,

Minimum Frame Size = 64 Bytes.

↓ below this collision will not be detected by CSMA/CD.

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

$\boxed{x = 46}$ minimum becoz it supports CSMA/CD and minimum frame size of CSMA/CD is 64B.

→ Maximum 1500 Byte restriction becoz if one station has more data it will going to transmit continuously and even other stations have data then also they can't get chance to transmit data on channel. So it will then become unfair channel.

So, the maximum payload that can be given to IEEE 802.3 is 1500 Bytes. this restriction is to support giving a fair chance to all stations in the n/w.

Ques - If 10 base 2 coaxial cable is used. Calculate the minimum frame size that can be transmitted in CSMA/CD network. if the velocity of the data is 2×10^8 m/sec.

10 base 2 ⇒ 10 = BW ie 10 Mbps

→ baseband Signalling → on one channel you can transmit only one type of data at a time.

→ 200 = metres of the cables.

In broadband signalling, parallely we can transmit multiple type of data at a time ie video, audio, Text can be transmitted at a time.

$$T\cdot T = 2\times PT = \frac{2\times 200}{2\times10^8}$$

$$= 20\times10^{-7} = 2\,\mu sec$$

$\frac{\text{Frame size}}{BW} = 2\,\mu sec$

$x = 2\times10^{-6}\times10^{7}$

$= 2000$ bytes

If 10 base 5 cable is used in the above problem what will be the minimum frame size in CSMA/CD.

$$PT = \frac{500\,m}{2 \times 10^8}$$

$$= 25 \times 10^{-7}$$

$$= 2.5\ \mu sec.$$

$$TT = 2 \times 2.5$$

$$= 5\ \mu sec.$$

$$\frac{\text{Framsize}}{BW} = TT$$

$$x = 5\ \mu sec \times 10^7 \times 10^{-6}$$

$$= 50 \text{ bytes.}$$

Qns. The propagation time is 25.6 µsec & velocity of data is $2 \times 10^8\ msec^{-1}$. Calculate the length of the cable in CSMA/CD.

$$PT = \frac{x}{\text{Velocity}}$$

$$25.6\ \mu sec = \frac{x}{2 \times 10^8\ msec^{-1}}$$

$$x = 25.6 \times 2 \times 10^8 \times 10^{-6}$$

$$= 51.2 \times 10^2$$

$$= 5120 \text{ meters}$$

$$= 5.12 \text{ km}$$

Qn. Calculate the frame size if the PT = 25.6 µsec in IEEE 802.3 frame. BW = 10 Mbps

$$\frac{x}{10^7} = 2 \times 25.6 \times 10^{-6}$$

$$x = 51.2 \times 10^{-6} \times 10^7$$

$$= 51.2 \times 10$$

$$= 512 \text{ bits}$$

$$= 64 \text{ bytes}$$

Date:

Ques- To support maximum frame size in IEEE 802.3. Calculate the P.T that is required, if BW = 10 Mbps.

$$\cancel{\frac{1508}{10^7} = 2 \times P.T}$$

$$\cancel{PT = 2 \times 1508 \times 10^{-7}}$$

$$\cancel{= 6000 \times 10^{-7}}$$

$$\cancel{= 6 \times 10^{-4}}$$

$$\frac{\text{Frame Size}}{BW} = 2 \times P.T$$

Payload ← 1500 + 6 + 6 + 4 + 2 ← 1518

$$\frac{1518}{10\ Mbps} = 2 \times PT$$

$$PT = \frac{151.8\ \mu sec \times 8}{2}$$

$$= 151.8 \times 4$$

$$= 607.2\ \mu sec$$

Ques- If the frame size is 60 bytes, BW = 10 Mbps, velocity is $2 \times 10^8\ m sec^{-1}$. Calculate the length of the cable in IEEE 802.3.

$$\frac{60 \times 8}{10^7} = 2 \times \frac{x}{2 \times 10^8}$$

$$60 \times 8 = 2 \frac{x}{10}$$

$$x = 4800 \text{ metres.}$$

$$= 4.8\ Km$$

→ ARP PROTOCOL :-

↳ Address Resolution protocol.

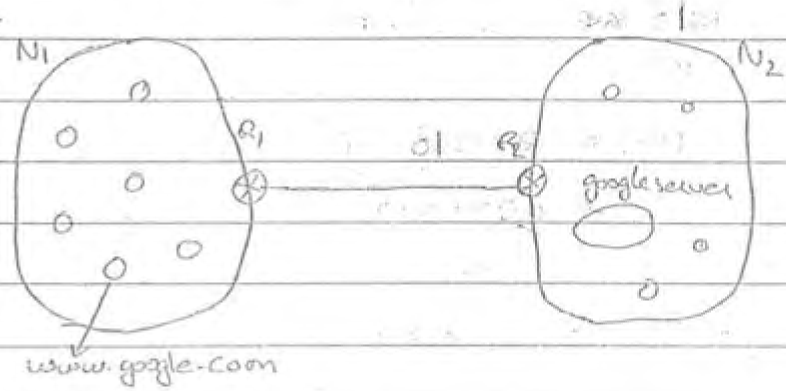
↳ It can be used outside the n/w as well as in inside network.

→ ARP request is broadcast and ARP reply is unicast.

Date: 13/9/11

→ When IP address is given to ARP protocol, MAC address can be resolved.

example:-



Where ARP is used and how :-

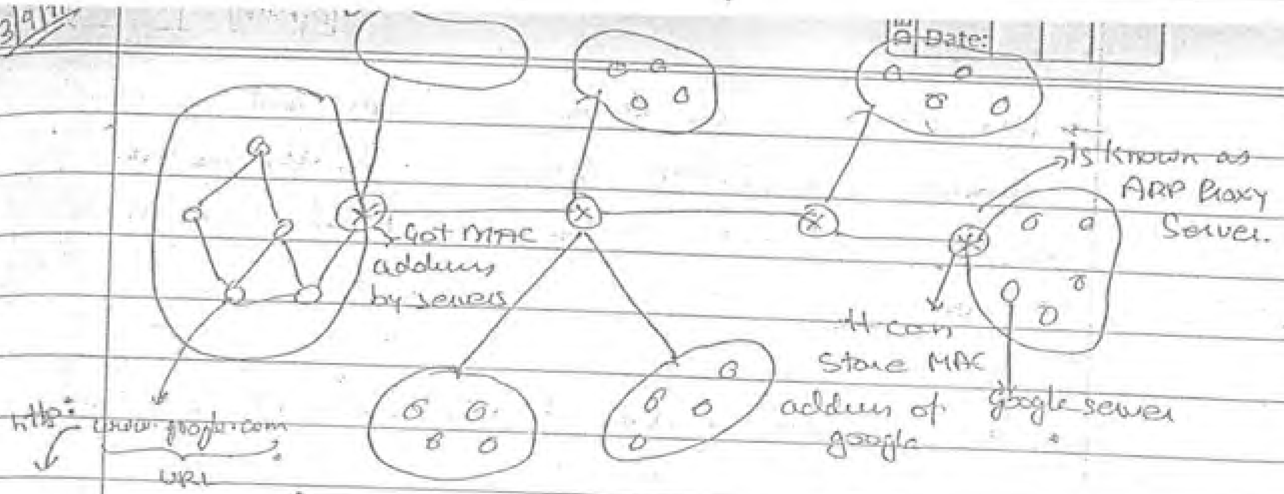
- Suppose router of N_1 network got request for www.google.com.
- It send IP packet to R_1 router giving MAC address of sender, private IP of sender and public IP of destⁿ.
  R_1 will convert private IP to public IP and send the packet to R_2 by checking masks.
- R_2 don't know MAC address of destⁿ; So here ARP protocol get highlighted.
- ARP has sender MAC address. So to know destination MAC address it will broadcast ~~a~~ packet to ARP packet to all.
- Google server will reply back to ARP with its MAC address.
- Now R_2 will send data packet to google server by using its MAC address.

ARP PACKET :

HARDWARE TYPE 16bit		PROTOCOL TYPE 16bit
HARDWARE LENGTH 8bit	PROTOCOL LENGTH 8bit	OPERATION REQUEST (OR) REPLY
SENDER H/W ADDRESS (6B)		
SENDER PROTOCOL ADDRESS (4B)		
TARGET H/W ADDRESS		
TARGET PROTOCOL ADDRESS		

DNS server gives → TARGET PROTOCOL ADDRESS

13/9/17 Date:

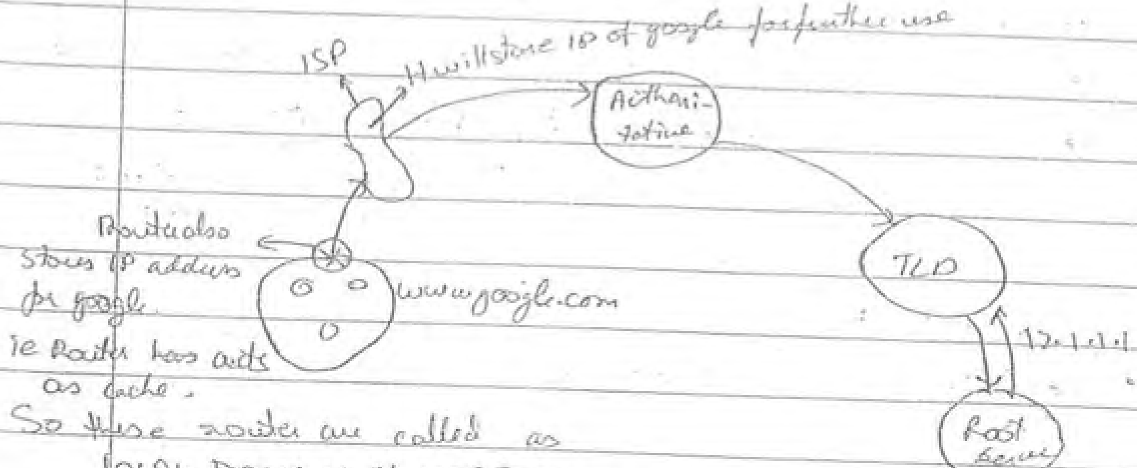


→ Though out the world we have 13 root servers. below root servers we have Top level domain servers (1000).

(Gives IP address of websites) → Root server
↓
(com, org, edu) → Top level domain servers
↓
(Info about all .com servers) → Authoritative servers
↓
~~Local Domain Name servers~~

} All are DNS Servers

→ DNS servers are the servers which is going to hold the IP addresses of public host.



So these router are called as LOCAL DOMAIN NAME SERVER.

How much time IP address of rarely accessed websites will be remain at ISP & Local Domain Servers.

→ Local domain servers will acts as a PROXY Servers for the authoritative under root server and TLD servers.

→ It will remain until TLD timer expires.

→ MAC addresses are stored in servers and server will provide MAC addresses of that n/w to the routers.
So, now that n/w router has info.^{n} about sender IP address, sender MAC address and Destination IP address.

→ While requesting target h/w address, ARP places all zero's in that field.

→ A router can do many functionalities.

HARDWARE TYPE :

- This is a 16-bit field defining the type of the n/w on which the ARP is running
- ARP can be used on any physical network.
- It indicates on which LAN ARP is running.
- Each LAN has been assigned an integer based on its type.
  eg:- Ethernet is given Type 1

PROTOCOL TYPE :

- Indicates who is requesting ARP like UDP, TCP or etc.
- The value of the field for IPv4 is $(0800)_{16}$
  each no. has nibble ie 4bits.

HARDWARE LENGTH :

- It indicates which MAC address is requested or using.
- Defines length of the physical address in bytes.

PROTOCOL LENGTH :

- It indicates which length of protocol is using.
- Is an 8 bit field defining the length of logic address in bytes.

Date:

OPERATION :

- This is a 16-bit field defining the type of the ARP packet.

→ A proxy ARP is an ARP that acts on behalf of a set of hosts.

- Whenever a router running a proxy ARP, it receives a ARP request looking for the MAC address of one of the host.
  - The router sends an ARP reply, announcing its own hardware address.

→ ICMP :-

- Related to N/w layer.

Format :

← 8 bit →	← 8 bit →	← 16 bits →
TYPE	CODE	CHECKSUM
REST OF HEADER		
DATA SECTION		

ERROR REPORTING MESSAGES :

	TYPE	MESSAGE
	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter Problem
	5	Redirection
Query Msgs. [	13, 14	Timestamp request or reply.

* IP is a connection-less, ~~less~~ best effort delivery protocol

TYPE :

Indicates type of message that is send by ICMP.

Date:

CODE :

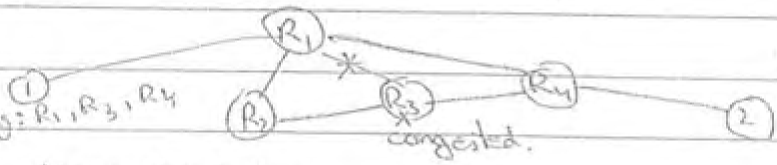
Tells the reason behind the message why data is not reachable.

DESTINATION UNREACHABLE :

ICMP will generate this message to the source when ;

1) the n/w is unreachable.
2) Host is unreachable
3) Protocol is unreachable

Strict routing : R_1, R_3, R_4



Now ICMP has,

Type : dest.ⁿ unreachable

Data section : R_3 congested.

or Data Section : link breakage

SOURCE QUENCH :

When a router or host discards a datagram due to congestion it sends a source quench message to the sender.

TIME EXCEEDED :

When TTL becomes zero, time exceed message is generated.

PARAMETER PROBLEM :

If error is in IP header, it can identify the error in header but ICMP is generated.

- Whenever the header bits are modified by the noise of the IP packet, then it can be identified by the header checksum.

- But IP cannot report the errors becoz it has no error control.
- Then ICMP will take the infoⁿ and informs to the source that it is a parameter problem.

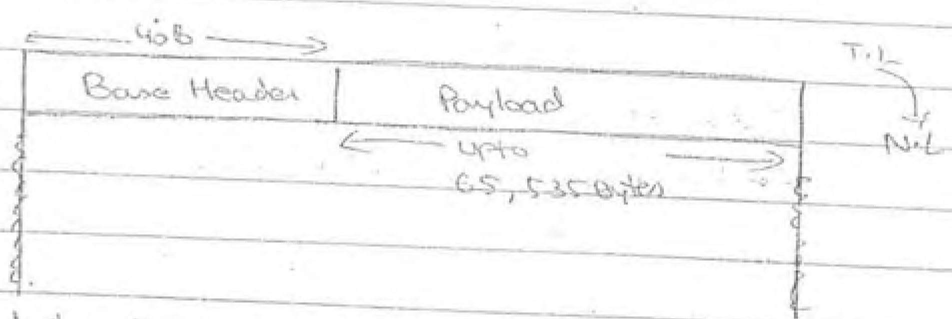
REDIRECTION :

Due to breakage router can change the virtual path, then ICMP report to sender redirection message ie packets are redirected or path is changed.

TIMESTAMP REQUEST OR REPLY :

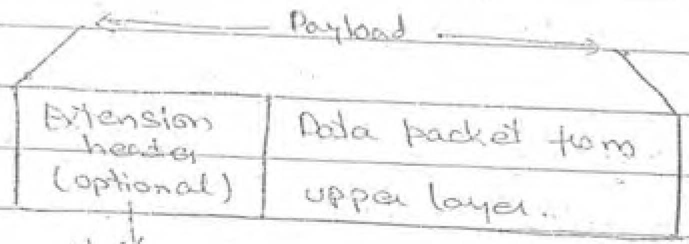
ICMP is used for regenerating timestamp reply or request for managing the network.

→ IPV6 :-



IPV6 is faster than IPV4 :-

becoz i) It does not require fragmentation at each stage



extra services are mentioned here. like strict routing, loose routing.

→ Security is high in IPV6.

→ It is connection - oriented becoz of flow-label. ie logically connected.

Date:

Format of Base header:

0 — 3 4	— 12	— 32 (each row 4 bytes)	
VER 4 bits	TRAFFIC CLASS	FLOW LABEL (24 bits)	
PAYLOAD LENGTH (16 bits)		NEXT ~~HEADER~~ (8 bit)	HOP LIMIT (8 bits)
SOURCE IP ADDRESS (128 bits) (require 4 rows becoz each row is 4 bytes)			
DESTINATION IP ADDRESS (128 bits)			

TRAFFIC CLASS :

→ It is called as priority. In IPV6 there is 256 priorities availabe.

FLOW LABEL :

→ For each flow labl there is a 1 no. assigned.
So 0 to $2^{24}-1$ no. can be assigned.

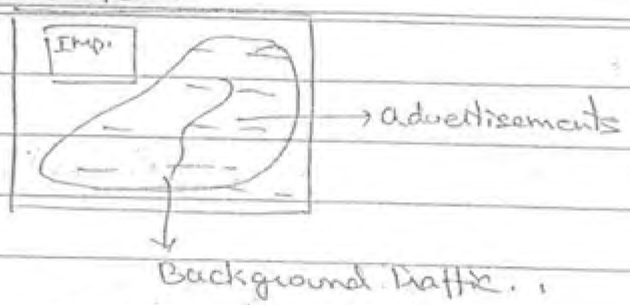
Priority 1 : Control packets → identify status of router.
Priority 2 : Data packets.
ie. Top-most priority is given to control ~~priority~~ packet.

• For highest priority packet, it assigns a ~~f~~ one flow label to provide services.

→ According to priority ~~packet~~, no. of services are ~~are~~ provided to packets.

highest → more services
lowest → less services

→ Data packet :



ie along with important data we are unintentionally getting ~~unwanted data also. that data is known as background traffic.~~

NEXT HEADER :

- It tells extra headers that are added to IPV6. ie if next header 8 bits all are zero then there is no extra header. ie Data has only base ado header.

Traffic class indicates the priorities of the packet. Based on the traffic class and flow label routing of the packets is done in IPV6.

A Flow label can be used to speed up the processing of the packet by the router.

→ When a router receives a packet, instead of consulting the routing table and going through routing algorithm to define the address of next hop, it can easily look in the flow label table for the next hop.

HOP LIMIT :-

- It is similar to TTL which is in IPV4. It tells the maximum time to 'or' loop time.
- Hop limit can be 0 to '256.

→ Whenever a packet reaches to a router, router provides resources with the help of resource ~~ser~~ reservation protocol, To support real time audio-video RTP is used. (RSTP)

RTP : Real time Protocol.

Pg 104

Ques 11 - PD = 50 sec

$$L.U = \frac{T.T\ data}{TT_{data} + TT_{Ack} + Procundata + PT_{ack} + 2\ Propagation\ delay}$$

~~10 1sec~~ → 10^8 bits ~~400 byte~~ $TT_{data} = \frac{400 \times 8}{100 \times 10^6} = 32$

$$TT_{ACK} = \frac{64 \times 8}{100 \times 10^6} = 5.12$$

$$L.U = \frac{32}{32 + 5.12 + 10 + 5 + 2 \times 50}$$

$= 21.02 = 21\ \%$

Ques 12 -

Pg 106

Ques 18

$1 \xrightarrow[150\mu s]{1000\text{ bytes long}} 2$

5 packet — each packet occupy – 50 µs.

T.T = 5×50 = 250 µS.

PT = 200 µsec.

Total time = 250 + 200

= 450 µS.

Pg - 109

Ques 19 Throughput = $\frac{5 \times 1000}{450\ \mu sec}$

$= 11.11 \times 10^6$ Bps.

Date:

To correct d errors, the minimum distance is 2d+1

Pg 108

Q.No.24-

$$\begin{array}{l} 00000000 \\ 00001111 \\ 01010101 \\ 10101010 \\ 11110000 \end{array}$$

(distances: 4, 4, 8, 4; 4; 4)

To correct = 2d+1 = Min. distance

4 = 2d+1

3 = 2d

$d = \frac{3}{2} = 1.5$

→ So it is correcting 1 error, but it may not exactly correct 2nd error.

→ NYQUIST THEOREM :

Message Signal + Carrier Signal ⇒ Modulated Signal.

$\boxed{f_s \geq 2 f_m}$ → modulating frequency

↳ sampling rate frequency

$BW = f_2 - f_1$

f_2 ↓ upper, f_1 ↓ lower frequency

$f_s \geq 2(f_2 - f_1)$ → it considers range of sampling signal & modulated signal.

If $f_2 \gg f_1$

then $f_s \geq 2 f_2$

Problem with the redundant bridges is, there may be a chance of occurrence of loops for that data. So spanning tree bridges solve this problem.

pg 112

Q8 -

$BW = 16\ Mbps$.

$$PT = \frac{D}{V} = \frac{1000\ m \times 100}{60 \times 3 \times 10^8\ m}$$

$$= \frac{1}{18} \times 10^{-4}$$

$$= \frac{100}{18} \times 10^{-6}$$

$$= 5.5\ \mu sec$$

~~Ring latency = P.D of ring + Interface delay + Token holding time of each station~~

Time taken = Ring latency + Token holding time for each station

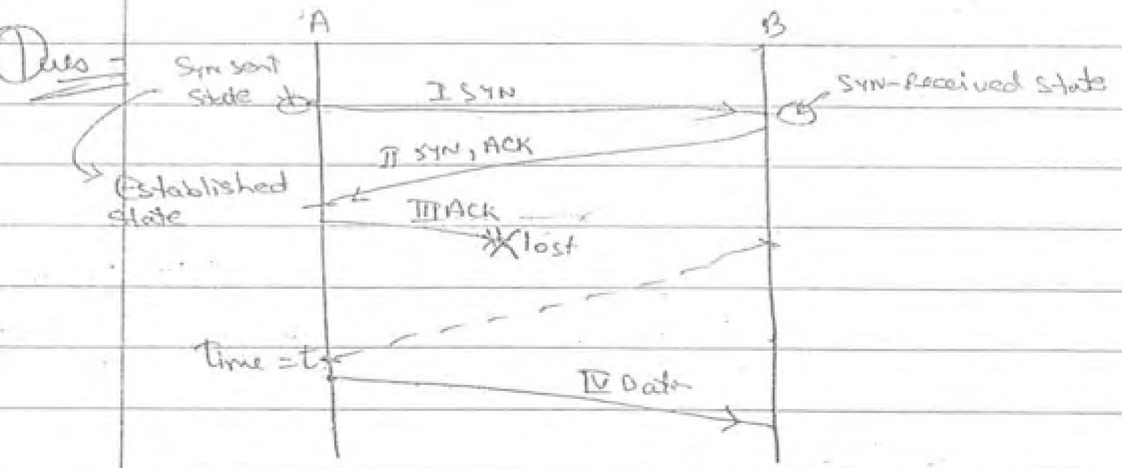
$= 5.5\ \mu sec + 25 \times 5\ \mu sec$

$\quad = 125\ \mu sec$

$= 130.5\ \mu sec$

$= 1.305 \times 10^{-4}\ sec$

Ques -



Time line showing exchange of some segments b/w TCP_A & TCP_B. The X indicates that the ack segment was lost

a) What are the states of TCP_A and TCP_B at time t.

TCP_A = Established state.

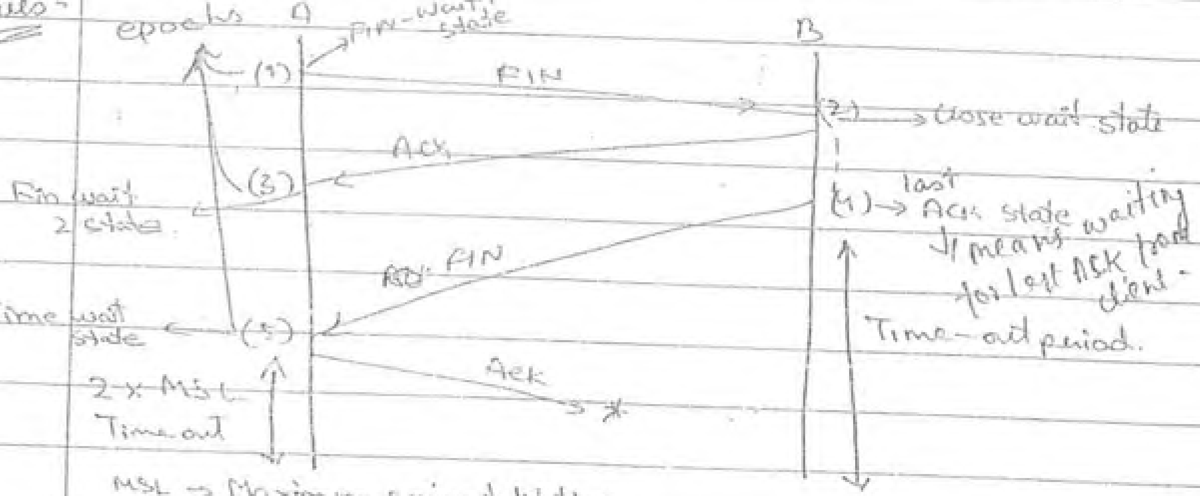
TCP_B = SYN - Received state.

b) After time t, can A sends a data segment as shown in the figure.
- Yes.

c) How will this data be handled at B.
A will send lost ACK again with data segment. So B will get to know data is coming from A only.
So, at this time, B is in established state, and can parallely send data to A.

(A) $\underbrace{\text{ACK + data Segment}}_{\text{Piggy backing}} \rightarrow$ (B)

ie when ACK for connection is send with data segment to requester.

Ques-


MSL → Maximum segment lifetime

a) What are the states of TCP_A at epochs 1, 3, and 5
Mention the states ~~of~~ at of TCP_B at epochs 2 and 4.
(1) → FIN - WAIT 1 state.
ie when data transmission in completed and it has to release the connection, ~~th~~ it sends FIN segment and goes to FIN-wait 1 state.
→ When a FIN segment is received from a client and if the server has ~~d~~ some data leftover at that point, then it go to Close - wait state.

Date: 14/9/

→ When the ACK is coming from server without the FIN segment then it indicates that some data has to come from server or B. then, TCP go to FIN-wait 2 state.

→ If ACK lost then next FIN segment must reach within 2 ×MSL time out.
If not come within that time then A voluntarily releases connection.

→ (5) → Time wait state becoz if ack lost and next FIN has to come then A must be in some state so it is in this state.

→ Congestion :-

- Senders maintains 2 windows :
  - Receiver advertised window
  - Congestion window.

⇓

It tells the maximum size that can be transmitted through virtual path.

⇓

If more than that then packet will not be transmitted.

⇓

Is given by the router in the virtual path.

Receiver Window Size > Congestion Window Size

then,

Congestion window size data should be transmitted so that no Congestion.

→ Hence, Sender window size = min(C.wnd, R.wnd)

- If R.W << C.W, then

  S.W.S = R.W

  At this type TCP implements, Flow of control policy.

- If R.W >> C.W, then

  S.W.S = C.W

  At this point TCP implements policy called Congestion policy.

Date:

CONGESTION POLICIES OF TCP :

→ It focuses on condition :

If R-window >> C-window

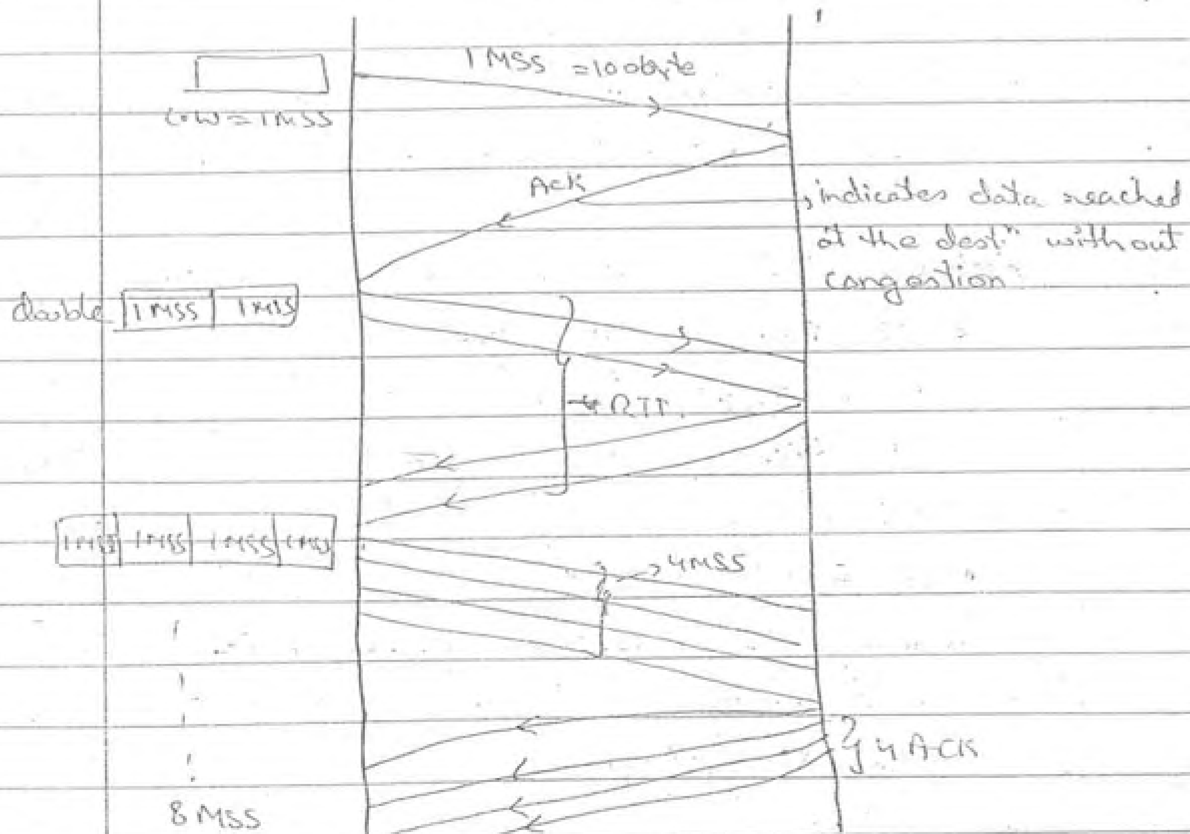
then, S.W.S = C-window

→ They are :

1) Slow start
2) Congestion Avoidance
3) Congestion detection

1) SLOW START POLICY :

→ During connection establishment, congestion window size is fixed at 1 MSS at the sender side.



Date:

→ Initially, C window = 1 MSS
After 1st RTT = 2 MSS
After 2nd RTT = 2^2 MSS
After 3rd RTT = 2^3 MSS
↓
exponentially grows

→ In slow-start algo, the increase of congestion window is based on No. of ACKS.

→ Initially, slow-start algo start slowly but increases exponentially.

Slow-Start threshold :
↳ 100 byte
↓
200 byte
↓
400
↓
800
↓
1600 → Algo Stops here. ie at S.S threshold.
↓
3200 → Called slow start threshold

Becoz Router tell that the max. 4000 Byte

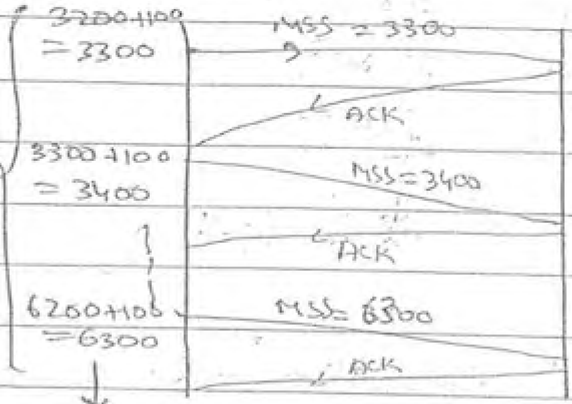
↓
6400
↓
Here congestion occurs.

→ After slow-start algo, congestion avoidance, will comes
ie After threshold slow start.

2) CONGESTION AVOIDANCE :

will continue upto 6300 bytes

linear 6400 occurs



But at 6400 congestion will occur.

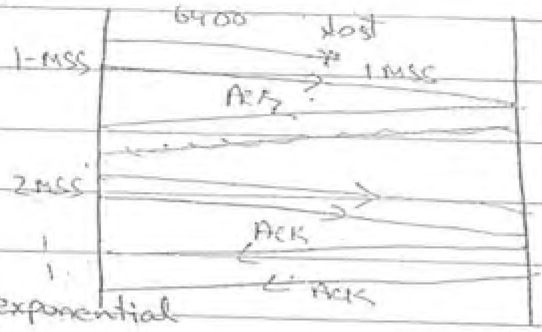
→ In slow start algo, the increase of congestion window is based on no. of ACKS.
Where as increase of congestion window in congestion avoidance is based on the Round Trip time (RTT)

3) CONGESTION DETECTION :

↳ This 6400 is lost becoz of 2 reasons:

Case 1: Stronger possibility of congestion.

Case 2: Weak possibility of congestion.



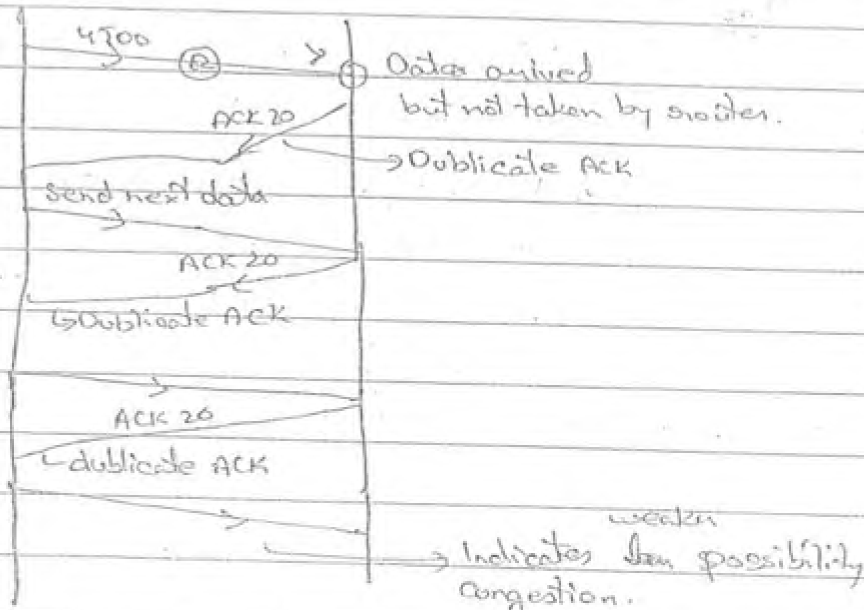
→ If case 1 : then, start with slow-start algo.
↓
If ACK received
↓
then exponentially grows.

ONCE A CONGESTION IS DETECTED IF THERE IS STRONGER POSSIBILITY OF CONGESTION THEN
Congestion window is made as and then start the slow start algo.

→ If Case 2: Weaker possibility is detected by duplicated Acks.

→ Once a congestion is detected and if there is a stronger possibility of congestion, then congestion window is made as 1MSS and ~~strassen~~ algo. is started.
Slow start window

Eg:-



→ If after 3 duplicate ACK, if the data is taken by few time then, it is a weaker possibility of congestion. then,

- Congestion window will be not made 1MSS but made half of previous
- So we apply congestion avoidance algo.
  it also known as

→ Even after the time-out if the data is not taken then there is stronger possibility of congestion.

→ When there is a weaker possibility of congestion, then it is detected by 3 duplicate ACK. and congestion avoidance algo is applied.

→ If there is a stronger possibility of congestion, reduce the congestion window to 1MSS and start the slow start algorithm.

→ These congestion policies are applied only when congestion window size is less than the receiver window size.

Ques17 Pg-138

1 MSS = 2000 bytes

Got 2 Acks.

→ Increase based on no. of Acks.

So, 4000 + 4000

= 8000 bytes

Ques18 Pg-138

Congestion window = 4KB

Advertise window = 6KB

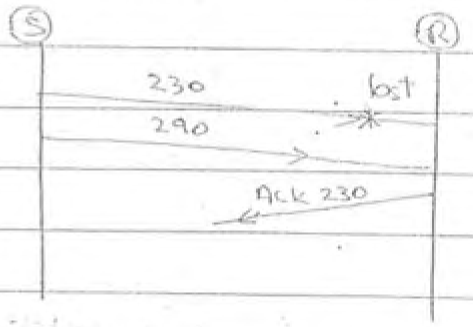
Current Window size = Min(c.w, a.w)

= Min(4KB, 6KB)

= 4KB

= 4096

Ques19 - Pg-138



So, Y = 230

X = 290 − 230

= 60

Ques22 Pg-139

C + ρS = MS

6 + 2·8 = M·8

22 = M8

M =

Ques 8 - Pg-136

I.R.T.T = 30 msec

N.R.T.T = 26.32 msec

$\alpha = 0.9$

~~N.~~ E.R.T.T = $\alpha \cdot$ IRTT + $(1-\alpha)$ NRTT

= $0.9 \times 30 + 0.1 \times 26.32$

= $27 + 2.632$

= $\underline{29.632}$ msec.

↓

IRTT

~~[illegible]~~

N.R.TT = 24 msec

ERTT = $0.9 \times 29.632 + 0.1 \times 24$

= ~~[illegible]~~ $2.4 + 26.64$

= 29.04 msec.

(C) ✓

Ques 9 - Pg-136

24 bytes

→ 4 ⇒ $\boxed{3 \mid 1}$ only 1 byte so transmit 24 times

→ 6 ⇒ $\boxed{3 \mid 3}$ 8 times transmit

→ 7 ⇒ $\boxed{3 \mid 4}$ 6 times transmit

→ 9 ⇒ $\boxed{3 \mid 6}$ 4 times transmit

So 9 is answer

Ques 10 Pg-137

HTTP

TELNET } uses TCP in Transport layer.

SMTP

Ques 2 - Pg-135

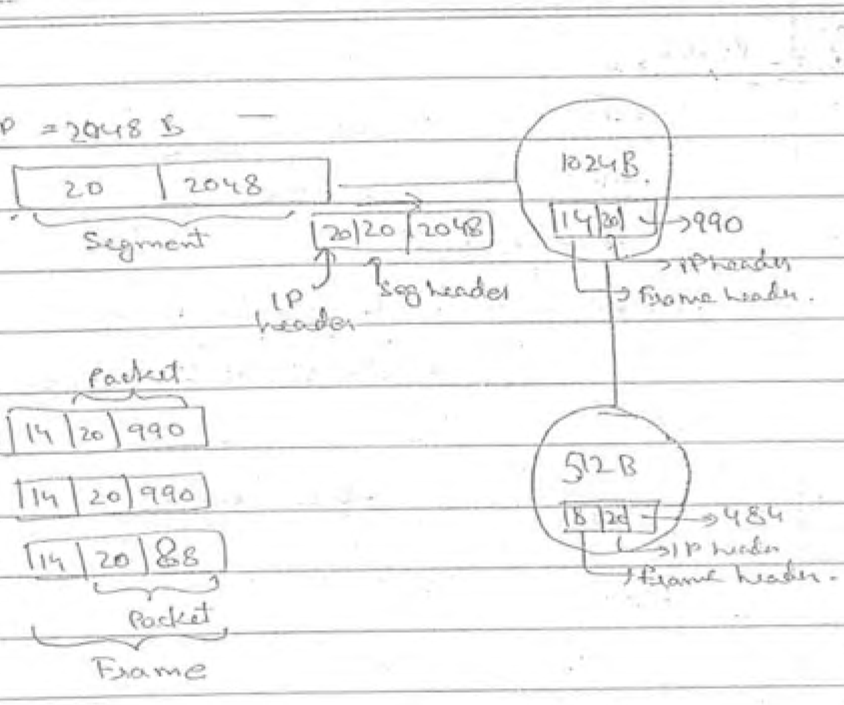
R.T.O = 2 × R.TT

= 2 × 35.23

= 70.46 ms

Ques4 → Pg 135

TCP = 2048 B



cont. to Q4

Ques5 → 990 → | 8 | 20 | 484 |

→ | 8 | 20 | 484 |

→ | 8 | 20 | 22 |

Ques26 Pg-116

$V = 2\times10^8$ m/sec

Length $= 1\times10^3$ m

BW = 10 Mbps

length of each slot = Transmission time of 100 bits + Propagation delay

$PD = \dfrac{1\times10^3}{2\times10^8} = 0.5\times10^{-5}$ sec

$= 5\ \mu sec$

$TT = \dfrac{\text{Msg size}}{B.W}$

$= \dfrac{100 \text{ bits}}{10^7 \text{ bits/sec}}$

$= 10\ \mu sec$

Let N no. of stations

For N ~~length of~~ cycle $= N(10+5) = 15N\ \mu s$

$N(PT+T.T)$ Date:

Each user transmit $= \frac{10}{15N} \times B.W$ → only $\frac{10}{15N}$ is used out of total BW.

given $\frac{2}{3} = \frac{10}{15N} \times 10^9$ Mbps

It is throughput.

$N = 10$

Ques-27 Pg-116.

$B.W = 100$ Mbps, $RTT = 64\ \mu sec$

CSMA/CD;

So $TT = 2 P.T$

$\frac{\text{Msg size} + 48 \text{ bit}}{B.W} = 64\ \mu sec$

$\frac{n +}{100 \text{ Mbps}} = 64$

$n = \frac{64 \times 100}{8}$ bytes

$= 800$ bytes.

Jamming signal is not included becoz in frame size itself we are adding jamming signal.

Ques) Pg-118

X.25 can be routed becoz it has 3 layer.
but N/w link cannot be routed becoz it is only in n/w layer.

Ques 5 Pg-119

$C + FS = MS$

$8 \times 40 +$

Ques 8. → $BW = 100$ Mbps

$= \frac{1}{2} \times \frac{84 \cancel{42}}{10^6}$

$T = \frac{84 \times 8}{10^8} = 6.72\ \mu sec$

FTP PROTOCOL :-

↳ has 2 versions : 1) FTP → uses TCP at T.L
2) TFTP → uses UDP at T.L

Reason behind this.

becoz ① FTP has no flow control whereas TFTP has internal flow control.

② FTP is authorized users & TFTP is anonymous users.

→ This protocol is client - server protocol or synchronous protocol becoz client is directly contacting the server.

becoz clocks are synchronize while downloading

→ At client side we use dynamic ports (49151 to 65,535) and at server side we use well known or predefined port (0 to 1023)

→ Server maintains 2 connections
1) Data Connection → use port 20
2) Control Connection → use port 21
↳ always in open state

→ Client will always be in active open state
⇓
port which generate control / data.

→ Server will always be in passive open state
⇓
state when data is entered into the port
ie that receiving data.

→ When connection is established then server will automatically create or open data connections.

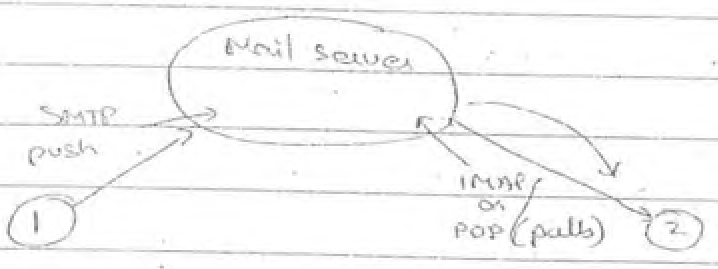
→ For providing FTP service ; the server will have control connection in passive open state.

→ Whenever a request comes from a client, server is going to execute a Fork system call so that it can have 2 connections : 1) Data connection → at child
2) Control connection → at parent.

- Now the data is transmitted b/w client and server via data connection on port 20
- Port 21 is free for new client connection.

→ SMTP PROTOCOL :-

- Is a application protocol providing mail services.
- It is a host to host protocol.
- It is asynchronous protocol. → becoz it is contacting to ~~other host through server.~~
- It is a text based protocol.



→ With help of MIME extension we can send multimedia data also.
MIME ⇓ Multipurpose internet multimedia extension

→ Is called as a PUSH Protocol becoz it pushes the mail of clients to in the mail server.

→ POP3 or IMAP-4 are pull protocol becoz they pulls data into the inbox at next host
IMAP-4 → it is better than POP
POP3 → Post office Protocol
IMAP-4 → Internet Message Access Protocol

→ It uses TCP protocol at transport layer :-
- It uses port 25 for connection to TCP

→ HTTP PROTOCOL :-

- Is a client - server protocol
- It uses port 80
- It is known as State-less protocol.

↓

becoz one browser is closed no related infor^n is loaded at Client side.

- Due to cookies data is transmitted very fastly becoz it stores the state of termination where browser is terminated.

→ It has versions ie,

1) HTTP 0.9 → Non-Persistant
2) HTTP 1.0/1.1 → Persistent http.

In non-persistant, for every data you transfer connection is automaticaly closes.
ie for every data transfer connection is closed.

In Persistent connection, connection remains open until the whole data is transmitted.

Date:

→ It supports 8 methods at client side :

Safe

- Head
- Get
- Put
- Post
- Trace
- Connect
- Delete
- Options

Unsafe methods
⇓
can change the content in the server..

HEAD : When a client contacts a server, using this method that get name of browser, type of browser, type of O.S and version of O.S. that is used.

PUT : This method is used to create an object in the server.

Client can access data on server by using server methods and these methods are in interface.

POST : Used to access the content of the server and can modify the content in the server.

DELETE : Using this we can delete the contents of the server.

TRACE : Is used for ~~be~~ debugging. It is tool which is provided by http.

CONNECT : Is used for secure connection.

GET : Client gets data from server.

OPTIONS : Used for transfering data, and it defines authorized and anonymous user.

INTRA DOMAIN PROTOCOL :

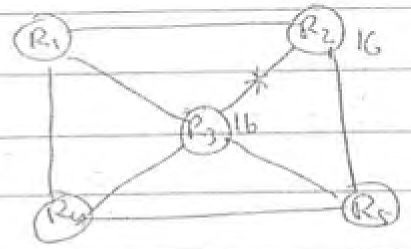
Theses are used for small areas.

RIP → uses distance vector Routing

OSPF → uses link state routing algorithm.
→ No count to infinity problem.

RIP :

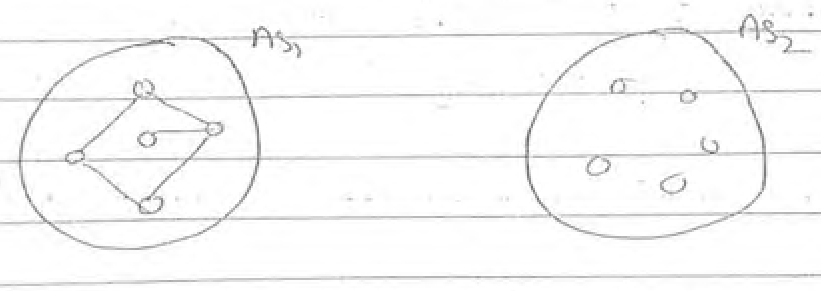
- It supports maximum 15 hops.
- Used for lesser no. of routers.
- When there is breakage 16 is automatically assigned



- Count to infinity problem will be known to all routers after some time then that path will be discarded

OSPF :

Occurs in between anonymous state n/w.
It has control packets.



Initially in AS, one router generate a control packet that is called link state packet.

(1)

Date:

→ This packet contains infoⁿ about :

1) How many routers
2) No. of links
3) No. of up and down links
4) Type of topology is used at the router.

} ⇒ Defines entire topology of domain

→ For generating LS packet, cost is more becoz entire infoⁿ of autonomous system or routers infoⁿ has to be there in LS packet.

→ In LINK STATE ROUTING ALGORITHM, LSP packet will consist of entire topology of the domain.

• After generating LSP, that router broadcast that packet to all neighbouring routers

⇓

• Neighbouring routers now get to know all information of autonomous system.

→ Generation of LSP is not one time process ie it is generated periodically becoz if there is breakage in link that can be updated.

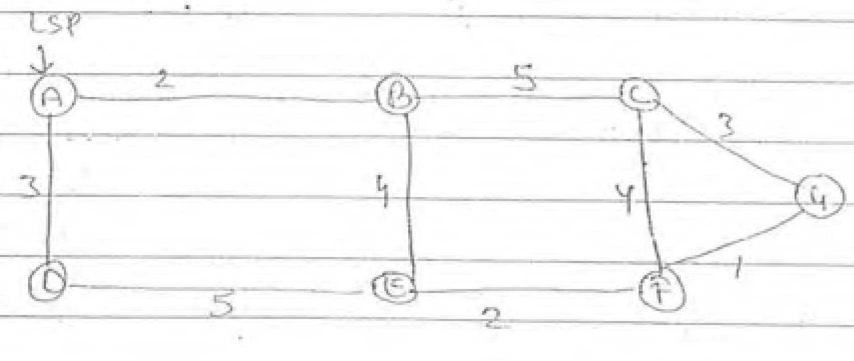
→ For LSP there is timestamp packet and sequence packet

⇓

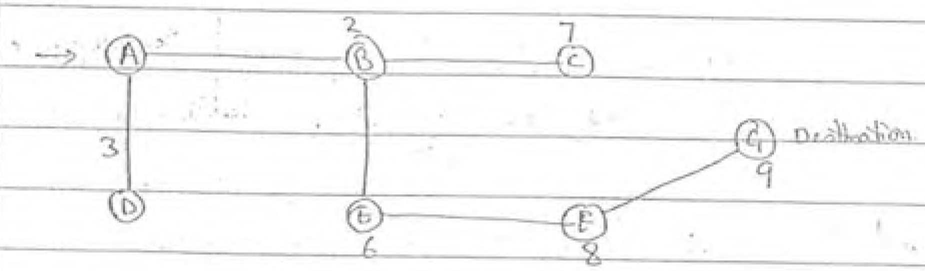
new value is considered true

→ For broadcasting we use Dijkstra shortest path algo.

Q) Ans-

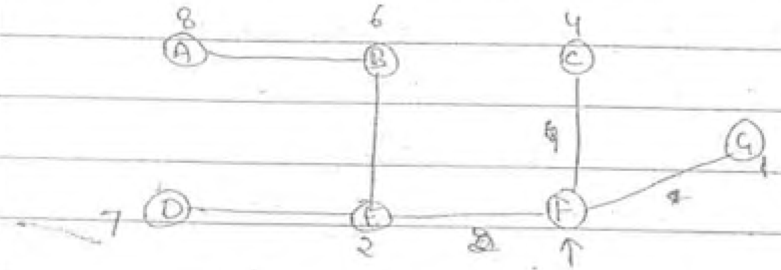


In above diagram calculate shortest path tree for router A in a graph.

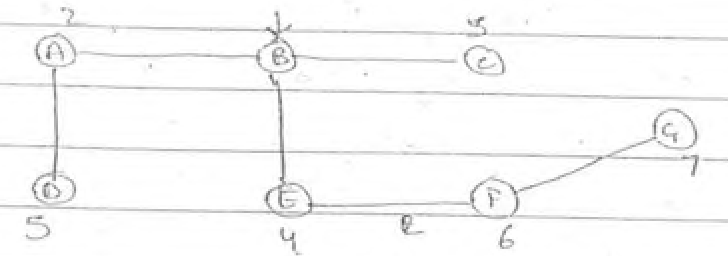


• While broadcasting, there will be no redundant packets and their will be no loop formation for LSP packet....

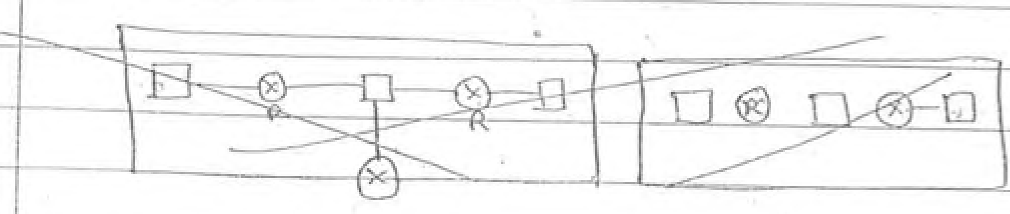
For F router :



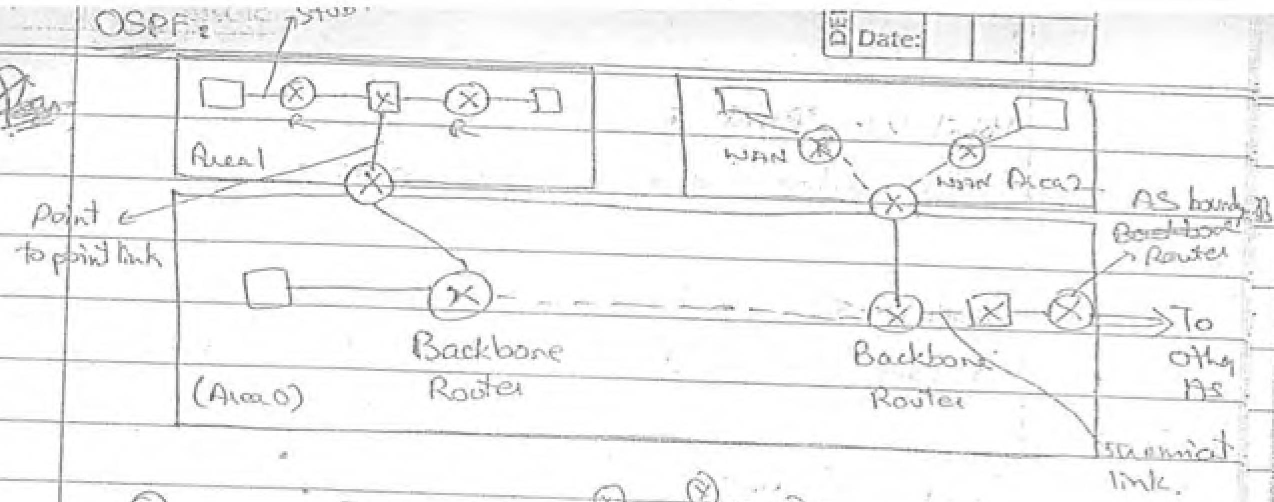
For B router :



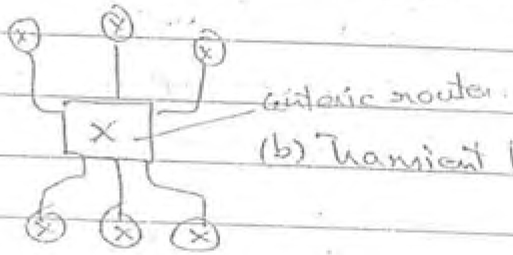
Ques-



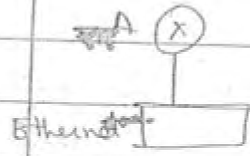
OSPF:



(a) Point - Point link
(b/w link of routers)



(b) Transient link



(a) Stub link

→ The autonomous system are divided into areas and the default area is area 0 which is used to connect different areas.

→ If a packet has to be transmitted from system in area 1 to system in another area, 1st it has to pass through a area boundary router and then through backbone router.

→ A system in one area to a system in another area of another autonomous system (AS), it has to pass via AS boundary router.

Now link breakage will be :

1) Stub link break
2) Point-to-point break
3) Transient break

VIRTUAL LINK : Created by admin to transfer data b/w AS & inside AS when there is breakage. It is end to end link.

Point – to – Point :

Is connected between two routers.

STUB LINK :

Is connected between a router and a LAN

TRANSIENT LINK :

Is created between many routers: ie is connected to many routers.

→ Whenever there is a breakage in links, a virtual link is created over the entire autonomous system. So, no area will not stop the data transmission of the packets.

→ HIERARCHIAL ROUTING :-

↳ Is used in inter-domain routing.

↳ It reduces size of the routing table due to which access time ↓ & performance ↑ es:

eg:-

Before → After.

000
001
010
011
100
101
110
111

↓

8 searches.

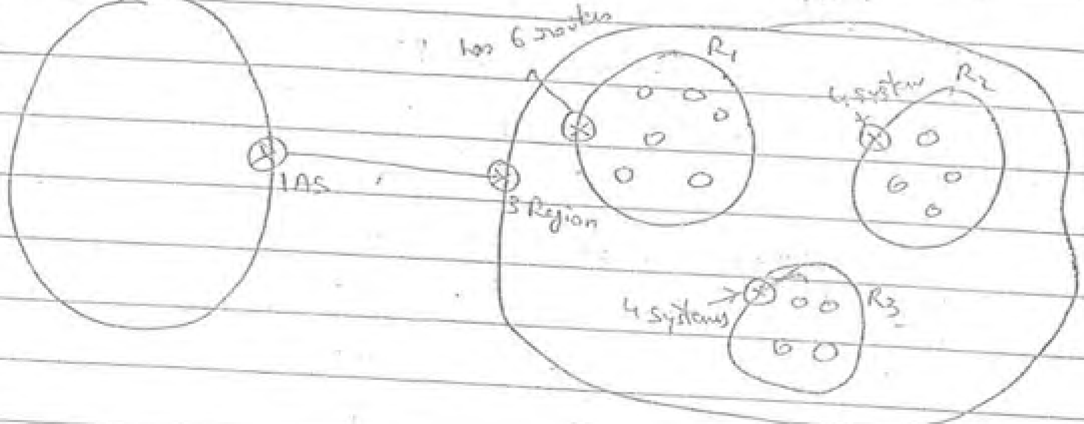
0	00
	01
1	10
	11

↓

2+4 = 6 Searches

Date:

→ Router at AS will only hold information ie value of other AS not their entire routers of that AS, ie packet has summarize info" when going to different A.S



To provide a summarize information, hierarchical routing technique can be used.

→ Path Vector Routing :-

↳ Inter Domain

↳ BGP implements path vector routing.

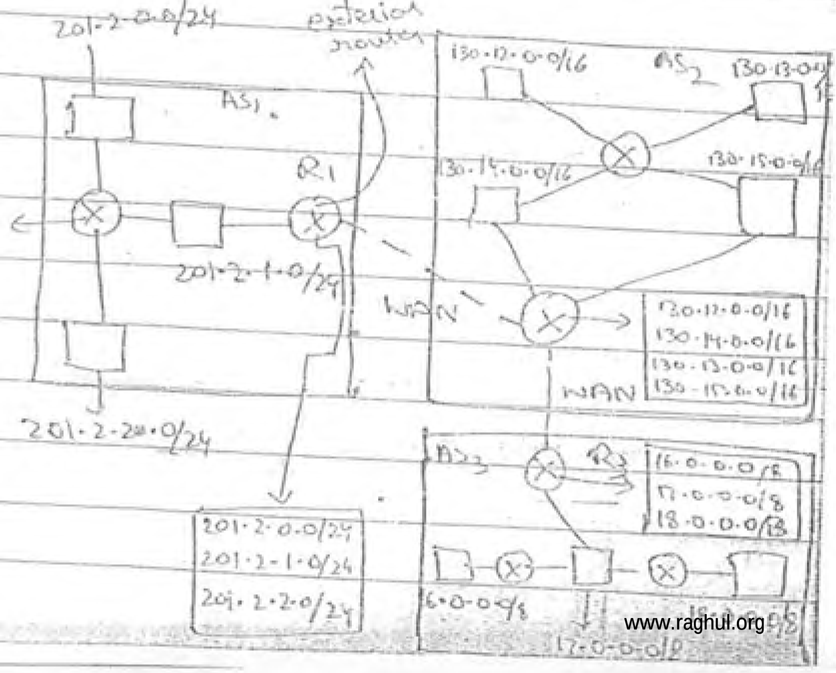
↳ Boarder Gateway Protocol

Ex: Distance vector : India map

Path vector : International map.

FUNCTIONALITIES :

1) Reachability :-



Date:

Qu. Calculate path vector table for router R_1 in above figure.

NETWORK	PATH
201.2.0.0/24	AS_1
201.2.1.0/24	AS_1
201.2.2.0/24	AS_1
130.12.0.0/16	AS_1, AS_2
130.13.0.0/16	AS_1, AS_2
130.14.0.0/16	AS_1, AS_2
130.15.0.0/16	AS_1, AS_2
16.0.0.0/8	AS_1, AS_2, AS_3
17.0.0.0/8	AS_1, AS_2, AS_3
18.0.0.0/8	AS_1, AS_2, AS_3

⇓ Reduced to

Network	Path
~~RS~~ 201.2.0.0/22	AS_1
130.12.0.0/14	AS_1, AS_2
16.0.0.0/6	AS_1, AS_2, AS_3

$2^{32-22} = 2^{10} = 4$

$2^{32-24} = 2^{8}$ → one block → 4 block → each block has 256

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

So, $2^{32-22} = 2^{8} = 1024$ → it can consist above all 3 LAN

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

$2^{32-14} = 2$

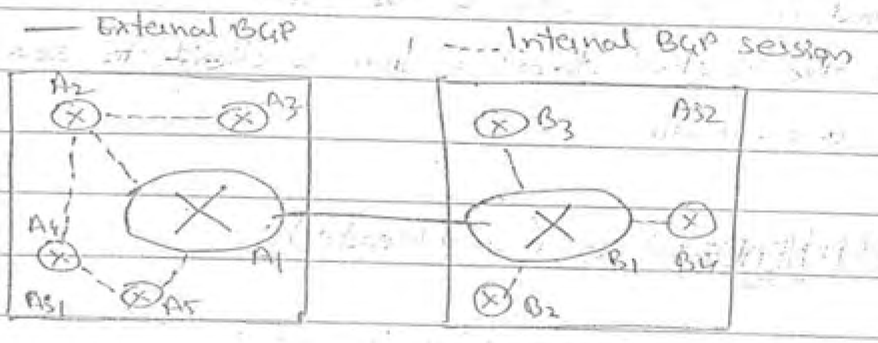
$2^{32-8} =$

$2^{32-6} =$

→ BGP is going to use path vector routing.

BGP PROTOCOL :-

→ Implements Path vector routing.



→ BGP takes help of TCP to provide sessions.

- Within AS, we can use RIP or OSPF
- Between other AS, we use path vector routing. So, it provides sessions.

→ A_1 connects session with B_1 and provide summarized information.

→ The session that are provided between the interior routers and the exterior routers is known as I-BGP session ie internal BGP.

- Virtual path is setup for all areas within a AS. Through this router collects information.

→ The session that are provided b/w two exterior routers of two autonomous system, then it is known as E-BGP session or exterior BGP.

Qn:- Following is a dump of a UDP header in a hexadecimal format :

CB84000D001C001C.

... length length no.
length of user datagram
vice versa. directed the data from a client to server

UDP HEADERS :- (UDP Header) :-

Source Port 16 bit	Destination Port 16 bit
TOTAL LENGTH 16 bits	CHECKSUM 16 bit

TCP	UDP
→ Is Reliable	→ Is unreliable
→ Segments travel in same direction becoz of virtual path	→ Datagrams travel different directions
→ Header is variable ie 20 to 60 Bytes	→ Header is fixed ie 8 bytes
→ Has flow & error control	→ Has no flow & error control
→ Is for sending long msgs	→ Is for sending short msgs.
→ It doesn't support multi-casting becoz of virtual ckt	→ It supports multi-casting becoz it has no virtual ckt so it can multi-cast msg.
 It can't multi-cast msg to all routers.	

UDP Eg:- 1) DNS (If DNS < 512byte) It can support upto 127 levels.
2) To manage SNMP becoz it have to update all devices for better managing.

Diagram :-

Header 8 bytes	Data

≤ 65,535 Bytes

Date:

→ UDP has checksum ~~bcoz~~ which is not mandatory ie it is optional.

→ It does not give error control for all datagram. but it provides error control for received ~~pac~~ datagrams.
ie checksum is for received datagram.

Solution of above Problem :-

CB84000D001C001C

each bit has 4 ~~bytes~~-bits

So,

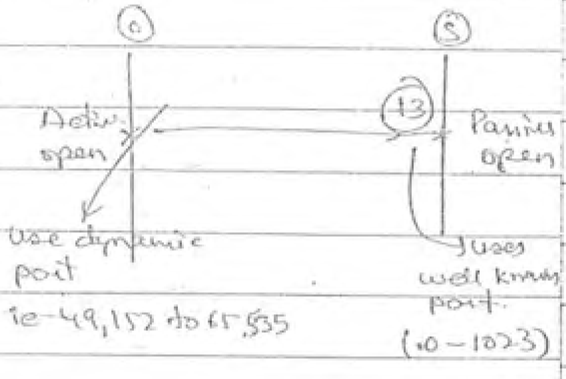
Source port $= (CB84)_{16}$
$= 52100$

Destination port $= (000D)$
$= 13$

Total length of datagram = 4 bits
= 001C
= 16+12
= 28

length of data = 8+10 = 28
= 10 data

So, packet is coming from client to server.



→ CHECKSUM :

→ No specific rule to calculate checksum
→ Same rules are applied at both sender and receiver side.

Eg:

$\underbrace{458367}_{\text{Data to Transmit}} \longrightarrow$ 8 bit checksum.

Sender side : 45
83
67

195

→ 95
+1

96 To improve complexity

→ FF
−96

69 Checksum calculated at sender side

ie

45836769 (codeword) → 45836789 → R

89 → modified checksum

Receiver side :

45
83
67

195

→ 95
+1

96 → FF
−96

69 Checksum at receiver side

but 89 is not equal to 69 so data is corrupted.

45836769 (codeword) → 45846869 → R

45846 8 → data modified.

45
84
68

197

→ 97
+1

98 → FF
−98

67 ≠ 69

So data is rejected by receiver.

PROBLEM : It cannot detect vertical bit errors but these can't occur in T.L becoz total content is 65,535B

when one increment & one decrement in data then modified data checksum will be ~~Equal to original at receiver~~ side.

eg: 457377 (69)

Decr. Incr.

Checksum at receiver = 69. and receiver receiver will accept it. but its wrong data.

→ Checksum calculation doesn't have any specific rules. but the rules that are applied at sender side same rules you have to apply at the receiver's side.

Qus. Calculate the checksum for a simple UDP user datagram

153.18.8.105			
171.2.14.10			
All 0's	17	15	
1087		13	
15		All 0's	
T	E	S	T
I	N	G	Pad

Pseudo header	32-bit Source IP address	
	32-bit Destⁿ address	
	All 0's | 8 bit protocol	16 bit UDP Total length
UDP header	Source port 16 bit	Destⁿ port 16 bit
	UDP Total length 16 bit	Checksum 16 bits
Data	DATA	

A = 65 (ASCII)

In 16-bit checksum :

SIP = 1001 1101 0001 0010   153.18

0000 1000 0110 1001   18.105

Date:

TCP is a connection-oriented. In this unreachability of port can be detected by using time out action of time.

In UDP there is no acknowledgement to inform the sender that the receiver is not reachable.

ICMP is used by the router to inform unreachability.

Ques- Consider a token ring with the latency of 500 usec. Assume that there are sufficiently many hosts transmitting. So that time spent in the token can be ignored. Frame size of 1500 byte ring has a B.W of 3 Mbps. What is the effective throughput that can be achieved.

(1) If delayed token strategies is used and if there is a single user in the ring.

R. latency = 500 usec

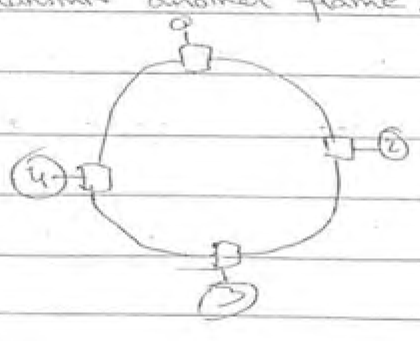
F.S = 1500

BW = 3 Mbps

$$TT = \frac{1500 \times 8}{3 \times 10^6}$$

$= 4000$ usec

If single user in there then their user transmit the frame and wait until last bit of the frame is received to it, and then user releases the token, token circulates in the ring. then comes back to user then user can transmit another frame.



Date:

Delayed token = TT. of data + R. latency of data + R. latency of token

= 4000 us + 500 us + 500 us

= 5000 us.

L.U = Throughput = $\frac{1500 \times 8}{5000}$ = Q.

= 2.4 Mbps

% throughput = $\frac{2.4}{3} \times 100$

= 80 %

Qn- If delayed token release strategies is used and if there are many users in the ring. Calculate the effective throughput rate that be reached.

by how much time it is going to transmit data.

$\frac{1500 \times 8}{4500 \text{ usec}}$ = 2.66 Mb

$\frac{2.66}{3} \times 100$ = 88 %

TT. of data + 1 Ring latency.

Questions of Network layer :-

Qn-7 IP addr. = 203.197.2.53 | 2 = 00000010

255.255.128.0 | 128 : 10000000

203.197.0.0 — ① | 00000000

IP addr = 203.197.75.201 | 75 : 01001101

255.255.128.0 | 128 : 10000000

203.197.0.0 — ② | 00000000

① = ②

G₁ assumes that G₂ is on same n/w.

Date:

Using : 255.255.192.0

C_1 : 203.197.2.3

255.255.192.0

203.197.0.0

C_2 : 203.197.75.201

255.255.192.0

203.197.64.0

C_2 assumes C_1 is on different n/w.

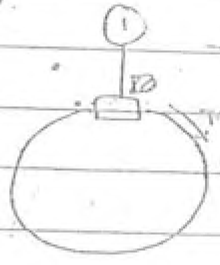
Ques-9- TCP doesnot have minimum comm.^{n} rate becoz

17/9/14

Date:

Ques- Consider a token ring with the latency of 500 usec. Packet size is 1500 bytes. and B.W is 3 Mbps.

① What is the effective throughput rate, that can be achieved if ~~delayed~~ early released token strategy is used and their is a single user in the ring.



→ Early token release.

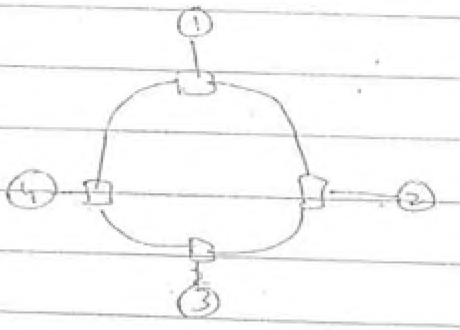
$= \frac{\text{Packet Size}}{\text{T.T}_{data} + \text{R. latency}}$

$\text{T.T} = \frac{1500 \times 8}{3 \times 10^6} = 4000$

$= \frac{1500 \times 8}{4000 + 500 \text{ usec}}$

$= 2.66$ Mbps.

② If early token released is used and there are many users in the ring.

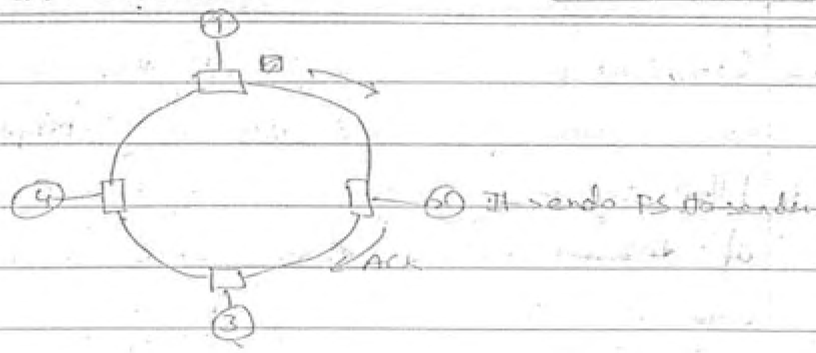


$= \frac{1500 \times 8}{\text{T.T}}$

$= \frac{1500 \times 8}{4000 \text{ usec}}$

$= 3$ Mbps.

→ Calculate Link Utilization:



① Delayed token release,

$$= \frac{TT \text{ of data}}{R.L \text{ of data} + \frac{R.L}{N}}$$

R.L → Ring latency.
N → no. of stations.

Qno 12 - 113 - Pg

$$TT = \frac{100 \times 8}{100 \times 10^6} = 8 \ \mu sec.$$

$$L.U = \frac{8 \ \mu sec}{\cancel{5 \times 10^3} + \frac{\cancel{5000}}{25} + 25 + \frac{25}{25}}$$

$$= \frac{8}{25+1} = \frac{8}{26} \times 100 = 30.8\%$$

P.D = 5 nanosec ⟶ 1m

25 μsec ⟷ 5000 m

② Early token release,

$$= \frac{TT \text{ of data}}{TT + \frac{\text{Ring latency}}{N}}$$

Qno 13 Pg - 113.

$$= \frac{8 \ \mu sec}{8 + \frac{25}{25}}$$

$$= \frac{8}{8+1} = \frac{8}{9} \times 100 = .88$$

$$= 88.8\%$$

Performance improved $= \frac{88.88}{30.8} \approx 3$ times

Date:

Ques 14 Pg-113

$BW = 100 \times 10^6$

$R.L = 200\ \mu sec$

$F.S = 1 \times 10^3 \times 8$

Maximum Throug. $TT = \frac{8 \times 10^3}{100 \times 10^6}$

$= \cancel{8 \times 10^{-6}}\ \cancel{\mu sec}\ 80\ \mu sec.$

$\text{Throughput} = \frac{\text{Data Size}}{\text{Total Time}}$

$= \frac{\text{Data size}}{R.L + TT_{data}}$

$= \frac{10^3 \times 8}{80 + 200}$

$= \frac{800\cancel{0}}{28\cancel{0}} = \frac{800}{28} = 28.5$ bits/μsec

Q 15 Pg-113

$\text{Throughput} = \frac{\text{Frame Size}}{TT + 2 \times RL}$

$= \frac{10^3 \times 8}{80 + 2 \times 200}$

$= \frac{8000}{400 + 80} = \frac{8000}{480}$

$= 16.7$ bits/μsec.

Q 23 Pg-115

$BW = 10 \times 10^6$

$R.L = 400\ \mu s$

$F.S = 1000 \times 8$ bits

$TT = \frac{1000 \times 8}{10^7}$

$= 800\ \mu Sec.$

$\text{Effective data rate} = \frac{8 \times 1000}{TT +}$

$= \frac{8 \times 1000}{800 + 2 \cdot 400} = \frac{\overset{5}{\cancel{8000}}}{\cancel{1600}} = 5$ Mbps

$TT + 2 \cdot RL$

Date:

Ques- Consider a token ring topology with N stations running a token ring protocol where the stations are equally spaced. Ring latency is t_p, transmission time of frame is t_x and all other latencies can be neglected. Calculate the Maximum utilization of the token ring when $t_x = 300$ millisec, $t_p = 5$ millisec & $N = 10$.

(a) If delayed token release is used.

(b) If early token release is used.

(a) $$L.U = \frac{300 \times 10^{-3}}{5 \times 10^{-3} + \frac{5 \times 10^{-3}}{10}}$$

$$= \frac{300 \times 10^{-3}}{10^{-3}(5 + 0.5)}$$

$$= \frac{\overset{600}{3000}}{\underset{11}{55}} = 54.\cancel{8}$$

(b) $$L.U = \frac{300 \times 10^{-3}}{300 \times 10^{-3} + 0.5 \times 10^{-3}}$$

$$= \frac{3000}{300.5}$$

$$= \frac{3000}{3005} = 9.98336$$

Ques- Find the ring latency in seconds for a 4 Mbps ring. The no. of stations are 40 separated by 50 metres. and bit delay at each station is 3 bits. Velocity is $2 \times 10^8 \, ms^{-1}$

a) 90 μs b) 160 μs

c) 40 μs d) None

$$\frac{\overset{150}{\cancel{200}}}{2 \times 10^8}$$

$$10^6 \times 15 \times 10^{-7} \times 4$$

$$\frac{}{10}$$

$= 60$

$= 6^{10}$

Ring latency $= \cancel{\square} + \cancel{\square} \; \overset{120}{\cancel{180}} +$

Date:

Qus- Consider a token ring with the ring latency of 200 usec and delayed token release is used. when packet size is 1 Kilobyte. What is the effective throughput that can be achieved if ring has a B.W = 4 Mbps.

$$T.T = \frac{1 \times 10^3 \times 8}{4 \times 10^6}$$

$$= 2000 \text{ usec.}$$

$$\text{Throughput} = \frac{8 \times 10^3}{2 \times 200 + 2000}$$

$$= \frac{8 \times 10^3}{2400 \times 10^{-6}}$$

$$= \frac{80}{24 \times 10^{-6}}$$

$$= \frac{1000}{300} \text{ Mbps.} \rightarrow \text{B.W that we are utilizing.}$$

$$\text{effective throughput} = \frac{\frac{1000}{300}}{4} \times 100$$

$$= \frac{1000}{300} \times \frac{100}{4}$$

$$= \frac{250}{3} = 82\%$$

Qus- Token ring uses 24 bit token and has 5 stations with 1 bit delay and total wire length is 230 meters. Propagation speed is 2.3×10^8 m/sec. How many artificial bits monitor must insert into the ring to avoid overlapping in 16 Mbps token ring.

$BW = 16 \times 10^6$

1 sec $\longrightarrow 16 \times 10^6$
1 usec $\longrightarrow 16 \times 10^6 \times 10^{-6} = 16$ bit

Ring latency = P.D + interface delay
= 16 + 5
= 21 bits.

5 bit delay i.e. interface delay

$Pd = \frac{230}{2.3 \times 10^8}$

$= 1$ usec

3 bits are artificial becoz we uses 24 bit token but we require only 21 bits, so 3 bits are artificial bits that are added.

Date:

Ques- For a token ring to work properly, the 1st bit of data should not come back to the place where it was produced until the whole frame is produced. Since the token is 3 bytes long and operates at 16 Mbps What should be the minimum length of ring for proper operation of the token passing method. Assume that Propagation speed is 60% of speed of light (3×10^8 m/sec)

a) 270 m

b) 1160 m

c) 100 m

d) 160 m.

$B.W = 16\times10^6$

$\text{Propagation speed} = \frac{60}{100}\times 3\times10^8$

$= 18\times10^7 = \frac{180\times10^8}{100}$

$= \cancel{180\times10^8}$

$1\text{ sec} \longrightarrow 16\times10^6$

$P.D \quad \frac{L\times100}{180\times10^8} \longrightarrow 16\times10^6$

$PD = \frac{L}{\frac{180}{100}\times10^8} = \frac{100L}{180\times10^8}$

$= \frac{16\times10^6\times L\times100}{180\times10^8}$

$= \frac{L\times10^7\times16}{18\times10^8}$

$= \frac{16\,L}{180}$

$= \frac{16}{180}L$ bits

PD = Token frame bits

$\frac{16}{180}L = 24$

$16L = 24\times180$

$L = \frac{24\times180}{16} = 270\text{ m}$

Date:

Ques- A token ring LAN interconnects 20 stations using a star topology in the following way:
All the i/p and o/p lines of the token ring station interfaces are connected to a cabinet where the actual ring is placed. Suppose the distance from each station to the cabinet is 100m. and ring latency per station is 8 bits. Assume that all packets are 1250 bytes and the ring BW is 25 megabits per second. , $V = 2\times10^8 \, m\,sec^{-1}$

(a) Find the ring latency in terms of bits.

a) 210 bits

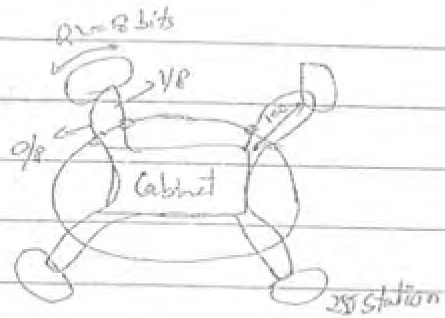
b) 310 bits

c) 410 bits

d) 510 bits.

250
410

Ring latency = P.D of ring + Interface delay.



$$P.D = \frac{D}{V}$$

$$= \frac{\cancel{20}^{10} \times 200}{\cancel{2}\times10^8 \, m\,sec^{-1}}$$

$= 20\ \mu sec.$

$\because$ 1 sec $\longrightarrow$ 25×10^6 bits

$20\ \mu sec \longrightarrow 25\times10^6 \times 20\times10^{-6}$

$= 500$ bits.

Interface delay :-

$20\times8 = 160$ bits.

Ring latency $= 160 + 500$

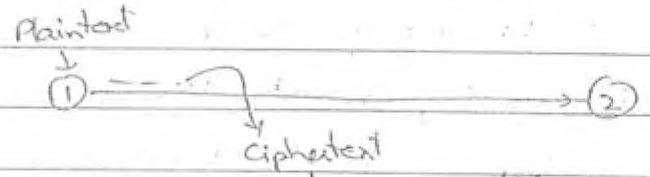
$= 660$ bits

Date:

Encryption & Decryption :-

Plaintext : Is the understandable form of data.

Ciphertext : Unundurstandable form of data ie converted data.



↳ Give confidendiality and authentiation.

→ Conversion of plaintext to ciphertext is done by technique called as Cryptography.

→ Stegnography : We hide the data behind the video or image.

CONFIDENTIALITY : It means data or information must not be known to unauthoized person

AUTHENTICATION : It means infor^{n} known to all but that must proof the authenticity of the person.

ENCRYPTION : Process of converting plaintext into ciphertext

ie

$$C = E_K(P)$$

↳ Encryption key

⇓

To generate key we use mathematical expr^{n}

DECRYPTION : Process of convertion ciphertext into plaintext

ie

$$P = D_K(C)$$

↳ ~~Enc~~ Decryption key.

Date:

→ Key can be :

1)

2)

→ If same key is used for encryption and decryption of data, it is known as Symmetric key cryptography

→ If two different keys are used to encrypt and to decrypt, it is known as Asymmetric key

→ Attacks can be :

1) Active (changing data)
2) Passive (not changing data)

ACTIVE ATTACK : Whenever data is going, attacker takes data and modifies that and sends modified data.

PASSIVE ATTACK : Whenever data is going, attacker takes data and without modifying it sends the data to receiver

• By passive attack, attacker can analyse traffic and type of data ie is transmitting.

ETHICAL HACKER : Attacks the data and ~~th~~ if there is loop hole then they inform the sender about the problems. in their n/w.

→ There are some softwares that can make server to believe that all requests are coming from different systems. ie
all other systems are not getting service and this attack is denial of service attack.

② ③ → Denial attack

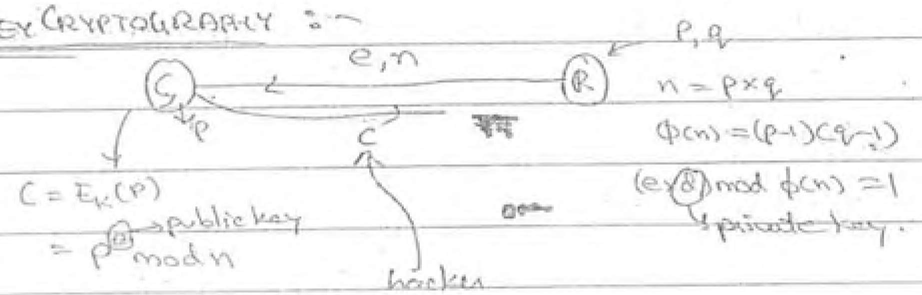
Date:

→ A system can create a fake IP addresses and make the server believes as they are coming from different clients

- All the resources of the server are blocked by a particular person.
- Then the actual clients will not get the service of the server. ~~Thus~~

This attack is known as DENIAL OF SERVICE ATTACK.

ASYMMETRIC KEY CRYPTOGRAPHY :-



(e, n, C) Known.

then, $P = D(P) = C^d \bmod n$

but e is public key.

So P cannot be retraced here.

→ This algo is known as RSA algorithm.

Ques- RSA algo is used by choosing 2 prime no.'s, $p = 3$, $q = 11$, Public key $e = 3$, Calculate the value of d.

a) 31

b) 9

✓ c) 7

d) 4

$n = 33$

$\phi(n) = 2 \times 10 = 20$

$3d \bmod \phi(n) = 1$

$3d \pmod{20} = 1$

$3d = 1 \quad \therefore d = 7$

$d = 7$

Date:

Ques- RSA algo is used with prime no.'s 7, and 11. to generate public key and private key's. If $e = 7$ then

a) Calculate d value.

1) 60

2) 55

3) 40

4) 43

$n = 77$

$\phi(n) = 60$

$7d \bmod 60 = 1$

$d = 43$

7×43

$\frac{301}{60}$

b) In the above problem encrypt the plaintext '9' using above data.

$C = P^e \bmod n$

$= 9^7 \bmod 77$

$= 4782969 \bmod 77$

$= 37$

a) 37

b) 43

c) 47

d) 53

Ques- RSA algo is used, using $p = 7$, $q = 11$ and (e, n) is (7, 77) Calculate the secret key i.e d.

$\phi(n) = 6 \times 10$

$= 60$

$(e \times d) \bmod \phi(n) = 1$

~~7d mod 456 = 1~~

$7d \bmod 60 = 1$

$d = 43$

a) 11

b) 17

c) 37

d) 43

Ques- RSA algo is used by choosing two prime no's $p = 19$, $q = 23$ and if $e = 5$, what is the value of Z ?

a) 317

b) 396

c) 437

d) 7

Date:

$n = p \times q = 19 \times 23$

$\phi(n) = 18 \times 22$

$z = n = 19 \times 23$

$= 437$

Qn. In above questions, what is the secret key in above problem.

a) 317 ✓ — $(d \times e) \bmod \phi(n) = 1$

b) 396 — $5d \bmod 396 = 1$

c) 437 — $d = 317$

d) 7

$\phi(n) = 18 \times 22 = 396$

Qn. RSA algo is used by choosing 2 prime no.'s p=7 and q=17. If e=5 calculate value of d.

a) 31

b) 99

c) 77 ✓

d) 44

$n = 119$

$\phi(n) = 96$

$ed \bmod \phi(n) = 1$

$5d \bmod 96 = 1$

$d = 77$

$77 \times 5 = 385$, $96 \times 4 = 384$

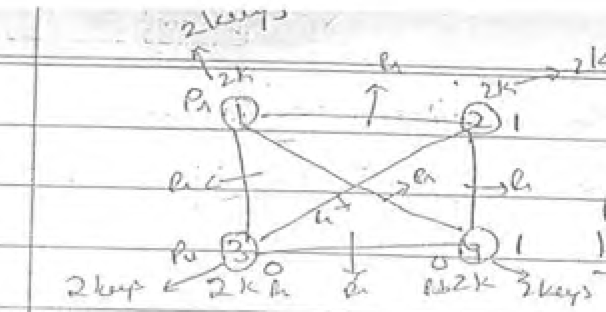
Qn. The total no. of ~~case~~ keys required for a set of n individuals to communicate with each other using secret key and public key cryptosystems.

a) $n(n-1)$ & $2n$

b) $2n$ and $\frac{n(n-1)}{2}$

c) $\frac{n(n-1)}{2}$ and $2n$ ✓

d) $\frac{n(n-1)}{2}$ and n.



Public keys = $2n$ in public key crypto.
→ 1 private & 1 public.

Private = $\frac{n(n-1)}{2}$
→ no. of cables.

DIFFI - HELMAN KEY XCHANGE :-

①   p, g are public   ②

x, p = random no.

$R_1 = g^x \bmod p$ $\xrightarrow{R_1}$ $R_2 = g^y \bmod p$

$\xleftarrow{\boxed{R_2}}$

$K = (R_2)^x \bmod p$
$= (g^y \bmod p)^x \bmod p$
$= g^{xy} \bmod p$

$K = (R_1)^y \bmod p$
$K = (g^x \bmod p)^y \bmod p$
$= g^{xy} \bmod p$

are same
So, are not transmitting on channel.

→ This algo creates a session key which is not transmitted over the n/w.

Ques. The Diffi-helman key xchange is being used to establish a ~~sender~~ session key b/w sender & receiver with the values of $n = 23$, $g = 7$, If senders secret key $x = 3$, then the message ie transmitted is $(23, 7, \underset{R_1}{\_\_})$

a) 4

b) 17

✓ c) 21

d) 28

$R_1 = g^x \bmod p$
$= 7^3 \bmod 23$
$= 21$

$343 \div 23 = 14$, $343 - 23 = 113$, $113 - 92 = 21$

Date:

b) In the above question if ~~the~~ $y = 6$ ie receiver secret key. Then it will respond with a msg ___ ?

a) ~~18~~ 4

b) 17

c) 21

d) 28

$R_2 = g^y \bmod p$

$= 7^6 \bmod 23$

$= 4.$

c) In above problem what is session key b/w sender and receiver.

a) 4

b) 7

c) 11

d) 18

$K = g^{xy} \bmod p$

$= 7^{3 \cdot 6} \bmod p$

$= 7^{18} \bmod 23$

$= \cancel{177649 \bmod 23}$

$= 18$

Qus. The DH-Key exchange is being used to establish a session key b/w sender and receiver with the values of $n = 47$, $g = 3$

1) Senders secret key is $x = 8$. Then it transmits a msg (47, 3, ___)

a) 4

b) 17

c) 21

d) 28

Date:

2) Receivers secret key is $y = 10$. Then H responds with a msg

a) 4

b) 17

c) 21

d) 28

3) Calculate the session key.

a) 4

b) 17

c) 21

d) 28

(1) $R_1 = g^x \bmod p$

$= 3^8 \bmod 47$

$= 28$

(2) $R_2 = g^y \bmod p$

$= 3^{10} \bmod 47$

$= 17$

(3) $K = g^{xy} \bmod p$

$= 3^{10 \times 8} \bmod 47$

$= 3^{80} \bmod 47$

$= 4$

$3^{80} = 3^{10}$ Remainder $= 17$

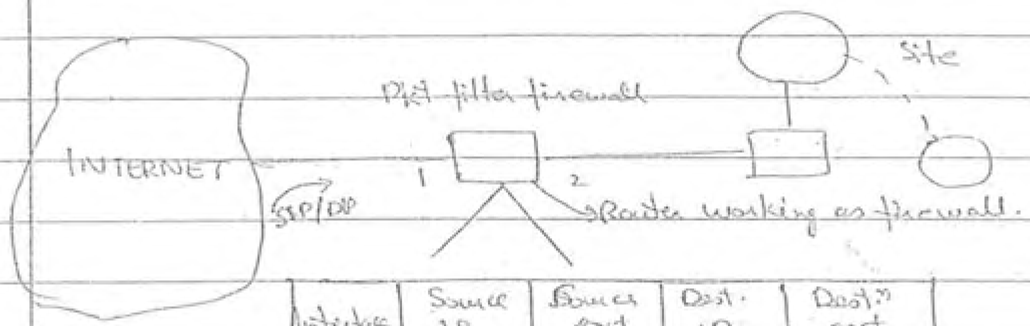
$(17)^8 \bmod 47$

$17 \times 17 = 289 \bmod 17$

$= 7$

$(7)^4 \bmod 47 = 4$

FIREWALLS :-



Interface	Source IP	Source port	Dest. IP	Dest.n port
1	131·34·0·0	*	*	*
1	*	*	*	* 23 → Telnet
1	*	*	194·78·20·8	*
2	*	*	*	80 → http

* : any or all.

- Any packet coming from SIP 131·34·0·0 router will block the packet in the n/w itself.
- Any packet ie coming for port no. 23 that will be not allowed.
- If sender is any and packet going to 194·78·20·8, then don't allow the packet to go out.
- To block the internet connection eg in college then, dest.n port is having 80 that causes router to block the paket for port 80.

→ Incoming packets for the internal host 194·78·20·8 are blocked. The org.n wants this host for internal use only.

→ Outgoing packets for the http server ie port 80. are blocked. The org.n doesn't want employs to browse the internet.

COMPUTER NETWORK R-S.PO