

COMPUTER NETWORKS

Handwritten Notes

VIVEKANAND VERNEKAR

GateWallah Parakram C 2024

(Hinglish Weekday)

Other Notes Uploaded Below

<https://t.me/pwgatenotes>

IPv4 ADDRESSING

Basics of IP addressing

$$2^1 = 2$$

$$2^2 = 4$$

:

$$2^9 = 512$$

$$2^{10} = 1024 = 1K \text{ (Kilo)}$$

$$2^{20} = 1024 \times 1024 = 1m \text{ (mega)}$$

$$2^{30} = 1G \text{ (Giga)}$$

$$2^{40} = 1T \text{ (Tera)}$$

$$2^{50} = 1P \text{ (Peta)}$$

$$2^{60} = 1E \text{ (Exa)}$$

$$2^{70} = 1Z \text{ (Zetta)}$$

$$2^{80} = 1Y \text{ (Yotta)}$$

Conversions :

$$1 \text{ Byte} = 8 \text{ bits}$$

$$1 \text{ KB} = 1024 \text{ Bytes}$$

$$1 \text{ MB} = 1024 \text{ KB} \text{ (Kilo byte)}$$

$$1 \text{ GB} = 1024 \text{ MB} \text{ (mega byte)}$$

$$1 \text{ TB} = 1024 \text{ GB} \text{ (Giga byte)}$$

$$1 \text{ PB} = 1024 \text{ TB} \text{ (Tera Byte)}$$

$$1 \text{ EB} = 1024 \text{ PB} \text{ (Peta Byte)}$$

$$1 \text{ ZB} = 1024 \text{ EB} \text{ (Exa Byte)}$$

$$1 \text{ YB} = 1024 \text{ ZB} \text{ (Zetta Byte)}$$

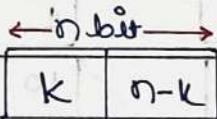
2 bit

00011011

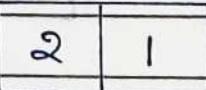
3 bit

000001010011100101110111

(find bit)

1 bit \rightarrow 2 pairs = 2¹ pair2 bit \rightarrow 4 pairs = 2² pairsK bit \rightarrow 2^K pairs2^K pairs 2^{n-K} (Size of each pair)2^K pairs \rightarrow 2ⁿ1 pair \rightarrow $\frac{2^n}{2^K}$ $= 2^{n-K}$

3 bit

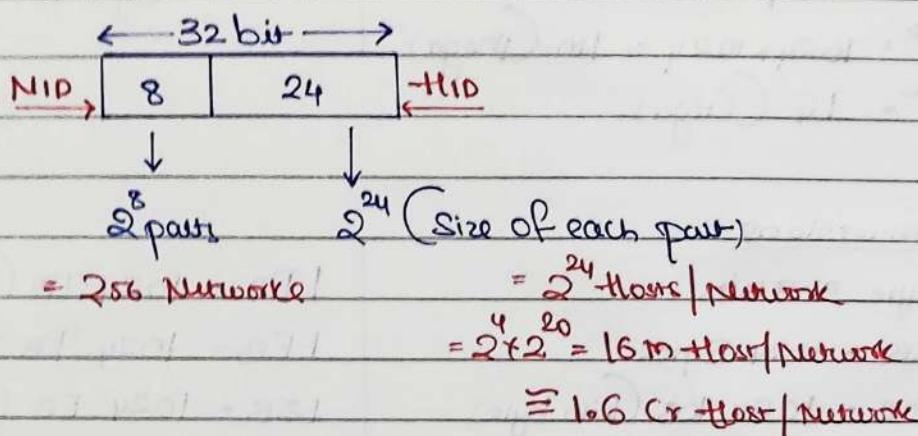
2² pairs 2 = 2 (Size of each pair)

Introduction to IP Addressing

IPv4 Address = 32 bit

Total number of IPv4 addresses = $2^{32} = 4,294,967,296$

Initially in 1980's IP addresses were divided into two fixed parts i.e. NID = 8 bit and HID = 24 bit.

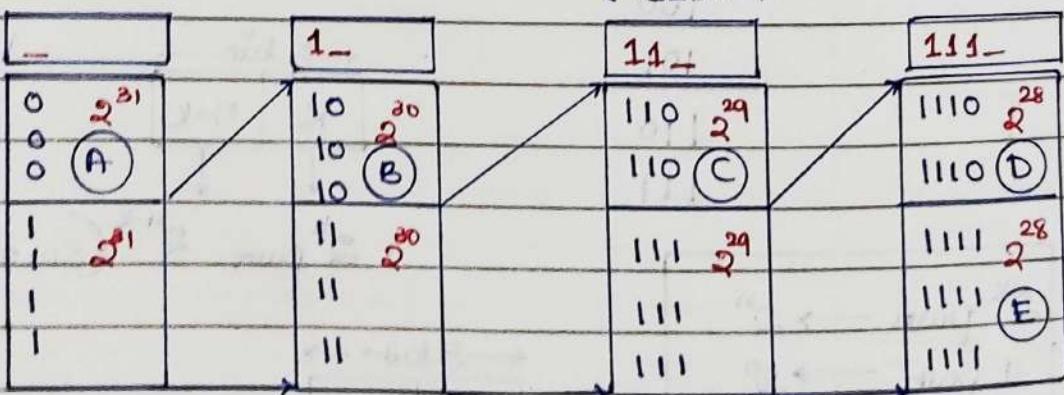


IANA : Internet Assigned Number Authority

Disadvantage: There are only 256 Networks, and even a small organization must buy 16m to purchase one network.

Classful Addressing:

← 32 bit →



No. of IP address present:

Class A: 2^{24}

Class B: 2^{16}

Class C: 2^8

Class D: 2^2

Class E: 2^0

Class A: 0

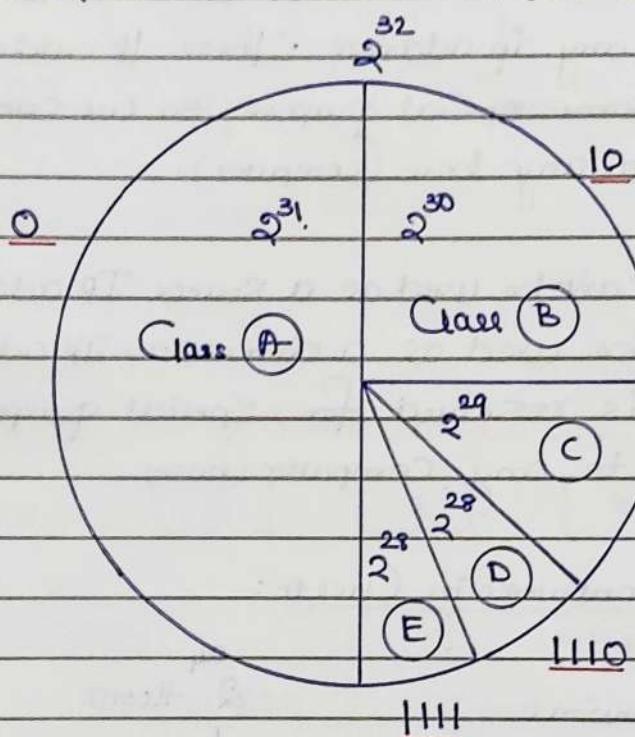
Class B: 10

Class C: 110

Class D: 1110

Class E: 1111

} Fixed bits?



Class A: 0.0.0.0
Class B: 128.0.0.0
Class C: 192.0.0.0
Class D: 224.0.0.0
Class E: 232.0.0.0

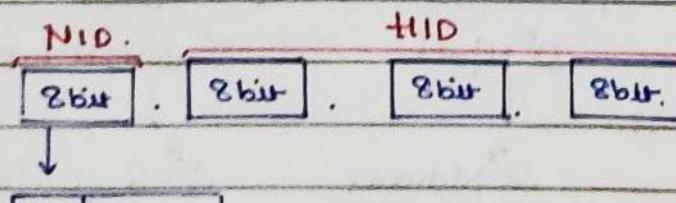
IP address representation:

Binary: - 11001000. 11111100. 00111111. 11110111

Decimal: - 200. 252. 63. 247

Hexadecimal: - C8. FC. 3F. F7

Class A : $0 \rightarrow 2^{31}$



first bit fixed

00000000 — 0 X

0000001 — 1

0000010 — 2

:

0111110 — 126

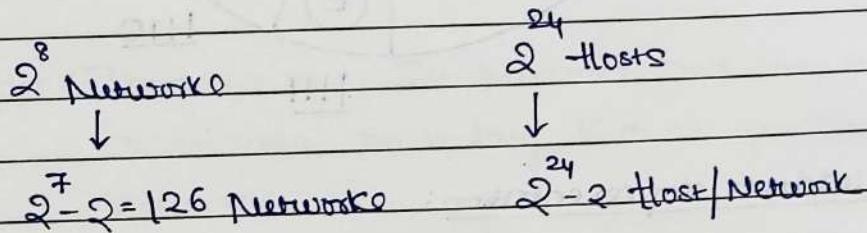
0111111 — 127 X

} 1-126

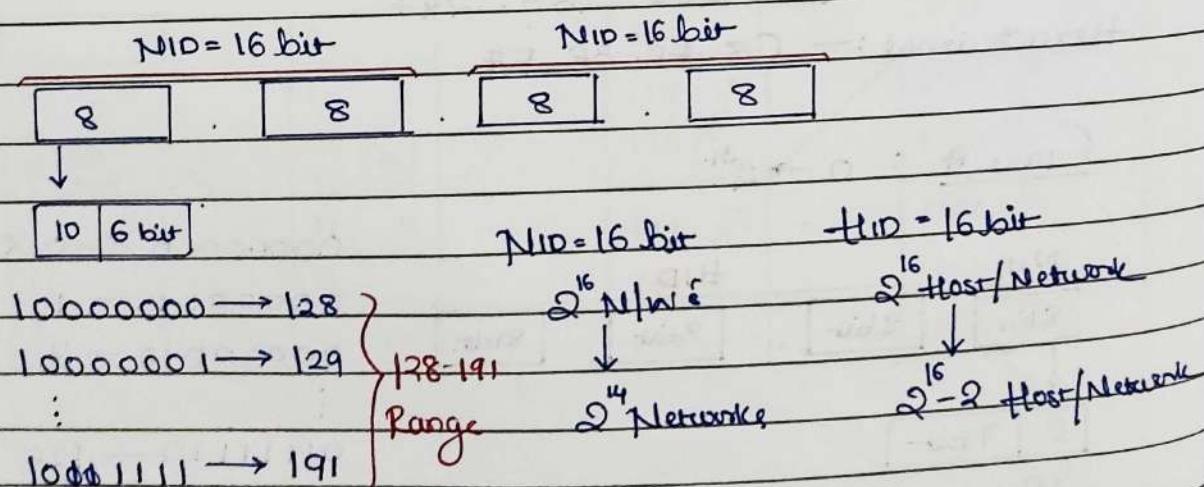
} Range

- * 0.0.0.0 : Default route or DHCP Client
- * 127.x.x.x : Self connectivity / Loopback testing / interprocess communication.
- * Whenever we have all zeros or all ones either in network id or host id of any ip address. These IP addresses are reserved for some special purpose, so we can't assign these IP addresses to any host (computer).
- * 127.x.x.x can't be used as a source IP address (S.TP). It will always be used as a destination IP address.
- * 127.x.x.x is reserved for special purpose so it can't be assigned to any computer (host).

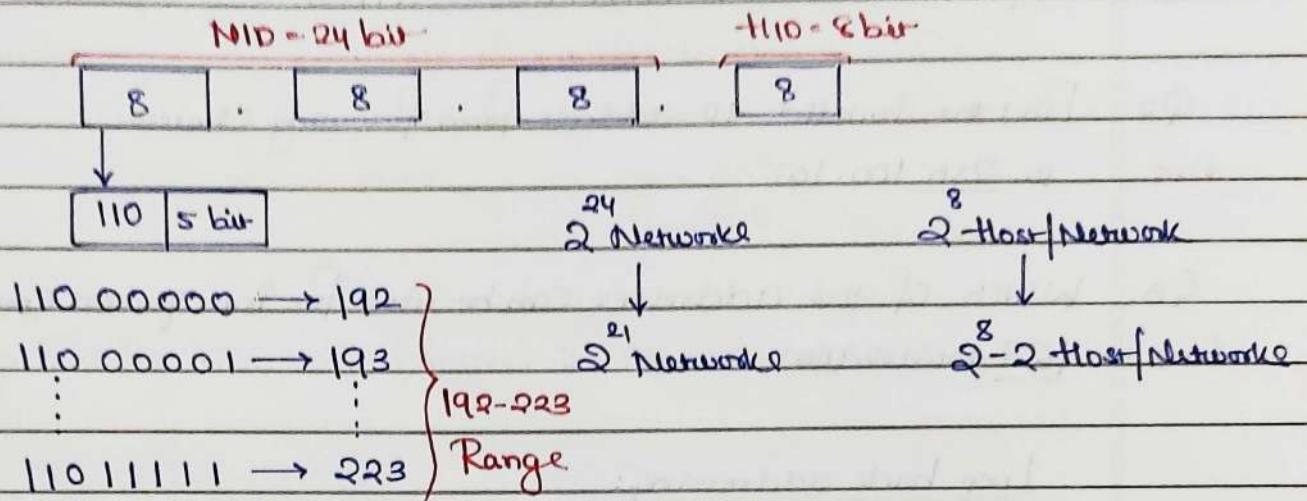
Practical no. of networks in Class A:



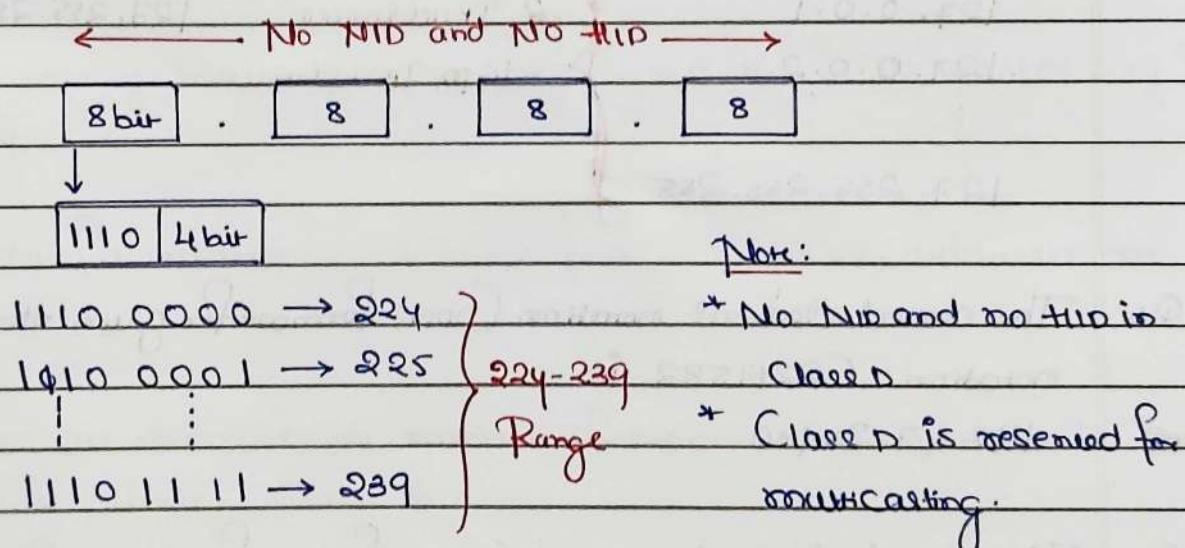
$$\text{Class B} : 10 \rightarrow 2^{29+1=30}$$



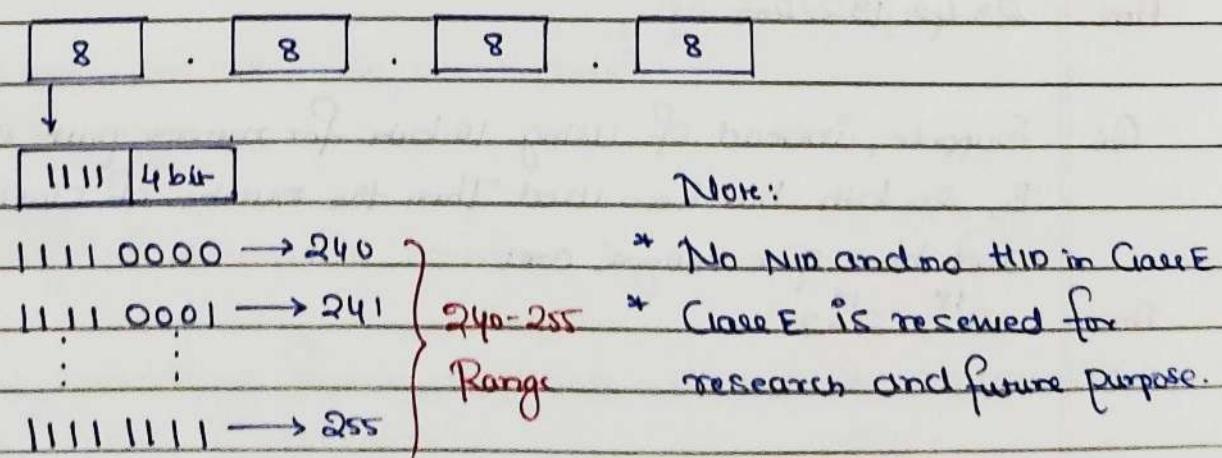
Class C : $110 \rightarrow 2^{29}$



Class D : $1110 \rightarrow 2^{28}$



Class E : $1111 \rightarrow 2^{28}$



Q1. Find the class B address from the following:

Ans: 10001111.00000011.1111100.00111100

Q2. Find the invalid IP address from following choices.

Ans 10.256.100.100

Q3. Which of the addresses can be used for inter process communication

Ans 127.100.100.100

Loop back addressing:

127.0.0.0

127.0.0.1

127.0.0.2

⋮

127.255.255.255

}
2²⁴
= 16 IP addresses

127.0.0.0 ×

127.255.255.255 ×

Q4. The dotted decimal notation (DAN) format for given hexadecimal notation C22F1582 is

Ans 192.47.21.130

Q5. The dotted decimal notation (DAN) format for given hexadecimal notation 172A84C8

Ans 23.42.132.200

Q6. Suppose, instead of using 16 bits for network part of a class B, 20 bits has been used. Then the number of Class B networks and hosts per network are:

Ans $2^{18}, 2^{12}$

Q7. Number of networks and number of hosts in Class B are 2^m ($2^n - 2$) respectively. Then the relation between m and n are:

$$\text{Ans} \quad 8m = 7n$$

$$\text{No. of networks in Class B} = 2^m = 2^{14}$$

$$\text{No. of networks in Class B} = 2^n - 2 = 2^{16} - 2$$

$$m = 14, n = 16$$

$$\frac{m}{n} = \frac{14}{16} = \frac{7}{8}$$

$$8m = 7n$$

Q8. How many networks possible in Class B addressing system?

$$\text{Ans} \quad 2^{14}$$

Q9. How many hosts can be present in Class C?

$$\text{Ans} \quad 2^8 - 2$$

Q10. How many bits are allowed for NID and HID in 23.192.157.234?

$$\text{Ans} \quad 8, 24$$

Q11. In classful addressing a large part of available addresses are wasted

Q12. What are the possible number of networks and addresses in each network under Class B

$$\text{Ans} \quad 2^{14}, 2^{16}$$

$$\text{No. of IP addresses}$$

$$\text{Per network} = 2^{16}$$

$$\text{No. of hosts/Network} = 2^{16} - 2$$

Q13. IP address: 200.198.32.65 which class?

Ans Class C

Q14. Percentage of addressees occupied by class D are 6.25%

Q15. In IPv4 addressing format, the number of networks allowed under Class C address is

$$\text{Ans} \quad 2^8$$

Q16. A host with IP address 10.100.100.100 wants to use loopback testing. What are the source and destination address?

Ans 10.100.100.100 and 127.0.0.1

Class A - 2^7 IP addresses in one Network

Class B - 2^11 IP addresses in one Network

Class C - 2^8 IP addresses in one Network.

Problems in Computer Networks

1. Communication Problem
2. Identification problem
3. Connection problem

1

Communication problems: Communication problems can be solved by using protocols.

A protocol is a set of rules that govern data communication.

Protocol defines:

what is communicated?

how it is communicated?

when it is communicated?

Key elements of Protocols:

1. Syntax: The term Syntax refers to the structure or format of data, meaning the order in which they are presented.

e.g.: Some protocols might accept the first 8 bits of the data to be the address of sender, the second 8 bits to be the address of receiver and rest of the stream to be the message itself.

II. Semantics: The word semantics refers to the meaning of each section of bits.

III. Timing: The term timing refers to two characteristics when data should be sent and how fast they can be sent.
eg:: if a sender produce data at 100 Mbps but receiver can process data at any 1 mbps, the transmission will overload the receiver and some data will be lost.

2) Identification Problem: To send a packet from source to destination, we need 3 identification steps

- Identify the network
- Identify the host within in the network i.e among all computers one computer is identified.
- Identify the process within the host.

Note: Whenever we have all 0's in the two part of any IP address, that IP address represent the IP of entire network, this is the reason we can't assign this IP address to any host (computer).

- Solution for identification of network is IP address or logical address. Now we get destination IP using DNS
- Solution for identification of host within the Network is physical address or MAC address. Given an IP address we get MAC address using ARP (Address resolution protocol).
- Solution for the identification of process within the host is Port Number.

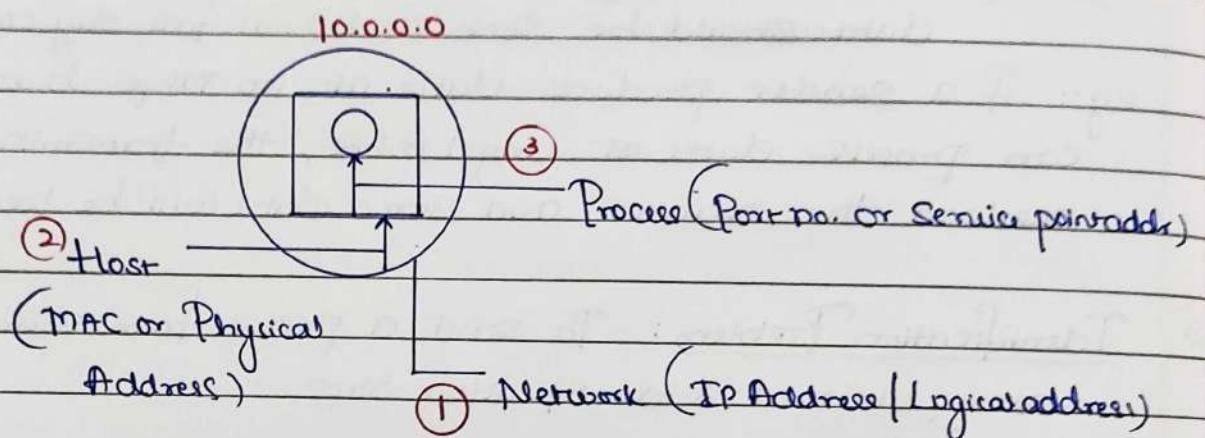
| | IP Addr. | Mac Addr. |
|-------------|-------------|-----------|
| ARP Request | 10.32.15.73 | ? |

* ARP request is broadcasting

* ARP reply is unicasting

| SIP | DIP |
|-----|-------------|
| ? | 10.32.15.73 |

$$\text{NID} = 10 \cdot 0 \cdot 0 \cdot 0$$



3

Connection Problem: There are various ways to connect the system.

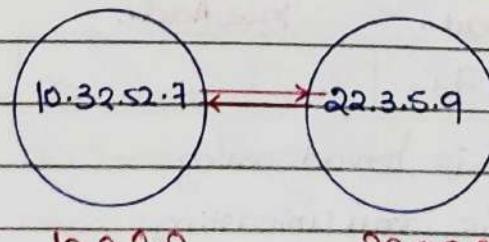
- (i) Bus topology
- (iv) Tree topology
- (ii) Ring topology
- (v) Star topology
- (iii) Mesh topology

Types of Communication

1. Unicast Communication (1 to 1)
2. Broadcast Communication (1 to All)
3. Multicast Communication (1 to many)

Unicast Communication: Transmitting the data from one computer to another computer is called as unicast communication. It is one to one communication.

eg::



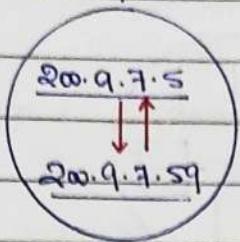
10.0.0.0

22.0.0.0

SIP : 10.32.52.7

DIP : 22.3.5.9 (also vice versa possible)

eg:: 200.9.7.0



Note:

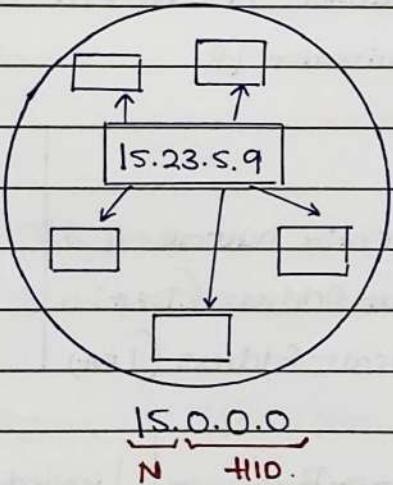
In unicast communication both source and destination can be present in same network or different network.

Broadcast Communication

- ① Limited Broadcasting ② Direct Broadcasting

(i) Limited Broadcasting: Transmitting data from one computer to all other computer in the same network is called as Limited Broadcasting.

eg::



SIP: 15.23.5.9

DIP: 255.255.255.255

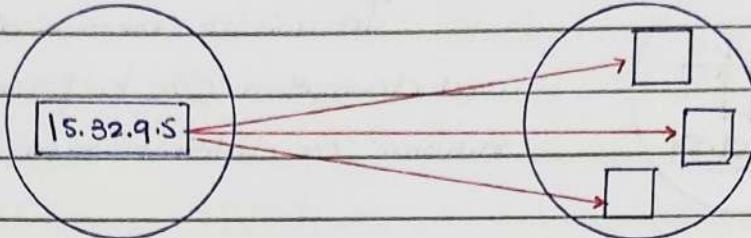
Also called as "Limited Broadcast Address".

* Limited Broadcast Address cannot be used as a Source address

* Limited Broadcast address will always be used as a Destination IP address.

* Doesn't matter the network size and class, in limited broadcasting, the DIP will always be 255.255.255.255.

(ii) Direct Broadcasting: Transmitting the data from one computer to all other computer in the different network is called direct broadcasting.

eg.: 15.0.0.0112.0.0.0

S.I.P - 15.32.9.5

D.I.P - 112.255.255.255

→ all "ones" in the tip part, it represents direct broadcast address.

Note:

- * Whenever we have all 1's in the tip part of any IP address, that IP address represents Direct Broadcast Address, so we don't assign it to any host (computer).
- * Direct Broadcast address Cannot be used as a source, it will be always used as destination IP.

| NID | HID | |
|--------------|---------------------------------------|--|
| Valid | 0's - Network Id of entire network | |
| Valid 1's | 1's - Direct Broadcast Address (DBA) | |
| | 1's - Limited Broadcast Address (LBA) | |

| IP Address | Network Id | Direct Broadcast Address | Limited Broadcast Address |
|---------------|--------------|--------------------------|---------------------------|
| 19.35.21.31 | 19.0.0.0 | 19.255.255.255 | 255.255.255.255 |
| 119.31.34.2 | 119.0.0.0 | 119.255.255.255 | 255.255.255.255 |
| 150.0.94.31 | 150.0.0.0 | 150.0.255.255 | 255.255.255.255 |
| 190.34.17.31 | 190.34.0.0 | 190.34.255.255 | 255.255.255.255 |
| 200.200.34.92 | 200.200.34.0 | 200.200.34.255 | 255.255.255.255 |
| 217.39.47.9 | 217.39.47.0 | 217.39.47.255 | 255.255.255.255 |
| 226.9.7.97 | X | X | X |
| 243.2.3.5 | X | X | X |

Network Mask:

A network mask helps you to know how portions of the address identifies the network-id and which portions of the address identifies the host-id. Class A,B,C networks have default masks, also known as natural masks, as shown here:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

In the network mask, no. of 1's indicate NID part and no. of 0's indicate the HID part.

| NID | HID |
|--|-----|
| Class A: <u>11111111. 00000000. 00000000. 00000000</u> | |
| <u>255.0.0.0</u> | |

| | |
|--|--|
| Class B: <u>11111111. 11111111. 00000000. 00000000</u> | |
| <u>255.255.0.0</u> | |

e.g.: IP Address = 200.200.200.96

Network mask = 255.255.255.0

[NIP: 200.200.200.110-96]

IP Address: 11001000. 11001000. 11001000. 011000000

Anding,

-AND

Net. Mask : 11111111. 11111111. 11111111. 00000000
11001000. 11001000. 11001000. 00000000

NID: 200.200.200.0

Q1. Identify the type of IP address 192.192.192.255

Directed Broadcast Address

Q2. What is the Network ID (NID) of address 230.100.23.70?

(Class D-network, so no Network ID.)

Q3 Which can be valid Class-C network ID?

- Ans b. 200.200.200.0 ✓
- c. 200.0.0.0 ✓
- d. 194.194.194.0 ✓

Q4 100.86.95.75, 157.192.190.253, 200.1.56.97, 10.34.87.95

Which of the following is common for all these IP addresses.

- Ans Limited Broadcast address.

Q5. For the IP address 132.54.78.98 identify the class, and Limited broadcast address.

- Ans The IP address belongs to class B and 180-255.255.255

Q6 One host having IP address 200.187.96.0, send a message to a host with IP address 205.54.83.97, what will be the destination address attached to message by source?

- Ans Not possible

Q7 Which of the following can be used as a source IP as well as destination IP?

- Ans 23.0.0.97

Q8. Which of the following IP address can be given to Computer or a host?

- Ans 157.54.255.254

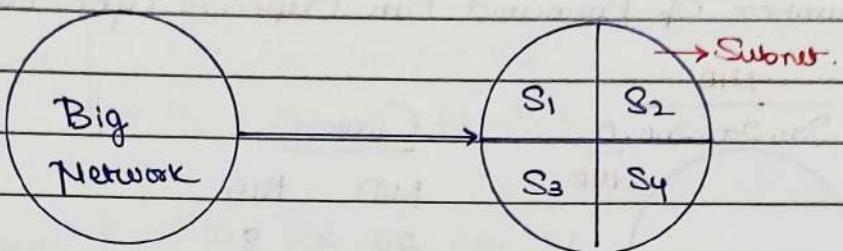
Classful Addressing

Class A : 2^7 IP Addresses in one network

Class B : 2^{14} IP Addresses in one network

Class C : 2^{21} IP Addresses in one network.

Subnetting: The process of dividing a big network into many smaller subnet is called subnetting.



Advantages of Subnetting:

1. Maintenance and administration is simple and easy
2. It provides security to one network from another network

Example: Code of developer department must not be accessed by another department.

Disadvantage of Subnetting:

1. Subnetting Complicates the communication process. Instead of 3 step procedure now it becomes 4 Step Procedure.

Step 1: Identify the network

Step 2: Identify the Subnet within the network

Step 3: Identify the host within the Subnet

Step 4: Identify the process visiting the host.

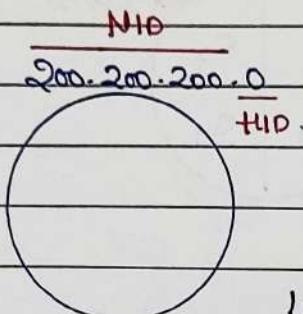
2. In case of single network, Only two IP addresses are wasted to represent Network id and direct broadcast address but in case of subnetting two IP addresses are wasted for each subnet.

3. Cost of overall Network also increase. Subnetting requires internal routers, switches, hub, bridge etc. which are very costly.

4. Subnetting and network management required an experienced network administrator. This adds to the overall cost as well.

Note: * The process of borrowing bits from HID to generate the subnet ID is also called as Subnetting.

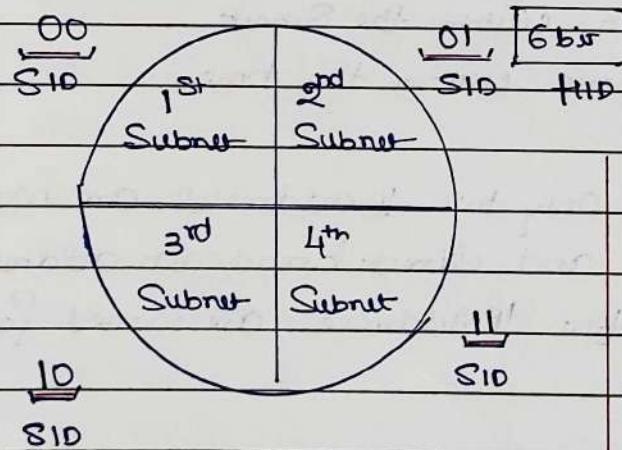
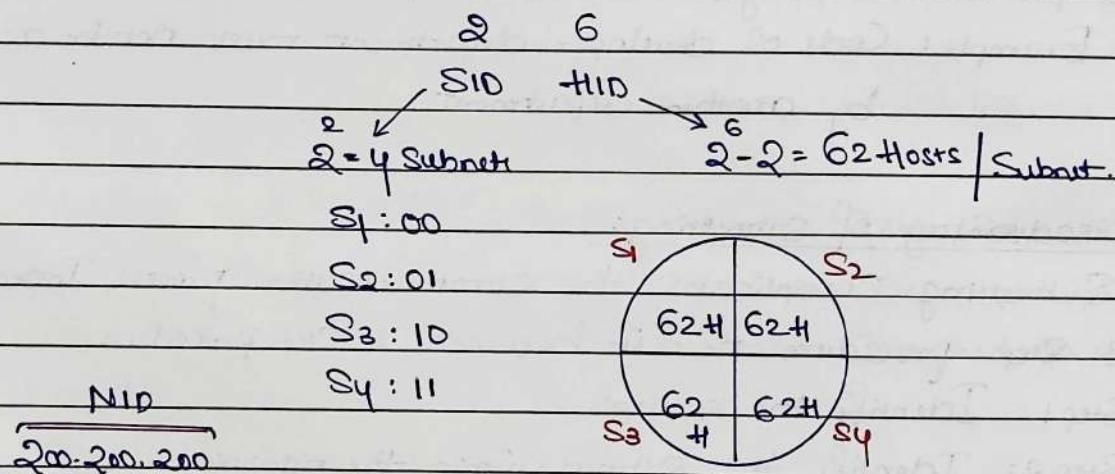
* The number of borrowed bits depends upon the requirement.



Class C

| | |
|-----|-----|
| NID | HID |
| 24 | 8 |

4 Subnets:



1st Subnet

S10 HID

200.200.200.00 6 bits

~~200.200.200.00000000 - 200.200.200.0~~

~~200.200.200.00000001 - 200.200.200.1~~

⋮

~~200.200.200.00111110 - 200.200.200.62~~

~~200.200.200.00111111 - 200.200.200.63~~

Subnet ID: 200.200.200.0

DFA: 200.200.200.63

First Host: 200.200.200.1

Last Host: 200.200.200.62

} Valid hosts from 1-62

1 Subnet. [SID : 200.200.200.0
DBA : 200.200.200.63]

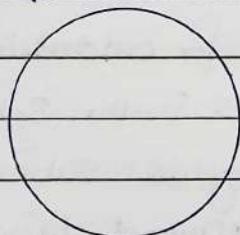
2nd Subnet [SID : 200.200.200.64
DBA : 200.200.200.127]

3rd Subnet [SID : 200.200.200.128
DBA : 200.200.200.191]

4th Subnet [SID : 200.200.200.192
DBA : 200.200.200.255]

e.g.: 2

200.200.200.0



Class C

| | |
|-----|------|
| NID | 1110 |
| 24 | 8 |

8 Subnets

| | |
|-----|------|
| 3 | 5 |
| SID | 1110 |

$$= \frac{8}{2} = \frac{8}{2^3} = 2^S \text{ IP in}$$

one
network

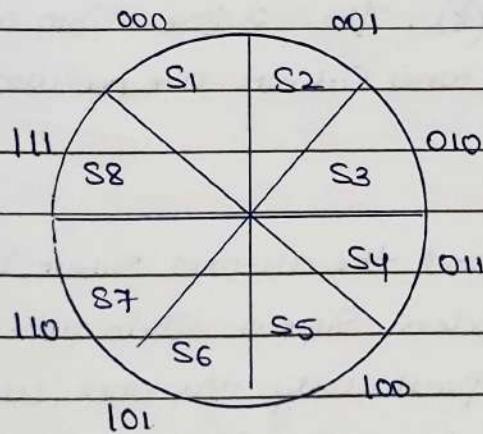
$$\text{Subnet} = 2^3 = 8$$

$$= 2^S - 32$$

no of IP/Subnet

$$= 2^S - 2 = 30$$

no of Host/Subnet



1st Subnet SID : 200.200.200.0

DBA : 200.200.200.31

8th Subnet SID : 200.200.200.224

DBA : 200.200.200.

SID = 3 bit

(decimal value) 0 ← 000 — 1st Subnet
1 ← 001 — 2nd Subnet
⋮
7 ← 111 → 8th Subnet

Subnetting Category 1

Note: In the past, there were limitations to the use of a subnet (all bits are set to 0) and all ones subnet (all subnet bits set to one). Some devices could not allow the use of these subnets.

$$S_{10} = 2 \text{ bit}$$

$\times 00$

01 } valid subnet.

$$\begin{array}{r} 10 \\ \times 11 \\ \hline \end{array} \quad \begin{aligned} \text{No. of Subnets} &= 2^2 - 2 \\ &= 2 \end{aligned}$$

Problem with Subnet zero and the all-ones Subnet:

Traditionally it was strongly recommended that Subnet zero and the all-ones subnets not be used for addressing. This means the values of all zeros and all ones in the subnet field should not be assigned to actual (physical) subnets. This is the reason any network engineer required to calculate the number of subnets obtained by borrowing three bits would calculate $2^3 - 2$ (6) and not 2^3 (8). The -2 takes into account that subnet zero and the all-ones subnets are not used traditionally.

Today, the use of subnet zero and the all-ones subnet is generally accepted and most vendors support their use. However, on certain networks, particularly the ones using legacy software, the use of subnet zero and the all-ones subnet can lead to problems.

Subnetting Category 2

Subnet Mask: It is a 32-bit number used to indicate number of bits borrowed from host-id and three positions were used on the following rules:

- * Rule 1: No. of 1's in the Subnet mask indicate $NID+SID$
- * Rule 2: No. of 0's in the Subnet mask indicate the part

Default Subnet mask:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

For Class A :

255.0.0.0

1111111.00000000.00000000.00000000

$NID+SID = 8$, $11+11=24$

$SID = 0$

Q1. If $NID = 200.200.200.0$ and Subnet mask = 255.255.255.192 then identify:

1. No of bits borrowed from host id: 2

2. No of Subnets possible and their Subnet id: 4

3. No of Host/Subnet: 62

255.255.255.192

200.200.200.0 - Class C

No. of 1's = 26

$NID+SID = 26$, $SID = 2$ bit

No. of Subnet possible = $2^2 = 4$

Hosts/Subnet = $2^6 - 2$

= 62

Subnet id's - 200.200.200.-----

200.200.200.00.00000000 → 200.200.200.0

200.200.200.01.00000000 → 200.200.200.64

200.200.200.10.00000000 → 200.200.200.128

200.200.200.11.00000000 → 200.200.200.192

AD Rule

128 64

00 - 0

01 - 64

10 - 128

11 - 192

Q2. If NID = 200.200.200.0 and Subnet mask = 255.255.224 then identify.

- No of bits borrowed from host ID = 3.
- No. of Subnets possible and their Subnet id's: $2^3 = 8$
- No of Host/Subnet: $2^5 - 2 = 30$

$$S10 = 3 \text{ bit}, \text{ H10} = 5 \text{ bit}$$

Subnet IDs : S10 = 3 bit

128 64 32

| | | |
|-------|-------|--------------------------|
| 0 0 0 | - 0 | Subnet id's (AD rule) |
| 0 0 1 | - 32 | |
| 0 1 0 | - 64 | |
| 0 1 1 | - 96 | |
| 1 0 0 | - 128 | |
| 1 0 1 | - 160 | |
| 1 1 0 | - 192 | |
| 1 1 1 | - 224 | |

Q3. If NID = 200.200.200.0 and the Subnet mask = 255.255.255.44 then identify.

- Number of bits borrowed from host-id = 3
- Number of Subnets possible and their Subnet id's = 8
- Number of Host/Subnet = 30

$$Sm = 1111111.1111111.1111111.00101100$$

$$\text{No. of } 1\text{'s} = 27$$

$$NID + S10 = 27$$

$$S10 = 3, \text{ Subnet} = 2^3 = 8$$

$$\begin{aligned} &\text{Hosts/Subnet} \\ &= 2^5 - 2 = 30 \end{aligned}$$

Subnet id's -

32 8 4

000 - 0

001 - 4

010 - 8

011 - 12

100 - 16 32

101 - 36

110 - 40

111 - 44

Q4 If NID = 200.200.200.0 and the Subnet mask = 255.255.255.252 then identify.

1. No of bits borrowed from Host-id : 3
2. No of Subnet possible and their Subnet ids : 8
3. No of hosts/Subnet : $2^3 - 2 = 6$

Q5. If NID = 173.173.0.0 and the Subnet mask = 255.255.128.128 then identify.

1. Number of bits borrowed from Host-id = 2
2. Number of Subnet possible and their Subnet ids. $= 2^2 = 4$
3. Number of hosts/Subnet = $2^{14} - 2 = 16382$

Subnet-ids :

173.173. ————— . ————— . ————— . —————
 s Host Host

173.173.0.0000000.0000000 — 173.173.0.0

173.173.0.0000001.0000000 — 173.173.0.128

173.173.1.0000000.0.000000 — 173.173.128.0

173.173.1.0000000.1.0000000 — 173.173.128.128

Q6. If NID = 173.173.0.0 and Sm = 255.255.255.0 then identify

1. No of bits borrowed from Host-id = 8
2. No of Subnet possible and their Subnet ids = $2^8 = 256$
3. No of hosts/Subnet = $2^8 - 2 = 254$

Q7. Which of the following is default mask for address 198.0.46.201?

Ans 255.255.255.0

Q8. If a Class B network on Internet has Sm 255.255.248.0 what is maximum no. of hosts/Subnet?

Ans $\text{Host} = 11 \text{ bit}$

$$= 2^{11} - 2 = 2046$$

Q9. A Subnet has assigned a subnet mask of 255.255.255.192
What is max no. of hosts?

Ans $\text{110} = 6 \text{ bits}, 2^6 - 2$
 $= \underline{\underline{62}}$

Q10 If a Class B network on the internet has SM 255.255.255.224
What is max no. of hosts?

Ans $\text{110} = 12 \text{ bits}, 2^{12} - 2$
 $= 4096 - 2 = \underline{\underline{4094}}$

Q11. An organization has a Class B network and wishes to form
Subnets for 64 dep'ts. The subnet mask would be

Ans 64 subnets
 $= 64 = 2^6, \text{ S10} = 6 \text{ bits}$
~~255.255.255.0~~

Q12. Consider default SM = 255.255.255.0 How many no. of hosts
Per subnet Possible if 'm' bits are borrowed from host ID

Ans $2^{\frac{m}{10}} - 2$

Q13. A university has LANs with 100 hosts in each lan. If we
use Class B then the subnet mask in dotted decimal notation
is 255.255.255.128

100 hosts in each lan.

= 7 bits should be two-, remaining 9 bits - S10
~~= 255.255.255.128~~

Q14 A university has 150 LANs, use Class B address and then
the subnet mask in Dotted decimal notation is 255.255.255.0

150 LANs

= 8 bits in two, 8 bit S10
~~= 255.255.255.0~~

Q15 Consider a Class C network with 7 subnets and 25 hosts per subnet. An appropriate subnet mask for this network?

Class C

$$7 \times 25 \leq 2^8 - 2$$

(possible)

for 7 subnets = 3 5

S10 + 110

$$= 2^3 = 8 \text{ subnets}$$

$$2^5 = 32 \text{ hosts/subnet}$$

$$= 256, 256, 256, 224 \quad (\text{first 3 bits borrowed from H10})$$

$$= 256, 256, 256, 7 \quad (\text{if last 3 bits borrowed}) - \text{also possible}$$

* No. of bits can be borrowed from any bit (theoretically)

* Any subnet mask whose subnet mask has 27 1's is correct

Answer

Q16 Consider a Class B network with 180 subnets and 20 hosts per subnet. An appropriate subnet mask for this network?

Class B.

$$180 \times 20 \leq 2^{16} - 2$$

$$36,000 \leq 65,534 \quad (\text{yes})$$

N10 + 110

16 16

$$180 \text{ subnets} \leq 2^8 \cdot (256)$$

8 bits to borrow

S10 + 110

8 8

$$\text{hosts/subnet} = 2^8 = 256$$

No of 1's in Subnet mask = 16 + 8 = 24 { Any Subnet mask with this combination
No of 0's in Subnet mask = 8. } is possible

Q17 Consider a Class C network with 15 subnets and 20 hosts/subnet.

An appropriate mask for this network.

Class C

$$15 \times 20 \leq 2^8 - 2$$

$$300 \leq 254 \quad (\text{Not possible})$$

N10 + 110

24 8. 15 Subnets

4 4

$$S10 + 110; 2^4 - 2 = 14$$

Hosts/Subnet

Q18. Consider a class C network with 3 Subnets and 60, 60, and 120 hosts per subnet. An appropriate subnet mask for this network?

Class C. N10 t10 A - 120

24 8 B - 60

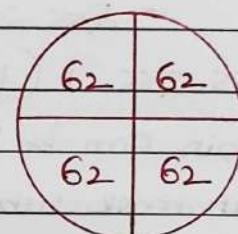
C - 60

$$240 \leq 2^8 \text{ (yes)}$$

Case I for 3 Subnet:

2 6
S10 t10.

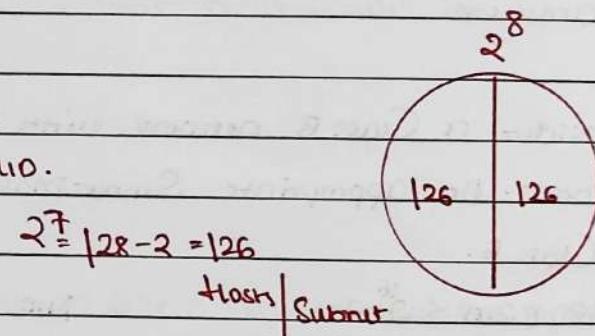
2 4 Subnets. $2^6 = 62$ hosts / subnet
(Not Possible)



Case II N10 t10

24 8 1 7
(S10 t10.)

(Not possible) Subnets.



Note: In both the Case it is not possible here. To solve this problem we use VLSM technique (Subnetting Category-4)

Subnetting Category-4

Q1. Consider a Class C network with 3 Subnets and 60, 60, and 120 hosts per subnet. An appropriate subnet mask for this network?

Class C

N10 t10

24 8

1 7
(S10 t10.)

$2^1 = 2$
Subnet.

t10 - 7

1 G

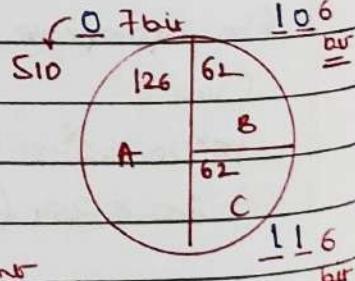
S10 t10.

$2^1 = 2$

Sub.

$$2^6 = 62$$

Hosts / Subnet



$$2^7 - 2 = 126 \text{ Hosts / subnet}$$

(A) SID : - 200.200.200.0

DBA : - 200.200.200.127

Sm : - 255.255.255.128.

(B) SID → 200.200.200.128

DBA → 200.200.200.192

Sm. → 255.255.255.192

C. SID → 200.200.200.192

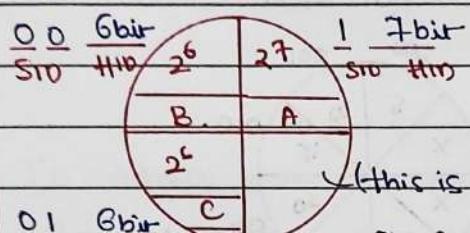
DBA → 200.200.200.255

Sm. → 255.255.255.192.

{ 1st way of finding the Subnets masks of 3 networks. Also Subnet mask of Band C can be replaced (both have same subnet mask).

OR

2



(A) SID → 200.200.200.128

DBA → 200.200.200.255

Sm → 255.255.255.192

(C) SID → 200.200.200.64

DBA → 200.200.200.127

Sm → 255.255.255.192

(B) SID → 200.200.200.0

DBA → 200.200.200.63

Sm → 255.255.255.192

{ Subnets of Band C can be inter changed }

Q2. Consider a Class C network with 4 subnets and 7s, 35, 25, 20 hosts per subnet. An appropriate subnet mask is?

Class C Network

$7s + 35 + 25 + 20 = 1ss \leq 2^8$

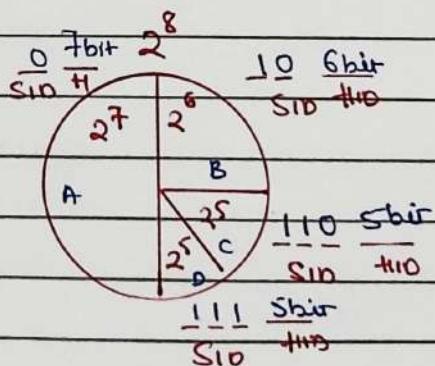
(400 possible)

A → 255.255.255.128

B → 255.255.255.192

C → 255.255.255.224

D → 255.255.255.224.



Q3. Consider a Class C network with 3 subnets and 130, 50, 50 hosts per subnet. An appropriate Subnet mask is?

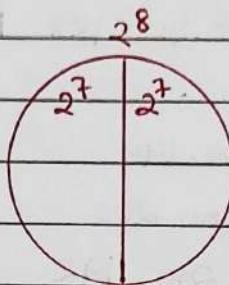
Ans $A = 130$

$$B = 50$$

$$2^{30} \leq 2^8 - 2$$

$$\begin{array}{r} C = 50 \\ \hline 2^{80} \end{array}$$

(possible)



1 bit borrowed

$$2^7 - 2 = 126 < 130$$

So not possible in this case.

Q4. Consider a Class C network with 6 subnets and 5, 10, 15, 20, 25, 30 hosts/subnet. An appropriate subnet mask?

Ans

$$5+10+15+20+25+30$$

$$= 105 \leq 2^8 - 2$$

(possible).

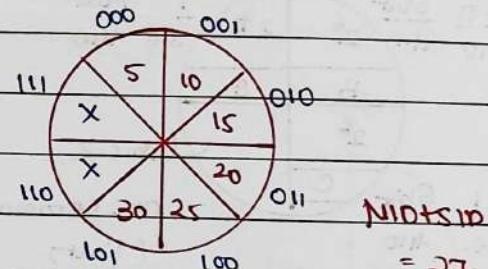
Class C.

6-subnets

$$\begin{array}{c} 3 \\ 5 \\ 10 \\ 15 \\ 20 \\ 25 \\ 30 \end{array} \quad \begin{array}{l} \text{Sub} \\ \text{t10.} \end{array}$$

$$2^3 = 8 \text{ subnets}$$

$$2^2 = 30 \text{ hosts/subnet}$$



Subnet mask = 255.255.255.224 (Binary)

Q5.

An organization is granted a block of address with beginning address 14.24.74.0/24. The organization need to have 3 subblocks of addresses to use in its three subnets: one block of 16 addresses, one subblock of 60 addresses and one sub block of 120 addresses. Find the first and last address of each sub block

Subnetting Category -5

Q1 IP address = 200.200.200.126

Subnet mask = 255.255.255.192 then find SID and HlD?

IP address = 200.200.200.01111110

Subnet mask = 255.255.255.11000000

First way (direct)

SID. +10

SID = 64

HlD = 62 (of IP address).

mark the 8 place, and write.

Another way:

Host Rd = IP address - SID.

HlD = 126 - 64

HlD = 62

=

Q2 IP address = 200.200.200.120

Subnet mask = 255.255.255.240 then find SID and HlD.

3rd way:

IP address : 200.200.200.01110

AND

AND

} 3rd method

Subnet mask : 255.255.255.11110000

200.200.200.01110000

= 200.200.200.112

Q3 IP address = 200.200.200.120

Subnet mask = 255.255.255.41 then find SID and HlD?

IP address : 200.200.200.01111000

AND

AND

Subnet mask : 255.255.255.00101000

200.200.200.00101000

= 200.200.200.40 //

Q4 Find the Subnet address for the following. IP address : 200.34.22.156

Mask : 255.255.255.240.

To address : 200.34.22.111000

AND.

Subnet mask : 255.255.255.11110000

200.34.22.10010000

= 200.34.22.144

Submitting Category - 6

Q1. If Subnet mask is 255.255.255.224 then find:

- (a). No of ip addresses / subnets possible 2^5
- (b). No of host / subnet possible $2^5 - 2$
- (c). No of Subnets in class A 2^{19}
- (d). " " " Class B 2^5
- (e). " " " Class C 2^3

$$255.255.255.224 = 111111.111111.111111.11100000$$

No. of 1s = 27, No. of 0s = 5

$\text{HID} = 5 \text{ bits}$, no of subnets $= 2^5 = 32$

Class A.

Host / subnet $= 2^5 - 2 = 30$

$$\text{NID} + \text{SID} = 27$$

$$\text{SID} = 19,$$

Class B

Class C

$$\text{NID} + \text{SID} = 27$$

$$\text{SID} = 11.$$

$$\text{NID} + \text{SID} = 27$$

$$\text{SID} = 3$$

Q2. If Subnet mask is 255.255.255.240 then find

i) No of IP addresses Possible 2^4

ii) No of Host / Subnet $2^4 - 2$

Ans Rule

iii) No of Subnets in class A 2^0

111111.111111.111111

iv) " " " Class B 2^{12}

11110000

v) " " " Class C 2^4

Q3 If Subnet mask is 255.255.252.0 then find:

No. of IP addresses / Subnet possible 2^{10}

No. of Host/Subnet: 2^{10}

1111111.1111111.111100.0000000

No. of Subnets in Class A 2^4

Only for A, B

" " " Class B 2^6

" " " Class C not possible

Q4 If Subnet mask is 255.252.0.0 then find

No. of IP addresses / Subnet possible 2^{18}

No. of Host/Subnet: 2^{18}

1111111.1111111.00.0.0

No. of Subnets in class A 2^6

A

" " " " Class B N.P

" " " " Class C N.P.

Subnetting Category - 7.

Q1. If DBA is 200.200.200.31 which of the following can be Subnet mask?

Ans Class C - 200.200.200.0001111

this can be last 5 bits | 4 | 3 | 2 | 1 bit also

Correct options:

this can be max 5 bit. ($t10 \leq 5$)

255.255.255.224.

255.255.255.248

255.255.255.282

Q2. Which could be the network mask, if DBA of a network is 168.17.7.255?

Class B - 168.7.00000111.1111111.

this can be maximum 13 bit. ($t10 \leq 11$)

255.255.255.248.0 }

255.255.252.0 } All of the above

255.255.254.0

Q.3. A Subnetted Class B network has the following broadcast address : 144.16.95.255 Its subnet mask.

Ans

Class B. 144.16.0101111.1111111.

-HID can be maximum of 13 bit. ($HID \leq 13$)

255.255.224.0

255.255.240.0

255.255.248.0

Q.4. Given DBA: 125.25.63.255 what can be the mask for this Subnetwork.

Ans

DBA: Class A.

125.00011001.0011111.1111111.

HID Can be maximum 4 bit. ($HID \leq 4$)

255.255.255.192.0 } Broadcast

255.255.224.0 } Correct.

Q.5. If DBA is 200.200.200.3, which of them can be Subnet mask?

Ans

Class C : 200.200.200.0001111

HID Can be maximum 5 bit ($HID \leq 5$)

255.255.255.224 ✓

255.255.255.248 ✓

255.255.255.198. ✗

↳ $HID \leq 5$ but not sequential, so not possible

Q.6. If Subnet mask is 255.255.255.240, then which of them can be DBA.

Ans.

$Sm = 255.255.255.11110000$ $HID = 4$ bit.

No of IP address = 2^4

No of Host/Subnet = $2^4 - 2 = 14$.

200.56.78.31. (last 4 bits are 1) ✓

200.56.78.15. ✓

200.56.78.47 ✓

Submitting Category - 8:

Q1. If Subnet mask is 255.255.255.248, then which of the following can be DBA.

Class C : 255.255.255.1111000

200.32.64.135 ✓

Last 3 bits are the part.

200.32.64.240 ✗

200.32.64.207 ✓

200.32.64.281 ✓

Q2. If Subnet mask is 255.255.240.0, then which of the following can be DBA.

Subnet mask : 255.255.11110000.00000000

Last 12 bits represent the part.

157.157.15.255 ✓

157.157.15.240 ✗

157.157.31.255 ✓

Q3. If Subnet mask is 255.224.0.0 then which of the following can be DBA:

Subnet mask : 255.11100000.00000000.00000000

Last 21 bits represent the

100.31.255.255 ($5+8+8$) ✓

100.63.255.255 ✓

Q4. If Subnet mask is 255.255.255.224, then which of following represent DBA?

Subnet mask = 255.255.255.11100000

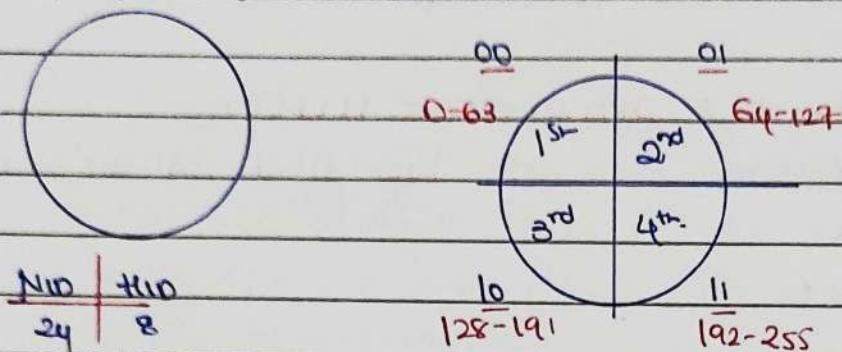
Last 5 bits represent the part.

202.15.19.127 { Both are

202.15.19.63 } correct.

Subnetting Category - 9

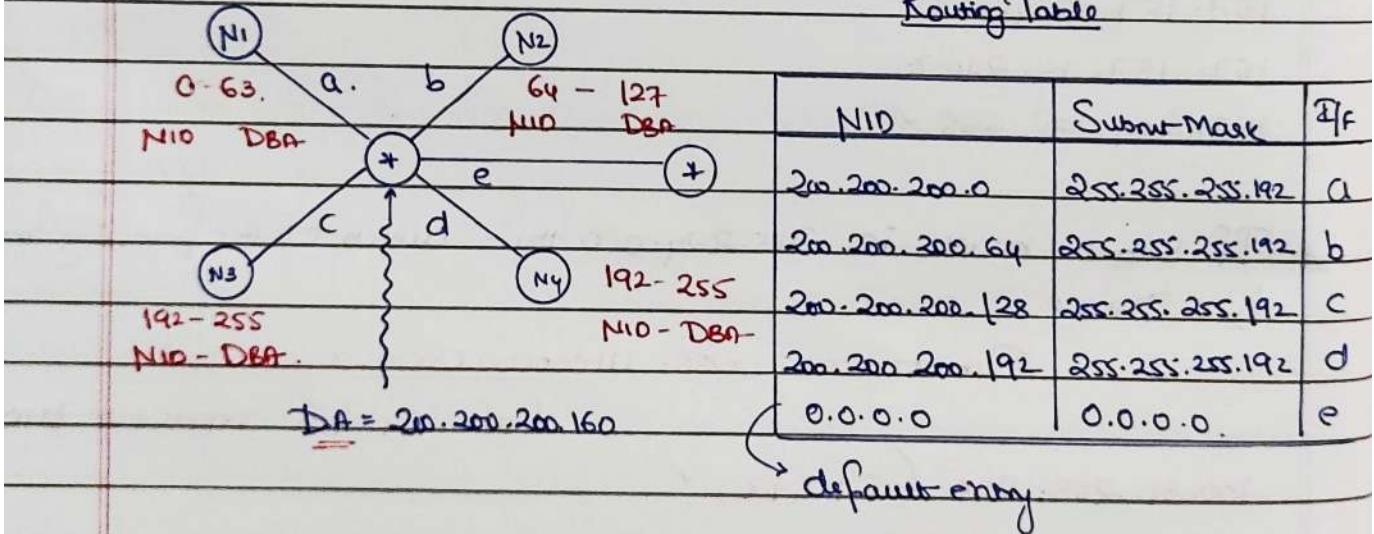
e.g.: 200.200.200.0



4 Subnets

$$\begin{array}{c|c}
 2 & 6 \\
 \hline
 S10 & H10 \\
 \hline
 2^2 = 4 & 2^6 = 62 \text{ Hosts} / \text{Subnet}
 \end{array}$$

Routing Table



Note: If destination IP address matched with more than one interface then router will forward the packet will forward it to the interface with the longer subnet mask.

Q1. The routing table of a router is shown below:

On which interface will router forward packets addressed to destination 128.75.43.16?

| Destination | Subnet Mask | Interface |
|-------------|-----------------|-----------|
| 128.75.43.0 | 255.255.255.0 | Eth0 |
| 128.75.43.0 | 255.255.255.128 | Eth1 ✓ |
| 192.12.17.5 | 255.255.255.255 | Eth3. |
| Default | | Eth2 |

Ans AD rule: first start with longer Subnet.

DIP = 128.75.43.16

AND

SM: 255.255.255.255

128.75.43.16

Not matched with Eth3

DIP: 128.75.43.16

AND

SM: 255.255.255.128

128.75.43.0

Matched with Eth1

Q2. A router uses the following routing table:

| Destination | Mask | Interface | A packet bearing a destination address 144.16.68.117 arrives at router. Which interface will the packet forwarded? |
|--------------|-----------------|-----------|--|
| 144.16.0.0 | 255.255.255.0 | Eth0 | |
| 144.16.64.0 | 255.255.255.0 | Eth1 | |
| 144.16.68.0 | 255.255.255.0 | Eth2 ✓ | |
| 144.16.68.64 | 255.255.255.224 | Eth3 | |

Ans DIP: 144.16.68.117

AND

SM: 255.255.255.224

144.16.68.96

Not matched with Eth3.

144.16.68.17

AND

255.255.255.0

144.16.68.0

Matched with Eth2.

Q3 A forwarding table of a router shown below:

| | | | |
|---------------|-----------------|-----|---|
| 200.150.0.0 | 255.255.255.0 | 1 | A packet with destination address 200.150.68.118 arrives at router and forwarded to interface 3 |
| 200.150.64.0 | 255.255.224.0 | 2 | |
| 200.150.68.0 | 255.255.255.0 | 3 ✓ | |
| 200.150.68.64 | 255.255.255.224 | 4 | |
| Default | | 0 | |

Ans

DIP: 200.150.68.118

AND

Sm: 255.255.255.254

200.150.68.96

(Not matched with I·4)

DIP: 200.150.68.118

AND

Sm: 255.255.255.0

200.150.68.0

(Matched with interface 3)

- Q4. An IP router implementing Classless Interdomain routing (CIDR) receives a packet with address 131.23.151.76. The router table has following entries.

| Prefix | Sm | Output Int. Index | The identifier on the output interface on which packet will be forwarded in <u>1</u> . |
|---------------|-------------|-------------------|--|
| 131.16.0.0/12 | 255.240.0.0 | 3 | |
| 131.25.0.0/14 | 255.252.0.0 | 5 | |
| 131.19.0.0/16 | 255.255.0.0 | 2 | |
| 131.22.0.0/15 | 255.254.0.0 | 1 ✓ | |

Ans

Start with the longest Subnet mask,

DIP: 131.23.151.76

AND

Sm: 255.255.0.0

131.23.0.0

(not matched with int.(2))

DIP: 131.23.151.76

AND

Sm: 255.254.0.0

131.22.0.0

(Matched with interface (1))

Subnetting Category - 10

- * If $NID_{AA} = NID_{BA}$ then A assumes that B is present in the same network.
- * If $NID_{AA} \neq NID_{BA}$ then A assumes that B is present in different network.

eg: A. $IP_A = 200.200.200.15$ B. $IP_B = 200.200.200.132$, $Sm_B = 255.255.255.128$. $NID_A = 200.200.200.0$

IP.B = 200.200.200.132

Ans.

IP.A Sm.A = 255.255.255.128

NID.BA = 200.200.200.128.

$NID_{AA} \neq NID_{BA}$ so 'A' assume
that 'B' is present in different
network.

eg:: 2. A

IP.A = 200.200.200.15 (Ans)

Sm.A = 255.255.255.128.

NID.AA = 200.200.200.0

B.

IP.B = 200.200.200.66 (Ans)

Sm.B = 255.255.255.192

NID.BB = 200.200.200.64,

IP.B = 200.200.200.66 (Ans)

Sm.A = 255.255.255.128

NID.BA = 200.200.200.0.

* $NID_{AA} = NID_{BA} = 20.200.200.0$

then A assume that B is present
in same network.

IP.A = 200.200.200.15

(Ans)

Sm.B = 255.255.255.192

NID.AB = 200.200.200.0.

* $NID_{BB} \neq NID_{AB}$ so 'B' assume

that 'A' is present in different
network.

eg:: 3. A.

IP.A = 200.200.200.15

Sm.A = 255.255.255.128.

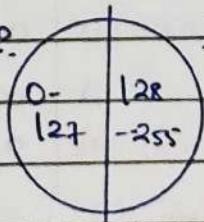
NID = 255.255.255. 10000000
Sub. H10.

NID Sub H10

2⁴, 1, 7 → 2⁷⁻²⁼⁵=32

2²=2 Subnets. Host/Cubnet.

0 H10.



1 H10.

B.

IP.B = 200.200.200.66

Sm.B = 255.255.255.192

NID = 20.200.200.64 [01000000]
Sub. H10.

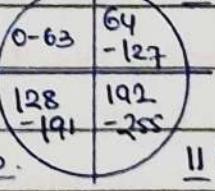
NID Sub H10

2⁴, 2, 6, 2⁶⁻²⁼⁶=64 Host/Cubnet

2²=4 Subnets.

00 H10

01 H10



01 H10

11 H10

Q1. Two computers C₁ and C₂ are configured as follows. C₁ has IP address 203.197.2.53 and mask 255.255.128.0. C₂ has IP address 203.197.75.201 and mask 255.255.192.0. Which one of following statements is true?

Ans

C₁IP.C₁ = 203.197.2.53. (Anding)Mask.C₁ = 255.255.128.0.NID.C_{1,C} = 203.197.0.0C₂IP.C₂ = 203.197.75.201Sm.C₂ = 255.255.192.0NID.C_{2,C} = 203.197.64.0IP.C₂ = 203.197.75.201 (Anding) TPC₁ = 203.197.2.53Sm.C₁ = 255.255.128.0NID.C₁ = 203.197.0.0Sm.C₂ = 255.255.192.0NID.C₂ = 203.197.0.0* NID.C_{1,C} = NID.C_{2,C}, so C₁Assume C₂ present in same network ✓* NID.C_{2,C} ≠ NID.C_{1,C}, so C₂ assumeC₁ is present in different network ✓

Problem Solving on Subnetting:

Q1. If subnet mask is 255.255.224 then no. of subnets are

Ans 2¹, 2².

Q2. If subnet mask is 255.255.255.192 then no. of subnets are

Ans 2¹⁸, 2¹⁰, 2².

Q3. IP address in a block = 200.200.200.60 and the subnet mask = 255.255.255.224 then find

(i) Subnet id = 200.200.200.32 (common in both)

(ii) Subnet number = 2nd.200.200.200. 00111100

(Sub. 3bit)

Value = 3 so 2nd Subnet0 | 000 - 1st Subnet -1 | 001 - 2nd Subnet -2 | 010 - 3rd Subnet -

Q4 IP address in a block = 200.200.200.80 and the Subnet mask = 255.255.255.224
then find

- | | |
|---|---|
| (i) Subnet id = 200.200.200.64 | $S_m = 255.255.255.224 \quad (128+64+32)$ |
| (ii) Subnet number = 3 rd subnet | $80 \quad (64+16) \rightarrow 64$ |
| 200.200.200. <u>01000000</u> | |
| (decimal value = 2, (3 rd subnet)) | |

Q5 IP address in a block = 200.200.200.128 and $S_m = 255.255.255.240$
then find

- | | |
|--|--|
| (i) Subnet id = 200.200.200.112 | $S_m = 255.255.255.240$ |
| (ii) Subnet number = 8 th subnet. | <u>11100000</u> SID. |
| 200.200.200. <u>01110000</u> | - decimal value = 7 (8 th subnet) |

Q6 IP address in a block = 157.157.52.80 then Subnet mask = 255.255.224.0
then find:

- | | |
|----------------------------------|----------------------|
| (i) Subnet id = 157.157.32.0 | $157.157.52.80$ |
| (ii) First host = 157.157.32.1 | $255.255.1110000.0$ |
| (iii) Last host = 157.157.63.254 | $(128+64+32)$ |
| (iv) DBA = 157.157.63.255 | $SID = 157.157.32.0$ |

157.157.00100000.0000000 → 157.157.32.0 (SID)

157.157.00100000.0000001 → 157.157.32.1. (First Host)

:

157.157.0011111.1111110 → 157.157.63.254 (Last Host)

157.157.0011111.1111111 → 157.157.63.255 (DBA)

Q7. IP address in a block = 157.157.52.80 and the $S_m = 255.255.192.0$
then find

- | | |
|------------------------------|----------------------------|
| (i) Subnet id: 157.157.0.0 | $157.157.52.80$ |
| (ii) First host: 157.157.0.1 | $255.255.11000000.0000000$ |
| $SID = 157.157.0.0$ | |

(iii) Last host: 157.157.63.254

(iv) DBA: 157.157.63.255

$157 \cdot 157 \cdot 00 \cdot 00000 \cdot 0 \rightarrow 157 \cdot 157 \cdot 0 \cdot 0$ (S10)

$157 \cdot 157 \cdot 00 \cdot 010000 \cdot 0000000 \rightarrow 157 \cdot 157 \cdot 0 \cdot 1$ (first)

$157 \cdot 157 \cdot 0011111 \cdot 1111110 \rightarrow 157 \cdot 157 \cdot 63 \cdot 254$ (last host)

$157 \cdot 157 \cdot 0011111 \cdot 111111 \rightarrow 157 \cdot 157 \cdot 63 \cdot 255$ (DBA)

Q9. IP address in a block = 200.200.200.90 and the subnet mask is 255.255.255.224 then find:

(i) 3rd Subnet id: 255.255.255.64

(ii) 7th Subnet id: 255.255.255.192.

$$Sm = 255 \cdot 255 \cdot 255 \cdot \underline{11100000}$$

S10 - 3 bits.

3rd subnet, so decimal value should be $2^3 = 255 \cdot 255 \cdot 255 \cdot 01000000$
 $= 255 \cdot 255 \cdot 255 \cdot 64$.

7th Subnet, decimal $\rightarrow 6 = 255 \cdot 255 \cdot 255 \cdot 110 \cdot 0000 \cdot 00000000$
 $= 255 \cdot 255 \cdot 255 \cdot 192$

Q10. IP address in a block = 200.200.200.90 and the subnet mask = 255.255.255.240 then find

(i) 4th Subnet id = 200.200.200.48 Sm: 255.255.255.11100000

(ii) 6th Subnet id = 200.200.200.80 S10.

$$4^{\text{th}} \text{ Subnet} = 0011$$

$$6^{\text{th}} \text{ Subnet} = 0101$$

Q1. IP address in a block = 125.200.100.90 and the subnet mask = 255.252.0.0 then find:

(i) 3rd host in 2nd Subnet: 125.4.0.3

(ii) 4th host in 3rd Subnet: 125.8.0.4

(iii) 1st host in 4th Subnet: 125.12.0.1

Ans

255. 11111100. 00000000. 00000000
S10. T10.

2nd Subnet. 3rd host: 255. 00000100. 00000000. 00000111
= 125.4.0.3

4th host in 3rd Subnet: 125. 00001000. 00000000. 00000100
= 125.16.0.4

1st host in 4th Subnet: 125. 00001100. 00000000. 00000001
= 125.12.0.1

Q2. IP address in a block = 157.157.100.90 and the subnet mask = 255.255.224.0 then find

i. 3rd host in 2nd Subnet = 157.157.64.3.

ii. 4th host in 3rd Subnet = 157.157.64.4

iii. 1st host in 4th Subnet = 157.157.128.1

Ans

Sm = 255.255. 11100000. 00000000

S10. 2nd Subnet → dec value (1). then

calculate.

H.W

Q3. IP address in a block = 200.200.200.90 and the subnet mask

= 255.255.255.240 then find

(i) 3rd host in 2nd Subnet :

(ii) 4th host in 3rd Subnet :

(iii) 1st host in 4th Subnet :

Sm: 255.255.255. 11110000

S10.

Q4. Consider the three machines M, N and P with IP addresses 157.157.38.90, 157.157.48.90 and 157.157.68.90 respectively. The Subnet mask is set to 255.255.192.0 for all the three machines. Which of the following is true?

Ans

$$Sm = 255.255.110000000.00000000$$

$$M = 157.157.38.90 \quad \text{Check for 3rd octet SID part.}$$

$$N = 157.157.48.90 \quad M : 38 \quad 00100110 \rightarrow M, N belong to$$

$$P = 157.157.68.90 \quad N : 48 \quad 00110000 \quad \text{Same subnet.}$$

$$P : 68 \quad 01000100 \quad (\text{Same bits in SID})$$

$\therefore M$ and N belong to same network.

Q5. Consider three machines with M, N and P with IP addresses 157.157.38.90, 157.157.48.90 and 157.157.68.90 respectively. The Subnet mask is 255.255.240.0 for all three machines.

Ans

$$Sm = 255.255.11100000.0$$

SID.

128 64 32 16

$$\text{AD Rule: } M : 38 : 0010 \quad \left. \begin{array}{l} M, N, P \text{ belong} \\ \text{to 3 diff} \end{array} \right\}$$

$$N : 48 : 0011$$

$$P : 68 : 0100 \quad \left. \begin{array}{l} \text{Subnet} \end{array} \right\}$$

Q6. Consider three machines with M, N, P with IP addresses 100.40.38.90, 100.92.48.90 and 100.80.68.90 respectively. The Subnet mask is set to 255.224.0.0 for all three machines.

$$Sm = 255.11100000.0.0$$

$$\text{AD Rule: } 40 : 001$$

$$48 : 010 \quad \left. \begin{array}{l} N \text{ and } P \text{ belong to same network} \\ 68 : 010. \end{array} \right\}$$

Q7. Consider three machines M, N, and P with IP addresses 200.40.38.50, 200.92.48.40, 200.80.68.60 respectively. The Subnet mask = 255.255.255.224. Then find

which host of which subnet?

$$Sm = 255.255.255. \underline{11100000} / \text{SID.}$$

Ans.

$$M: 200.40.38. \underline{00110010}$$

$$\begin{array}{ccc} \downarrow & \downarrow \\ \text{d.value} & \text{d.value.} \\ = 1. & 18 \\ (\text{2}^{\text{nd}} \text{sub}) & (\text{18}^{\text{th}} \text{host}) \end{array}$$

$$N: 200.92.48. \underline{00101000}$$

$$1 \rightarrow (\text{2}^{\text{nd}} \text{subnet}), \text{HID} = 8 \rightarrow 8^{\text{th}} \text{host.}$$

$$P: 200.80.68. \underline{00100010}$$

$$2 \rightarrow (\text{3}^{\text{rd}} \text{subnet}) \quad 1 \rightarrow (\text{2}^{\text{nd}} \text{subnet}), \text{HID} = 28, 28^{\text{th}} \text{host.}$$

HW

Q8. Consider three machines M, N and P with IP addresses

157.157.40.50, 157.157.48.40, 157.157.80.60 and Subnet mask is 255.255.252.0 then find which host of which subnet.

$$Sm = 255.255. \underline{1111100.00000000} / \text{SID.}$$

$$M: 157.157. \underline{00101000} \cdot \underline{00110010}, \text{d.value} = 50 \quad (50^{\text{th}} \text{host}) \\ (\text{d.value} = 10 \quad (10^{\text{th}} \text{subnet}))$$

N:

P:

Q9. Consider three machines M, N and P with IP addresses

HW 100.40.0.10, 100.96.0.22, 200.80.0.15, Subnet mask = 255.255.0.0 find which host of which subnet.

Q10. Consider three machines M, N and P with IP addresses 100.10.5.2, 100.10.5.5, and 100.5.6 respectively. The subnet mask is 255.255.255.252 for all the three machines.

$$SM = 255.255.255.1111100$$

$$M: 2 = 000000$$

$$\begin{array}{l} N: 5 = 000001 \\ P: 6 = 000001 \end{array} \quad \left. \begin{array}{l} N \text{ and } P \text{ belong to same subnet} \\ \end{array} \right.$$

Problem Solving part-3

Q1. The subnet mask for a particular network is 255.255.31.0 which of the following pairs of IP addresses could belong to this network.

Ans

$$\text{Option (d)} \quad 128.8.129.43$$

AND

$$255.255.31.0$$

$$128.8.161.55$$

AND

$$255.255.31.0$$

$$NID = 128.8.1.0 \checkmark$$

$$128.8.1.0 \checkmark$$

Q2 Suppose Computers A and B have IP addresses 10.105.1.13 and 10.105.1.91 respectively and they both use the same subnet N. Which of the values of N given below should not be used if A and B belong to same network?

Ans.

$$113.$$

$$91.$$

AND . 224.

AND with 224

$$NID = 96$$

$$NID = 64$$

$$\therefore 255.255.255.224$$

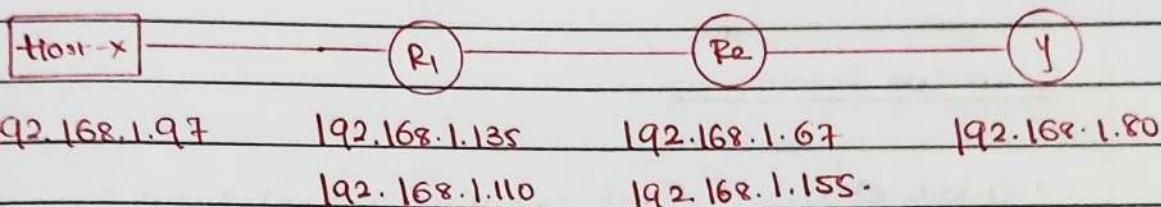
Q3. The address of a Class B host is to be split into subnets with a 6-bit subnet number. What is the maximum number of subnets and the maximum number of hosts in each subnet? [GATE 2007]

Ans 62 Subnets and 1022 hosts as per RFC-950. (but later \rightarrow 64 subnets)

Q4. Host X has IP address 192.168.1.97 and is connected through two routers R₁ and R₂ to another host Y with IP address 192.168.1.80. Router R₁ has IP address 192.168.1.135 and 192.168.1.110. R₂ has IP address 192.168.1.67 and 192.168.1.155. The netmask used in the network is 255.255.255.224. Given the information above, how many distinct Subnets are guaranteed to already exist in the network?

Ans.

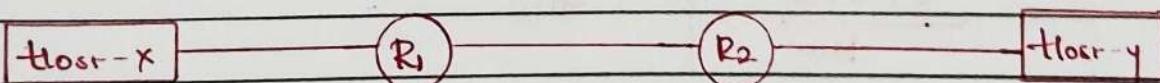
Network mask = 255.255.255.224.



| | | | | | | | |
|-------|------|------|-----|-----|-----|-----|---------------------------|
| (Ans) | 97. | 135 | 110 | 67 | 155 | 80. | { So 3 distinct Subnet |
| | 224. | 224 | 224 | 224 | 224 | 224 | |
| | 96 | 128. | 96 | 64. | 128 | 64 | |

Q5. Host X has IP address 192.168.1.97 is connected through two routers R₁ and R₂ to another host Y with IP address 192.168.1.80. Router R₁ has IP addresses 192.168.1.135 and 192.168.1.110. R₂ has IP address 192.168.1.67 and 192.168.1.155. The netmask used in the network is 255.255.255.224.

Which IP address should X configure its gateway as?



(b) 192.168.1.110.

Ans.

255.255.255.224

192.168.1.96

Disadvantage of Classful Addressing:

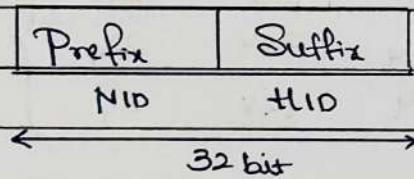
1. Waistage of IP addresses
2. Class C was generally more used (compared) to Class A and Class B

Advantages of Classful Addressing:

1. Easily determine the class of the IP address and the network ID and host ID present.

Classless Addressing:

→ a.b.c.d/n. (CIDR notation or Slash notation)
n → NID or Subnet mask.



e.g.: 10.32.96.64/20

$$\text{NID} = 22 \text{ bit}, \text{ HID} = 32 - 22 = 10 \text{ bit}$$

$$\text{No. of IP addresses possible} = 2^{10}$$

$$\text{No. of hosts possible} = 2^{10} - 2$$

| | |
|-----------------------------------|-----|
| 10.32.01011110.01000000, 8+8+6 | HID |
| NID | |

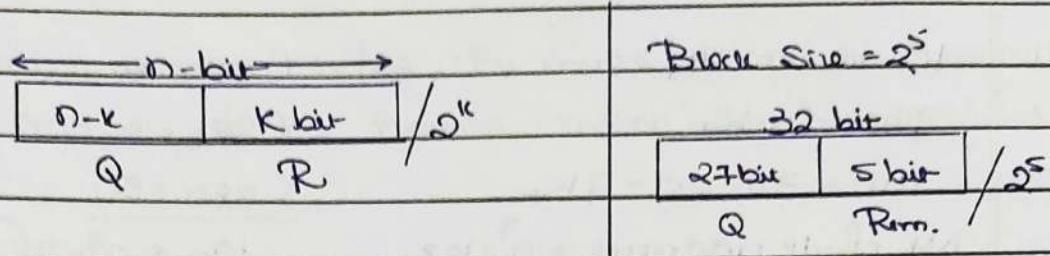
CIDR (Classless Inter Domain Routing)

Whenever any customer wants a block of IP address, BANCA or ISP will create the block assigned to customer.

Rules to be followed by BANCA for creating the block:

1. All the IP addresses in the block must be contiguous.

2. Block Size must be a power of 2



3. First IP address of the Block must be divisible by the size of the block

Note: First IP address must be used as a block-id

e.g.: One of the address of the Block is 100.100.100.64 | 27 thus find

1. Number of addresses in a block : 2^5 . NID = 27 bit

2. Range of IP Address : $2^{27-5} = 32 \times 2^5 = 512$

100.100.100.01000100
8+8+8+3, NID 5.
100.100.100.01000100

100.100.100.010.00000 } Block id
100.100.100.010.00001 } Range
100.100.100.010.11111 } DBA.

3. Blockid / Networkid : 100.100.100.64

4. First host : 100.100.100.65

5. Last host : 100.100.100.95

6. DBA : 100.100.100.96

e.g.: One of the address of the Block is given as 167.199.128.3 | 20, Find.

1. Number of addresses in a block = 2^{12} .

2. Range of IP Address : 167.199.100.0000000000 - 168.199.128.0

3. Networkid and DBA

= 168.199.128.0, 168.199.143.255

4. First and lasthost

= 168.199.128.1, 168.199.143.254

167.199.100.0000000001 - 168.199.128.1

167.199.100.0000000010 - 168.199.143.254

167.199.100.0000000011 - 168.199.143.255

VLSM in CIDR

1. 100.100.100.14 / 25

NID = 25 bit

HID = $32 - 25 = 7$ bitNo. of IP addresses = $2^7 = 128$ No. of Host = $2^7 - 2 = 126$

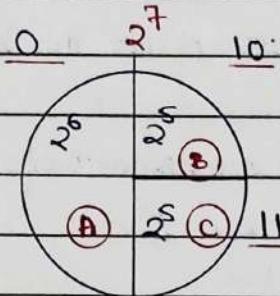
100.100.100.0 00001110

↳ NID = 25. ↳ HID = 7 bit

CSEA = 60

CSEB = 30

CSEC = 80

 $120 \leq 2^8 - 2$ (Yes)

CSEA: S10: 100.100.100.0 / 26

DBA: 100.100.100.63 / 26

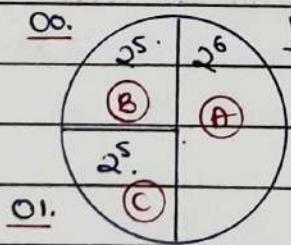
CSEB: S10: 100.100.100.64 / 27

DBA: 100.100.100.95 / 27

CSEC = S10: 100.100.100.96 / 27

DBA: 100.100.100.127 / 27.

* B and C are interchangeable.

(2nd way)(3rd way)

A: S10: 100.100.100.64 / 26

DBA: 100.100.100.127 / 26

B: S10: 100.100.100.0 / 27

DBA: 100.100.100.31 / 27

C: S10: 100.100.100.32 / 27

DBA: 100.100.100.63 / 27

* B and C are interchangeable (4th way)

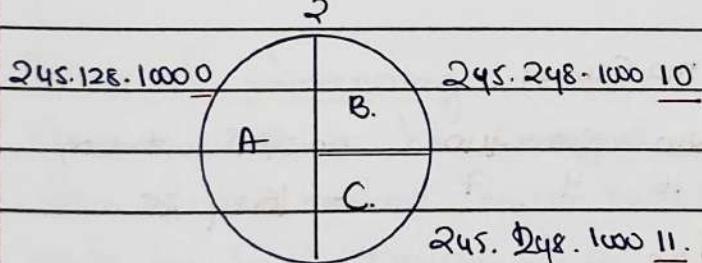
Problem Solving on Classless Addressing

Q1. In the network 200.10.11.144/27, the fourth octet (in decimal) of last IP address of the network which can be assigned to a host is 158.

Ans. 200.10.11.1001000 200.10.11.100
NID = 27, Sub = 5 bits 200.10.11.100 11110
158 (last host)

Q2. An internet Service provider has following chunk of CIDR based IP addresses available with it: 245.248.128.0/20. The ISP wants to give half of the chunk of addresses to organization A, and a quarter to Organization B, while retaining the remaining with itself. Which of the following is a valid allocation for A and B?

Ans. 245.248.1000 0 NID: Sub = 11 bits no. of IP addresses = $2^{12} = 4096$
245.128.1000 0 SID: Sub = 11 bits no. of hosts = $2^{12} - 2 = 4094$



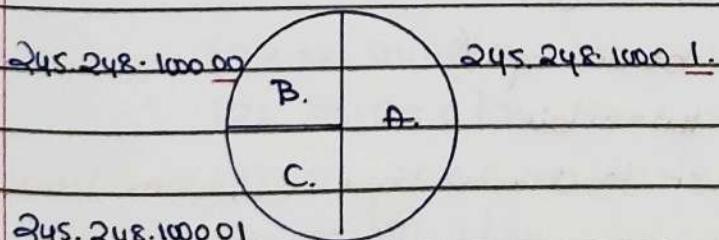
A: 245.248.128.0/21

B: (SID) 245.248.136.0/22

or

245.248.140.0/22

or



A: (SID) 245.248.136.0/21

B: (SID) 245.248.128.0/22

or

245.248.132.0/22

Q3. In IPv4 match the corresponding host IP address with their network ID.

| List 1 (NID) | List 2 (Host IP) |
|------------------|----------------------|
| P. 203.207.208.0 | 1. 203.207.175.45/20 |
| Q. 203.207.160.0 | 2. 203.207.190.37/20 |
| R. 203.207.176.0 | 3. 203.207.210.42/20 |

Ans 1) 203.207.175.45/20

$$\text{NID} = 20 \text{ bit}, \text{ HID} = 12 \text{ bit}$$

203.207.1010

\rightarrow 203.207.160.0 NID

2) 203.207.1011

203.207.10110000.00000000

= 203.207.176.0

3) 203.207.11010000.00000000

= 203.207.208.0

Q4. An organisation is granted the block 156.36.0.0/16. The administrator want to create 512 Subnets. What is the subnet mask?

Ans 156.36.0.0/16

NID HID
16 16

512 Subnets

NID. SID + HID no of 1's in the SM
16 9 7 = 16+9=25

= 255.255.255.128/25

Q5. Block contains 64 IP address. Which of the following can be first address of the block:

No of address in the block = $64 = 2^6$

Block size = 2^6 , HID = 6 bit

First IP address must be divisible by size of the block
= 200.50.60.192.

Q6. Block contains 16 IP addresses, which of the following can be first address of the block?

Ans 199.16.16.0

199.16.16.160

Q8 Which of the following would support best point-to-point link?

Supernetting: The process of combining two or more networks to get a single network is called as Supernetting, also called as "Aggregation".

Advantages of Supernetting:

- * Supernetting reduces routing table entry
- * Router can take less time for processing the packet
- * It improves flexibility of IP address allocation. If someone required 5000 addresses then we have no need to purchase Class B network we can combine ten Class C network.

Rules of Supernetting:

1. Network ID must be contiguous
2. Size of the network must be same and number of networks must be in a power of 2.
3. First network ID must be divisible by the total size of the SuperNet.

e.g.: 1. 128.56.24.0/24 NID = 24 bit, HID = 2^8 IP

128.56.25.0/24 NID = 24 bit, HID = 8 bit, 2^8 IP

128.56.26.0/24 NID = 24 bit, HID = 8 bit

128.56.27.0/24 NID = 24 bit, HID = 8 bit.

1. Network ID must be contiguous

N1: 128.56.24.0000000 → 128.56.24.0

128.56.24.0000001 → 128.56.24.1

$128 \cdot 56 \cdot 24 \cdot 00000010 \rightarrow 128 \cdot 56 \cdot 24 \cdot 2$

$128 \cdot 56 \cdot 24 \cdot 1111111 \rightarrow 128 \cdot 56 \cdot 24 \cdot 255$

+ 1

128.56.25.0

N2: 128.56.25.0

$128 \cdot 56 \cdot 25 \cdot 00000000 \rightarrow 128 \cdot 56 \cdot 25 \cdot 00000000$

$128 \cdot 56 \cdot 25 \cdot 00000001 \rightarrow 128 \cdot 56 \cdot 25 \cdot 1$

|

$128 \cdot 56 \cdot 25 \cdot 1111111 \rightarrow 128 \cdot 56 \cdot 25 \cdot 255$

+ 1

128.56.25.255 + 1

128.56.26.0 ↳

N3: 128.56.26.0

$128 \cdot 56 \cdot 26 \cdot 255 + 1$

= 128.56.27.0

N4: 128.56.27.0

$128 \cdot 56 \cdot 27 \cdot 255 + 1$

= 128.56.28.0

∴ Network IDs are Contiguous

2. Size of the network must be same and no. of networks must be in power of 2.

: Some Size = 2^8 , no. of networks = $4 = 2^2$.

3. First Network ID must be divisible by total size of the Supernet.

→ Total size of the Supernet = $2^8 + 2^8 + 2^8 + 2^8 = 2^{10}$.

128.56.24.0

= 128.56.00011000.00000000 (true)

REM.

Supernet Mask: It is a 32 bit number used to generate a single IP address for the group of network based on the following two rules.

Rule 1: No of 1's in the Supernet mask denotes fixed part.

Rule 2: No of 0's in the Supernet mask denotes Variable part.

e.g.: N₁: 128.56.24.0/24

N₂: 128.56.25.0/24

N₃: 128.56.26.0/24

N₄: 128.56.27.0/24

10000000. 00111000. 00011000. 00000000

10000000. 00111000. 00011001. 00000000

10000000. 00111000. 00011010. 00000000

10000000. 00111000. 00011011. 00000000.

Fixed.

Variable. Variable

Supernet mask

= 255.255.255.252.0

11111111. 11111111. 11111100. 00000000.

Answe:

Supernet id: First IP address Always

Supernet id = 128.56.24.0

Answe for Subnet mask

Total size of Supernet = 2^8

= 2¹⁰

Hence = 10 bit

NID = 32 - 10 = 22.

Supernet mask = 255.255.255.252.0

Problem Solving on Supernetting:

Q1. Perform Class aggregation on the following IP addresses

57.6.96.0/21

57.6.104.0/21

57.6.112.0/21

57.6.120.0/21

- Ans
- $110 = 11$ bit of an IP address.
 - Network Id is contiguous.
 - no of networks = $4 = 2^2$
 - First NID must be divisible by the size of Supernet.
- $$2 \times 4 = 2^{13}$$
- $$57.6.011\underline{00000.0000000}/2^{13}$$

$$\text{Supernet mask} = 57.6.96\ 0/19$$

- Q2. Perform CIDR aggregation on the following IP addresses.
- 194.24.0.0/21
- 194.24.8.0/21
- 194.24.16.0/20

- Ans
1. NID is contiguous.
 2. Same size of networks, network must be power of 2.

- 194.24.0.0/21 } 1. Contiguous (True)
- 194.24.8.0/21 } 2. Same size = 11 bit, no of networks = $2^2 = 4$.
3. Total size of Supernet = $2^1 + 2^2 = 2^{12}$.

194.24.0.0

194.24.0000000.0000000/2¹². (True)

Rem/H10.

- = 194.24.0.0/20 }
- 194.24.16.0/20 } 1. Contiguous (True)
2. Same size = 12 bit, no of networks = $2^1 = 2$.
3. Total size of Supernet = $2^{12} + 2^{12} - 2^{13}$

194.24.0.0

194.24.0000000.0000000/2¹³ (True)

Supernet id = 194.24.0.0, total size = 13 bit

Ans = 194.24.0.0/19

Supernetting in Classful Addressing:

eg1. 200.96.86.0

200.96.87.0

200.96.88.0

200.96.89.0

1. Contiguous (True)

2. Same size, 2^8 , no of subnets = $4 = 2^2$

3. Size of Supernet = $2^8 \times 4$

$$= 2^{10}$$

200.96.86.0

200.96.01010110.00000000

Rem.

Supernetting not possible

eg3. 128.56.24.0

128.56.25.0

128.56.26.0

128.56.27.0

Class B.

NID HID

16 16

We can't apply Supernetting on
Single Network

eg4. 128.56.0.0

1. Contiguous (True)

128.57.0.0

2. Same size = 2^6 . No of subnets = $4 = 2^2$.

128.58.0.0

3. Total size of Supernet = $4 \times 2^6 = 2^{10}$.

128.59.0.0

128.56.0.0

= 128.00111000.00000000.00000000 / 2^{10} (True)

Rem / Hid

Total size of

Supernet = 2^{10}

HID = 18 bit, NID = 14 bit.

Supernet mask = 255.252.0.0

Subnet Mask

Supernet Mask

1. No. of 1's in the Subnetmask either equal to NID bits or more than NID bits.

No. of 1's in the Supernet mask always less than NID bits.

| | | |
|----|---|---|
| 2. | Subnet mask is applicable for single network. | Super net mask is applicable for two or more network or supernetting is applicable for two or more subnets. |
| 3. | In subnetting we borrowed from host id. | In supernetting we borrowed from network id |

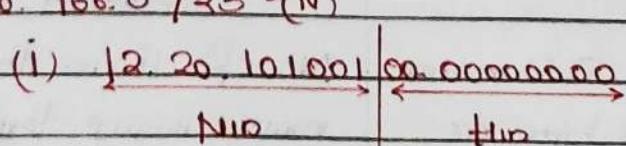
| Address. | Class A | Class B | Class C |
|---------------|---------|-----------|------------|
| 255.0.0.0 | Sub M | Sup. Mask | Sup. Mask |
| 255.255.252.0 | Sub M. | Sub Mask | Sup. Mask |
| 255.255.255.0 | Sub. M. | Sub Mask | Sub. Mask. |

Q1. Consider routing table of an organization's router shown below.

| Subnet number | Subnet mask | Next Hop |
|---------------|---------------|-------------|
| 12.20.164.0 | 255.255.252.0 | R1 |
| 12.20.170.0 | 255.255.254.0 | R2 |
| 12.20.168.0 | 255.255.254.0 | Interface 0 |
| 12.20.166.0 | 255.255.254.0 | Interface 1 |
| Default | | R3 |

Which of the following prefix in CIDR notation can be collectively used to correctly aggregate all the Subnets of the routing table?

- Ans
- 12.20.164.0/22 - (i)
 - 12.20.170.0/23 - (ii)
 - 12.20.168.0 /23 - (iii)
 - 12.20.166.0 /23 - (iv)



Range of (i)

12.20.164.0

↓
12.20.167.255

(ii) $12.20.101010/0.00000000$
 N10 | +10

Range: $12.20.170.0$
 ↓

$12.20.171.255$

(iii) $12.20.168.0$

- $12.20.1010100/0.0000000$
 N10 | +10

Range: $12.20.168.0$
 ↓

$12.20.169.255$

(iv) $12.20.166.0$

- $12.20.1010011/0.0000000$
 N10 | +10

Range: $12.20.166.0$
 ↓

$12.20.167.255$

* Network 4 is the part of network 1. So
 we can just ignore it.

$12.20.164/22$

$12.20.170.0/23$?

$12.20.168.0/23$

1. Contiguous (True)

2. Same size = 2^9 , no. of subnets = $2 = 2^1$

3. Total size of SuperNet = $2^9 \times 2 = 2^{10}$

$12.20.1010100.0000000/2^{10}$

Run or Hid pair.

SuperNet id = $12.20.168.0$

$12.20.164.0/22$

$12.20.168.0/22$

1. Contiguous (true)

2. Same size = 2^9 , no. of subnets = 2

3. Total size of SuperNet = $2^9 + 2^9 = 2^{10}$

$12.20.10100100.0000000/2^9$

Run or Hid pair.

Answers:

$12.20.164.0/22$

$12.20.168.0/22$

Q2 A company needs 600 addresses. Which of the following set of Class C blocks can be used to form a Supernet for this company?

Ans. 198.47.32.0, 198.47.33.0, 198.47.34.0, 198.47.35.0

1. Contiguous (True)

2. Same Size = 2^8 , no. of networks = $2^2 = 4$.

3. Total Size = $2^8 \times 4 = 2^{10}$

198.47.32.0

$$= 198.47.00100000.00000000 / 2^{10}$$

← →
Rm.

Q3. Consider 4 networks 199.202.0, 199.202.1.0, 199.202.2.0, 199.202.3.0 and Perform Aggregation to select one of the following Supernet mask.

Ans 1. Contiguous (True)

2. Same Size = 2^8 , no. of nets = $4 = 2^2$

3. Total size of Supernet = 2^{10} .

$$199.202.00000000.00000000 / 2^{10}$$

← →
Rm or flid

$$\text{Supernet mask} = 255.255.252.0$$

=

Q4. The mask is 255.255.252.0 can probably be used in Class A, C, B respectively.

Ans. Subnet mask, Supernet mask, Subnet mask.

Q5. In Class C, if Supernet mask is 255.255.224.0 then the number of Class C networks combined to form Supernet is

Ans. Supernet mask = 255.255.11000000.00000000

(Supernet id = 5 bit)

No of nets must be combined = $2^5 = \underline{\underline{32}}$

Q5. In class C, if Supernet mask is 255.255.252.0, then how many number of networks can be joined?

Ans. Supernet mask: 11111111.11111111.1111100.00000000
 NID. {10. NID + 10.

$$\text{No. of subnets that can be joined} = 2^2 = 4$$

Q6. One of the address of a Supernet is given as IP 201.99.89.113 and Supernet mask is 255.255.252.0. What will be the range of Supernet?

Ans. IP = 201.99.89.113

And (ing)

255.255.252.0

Supernet id = 201.99.88.0

S-mask = 255.255.1111100 - 0

Supernet bits,

$$= 2^2 = 4$$

$$\begin{array}{l|l} N_1 = 00 & N_2 = 10 \\ \hline N_2 = 01 & N_4 = 11 \end{array}$$

$$N_1 = 201.99.010110.00.0 \rightarrow 201.99.88.0$$

$$201.99.010110.00.255 \rightarrow 201.99.88.255$$

$$N_2 = 201.99.01011001.0 \rightarrow 201.99.89.0$$

$$201.99.89.255$$

$$N_3 = 201.99.01011010.0 \rightarrow 201.99.90.0$$

$$201.99.90.255$$

$$N_4 = 201.99.01011011.0 \rightarrow 201.99.91.0$$

$$201.99.91.255$$

Q7. If default Subnet mask for a network is 255.255.255.0 and if 'm' bits are borrowed from the network ID, then what could be its Supernet mask.

Ans.

$$S_m = 1111111.111111.111111.00000000$$

+10.

$$\text{Supernet mask} = 1111111.1111111.11110000.00000000$$

$\overbrace{\quad\quad\quad\quad}$
 $\text{Supernet id} = 4 \text{ bit}$

$$\text{Supernet mask} = 255.255.\underline{240.0}$$

$$(a) 255.255.(2^{8-m}) \times 2^m = (2^{8-4}) \times 2^4 \\ = (2^4) \times$$

$$(c) 2^{(8-m-1)} \times 2^{m-1} = 2^{(8-4-1)} \times 2^{4-1} \\ = (64) \times$$

$$(d) 2^{(8-m)} \times 2^{(m-1)} = 2^4 \times 2^3 = 2^7 (128) \times$$

Q8. An organization requires a range of IP addresses to assign one to each of its 1500 computers. The organization has approached an Internet Service Provider for this task. The ISP uses CIDR and serves the requests from the available IP address space 202.61.0.0/17. The ISP wants to assign an address space to the organization, which will minimize the routing entries in the ISP's router using router aggregation. Which of the following address spaces are potential candidates from which the ISP can allot any one to the organization?

I. 202.61.84.0/21

II. 202.61.104.0/21

III. 202.61.64.0/21.

IV. 202.61.144.0/21.

Ans.

202.61.0.0/17, N10 = 17 bit, #10 = 32-17 = 15 bit.

202.61.00000000.00000000

Range.

202.61.011111.11111111

(v) $202.61.64.0/21$, N10 = 21 bit, H10 = 11 bit

$202.61.01000000.00000000/21$ (Ans)

(vi) $202.61.104.0/21$, N10 = 21 bit, H10 = 11 bit

$202.61.01101000.00000000/21$ (Ans)

Ans = II and III

Q9. An Internet Service Provider (ISP) is granted a block of address starting with $162.72.0.0/16$. The ISP needs to distribute these addresses to three groups of customers as follows:

The first group has 128 customers, each need 256 addresses.

The second group has 128 customers, each need 64 addresses.

The third group has 64 customers, each need 128 addresses.

Find the last address of 6th customer of the 2nd group and how many addresses are still available with ISP after these allocations.

Ans $162.72.0.0/16$ N10 = 16 bit, H10 = 16 bit

No. of IP addresses available in the block = $2^{16} = 65,536$

I. First Group = 128 customers each need 256 addresses

$$128 \times 256 = 2^7 \times 2^8 = 2^{15} \text{ addresses}$$

II. Second Group = $128 \times 64 = 2^7 \times 2^6 = 2^{13}$ addresses

III. Third Group = $64 \times 128 = 2^6 \times 2^7 = 2^{13}$ addresses

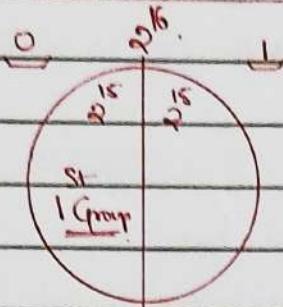
$$\text{IP addresses available} = 2^{16} - (2^{15} + 2^{13} + 2^{13})$$

$$= 2^{16} - (2^{16} + 2^{14})$$

$$= 2^{16} - 2^{14}(2+1) = 2^{16} - 3 \times 2^{14}$$

$$= 2^{16} - 3 \times 2^{14}$$

$$= 4 \times 2^{14} - 3 \times 2^{14} = 2^{14}$$



162.72.0 0000000.00000000

S10

162.72.0 0000000.00000000 - 162.72.0.0/17

162.72.0 1111111.11111111 - 162.72.127.255/17

162.72.0.0/16

X10 - 16, -110-16

162.72.0.0/17

First Group = 1 15
S10. +10

X10 +10
17 -15

128 customers
or Subtract

17 7 8
X10 S10 +10

162.72.0 -----
S10. ----- +10.

1st group = 1st customer

162.72.0 0000000.00000000 - 162.72.0.0/24

S10.

162.72.0 0000000.1111111 - 162.72.0.255/24

1st group → 2nd customer

162.72.0000001.00000000 - 162.72.1.0



162.72.0000001.1111111 - 162.72.1.0255

1st group → 3rd customer

162.72.0000010.00000000 - 162.72.2.0

162.72.0000010.0111111 - 162.72.2.255

1st group : 128th customer

162.72.127.0/24 → 162.72.127.255/24

2nd Group162.72, 100

N10 Sin +110

162.72 100 0000.0000000 - 162.72 128.019162.72. 100 1111.111111 - 162.72 159.255/19

N10 -110

19 12.

128 customer or 128 customers.

19 7 6
N10 Sin +110.2nd Group - 1st customer162.72 100

----- -----

Sin Sin +110

162.72 100 0000.00 0000000 → 162.72 128.0162.72 100 00000.00 11111 → 162.72 128.63/26+110

Continue the calculation

ERROR CONTROL

Error: If the data received is not same as the data sent then this means error has occurred.

Type of error:

1. Single bit error: The term single bit error means that only one bit of the given data unit is changed from 1 to 0 or 0 to 1.
2. Burst error: The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

e.g.:

Burst length = 4

Sent : 0 1 0 0 1 0 1 0

Received : 0 1 1 0 1 1 1 0

e.g.: 1 Data rate = 1 Kbps = 10^3 bits/sec

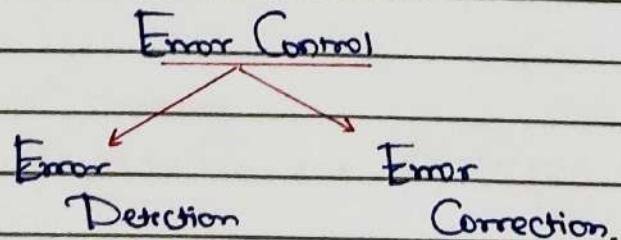
Noise duration = $\frac{1}{10}$ Sec

No. of corrupted bits = 10^3 bits/sec $\times \frac{1}{10}$ sec = 100 bits.

e.g.: 2 Data rate = 1 Mbps = 10^6 bits/sec

Noise duration = $\frac{1}{10}$ Sec

No. of corrupted bits = 10^6 bits/sec $\times \frac{1}{10}$ sec = 100000 bits.



- Note:
- * No. of corrupted bits or affected bits depend upon the data rate and duration of noise.
 - * Burst error is more likely to occur than Single bit error.
 - * No. of corrupted bits or affected bits

$$= \text{Data rate} \times \text{Noise duration}$$

Redundancy:

- 1) The central concept of detecting or correcting error is called redundancy.
- 2) To be able to detect or correct the errors, we need to send some extra bits with our data. These redundant bits are added by the Sender and received by the receiver.

Error detection: In error detection we are only looking to see if any error has occurred. The answer is simple yes or no, we are not even interested in the number of corrupted bits. A single bit error is same as double bit error.

Error Correction: In error correction we need to know the exact number of bits are corrupted and more importantly, their location in the message.

Error detection and Error correction points:

- * Correction of error is more difficult than detection.
- * If we need to correct a single error in a 8-bit data unit, we need to consider 8 possible error locations.
- * If we need to correct two errors in a 8-bit data unit, we need to consider 28 possibilities.

Error Control

Error Detection

Error Correction

1. Simple parity
2. 2D parity
3. Checksum
4. CRC
5. Data + Data.

1. Hamming Code

- * Capability of correcting error.
- * Does not require retransmission.
- * Hamming Code can correct single bit errors.

- * Once noticed error simply discard.
- * Ask for retransmission.

Logic for error detection:

- * Error detection is based on block coding.
- * In block coding, we divide our message into blocks, each of size k bits called data words.
- * We add ' r ' redundant bits to each data words and resulting word is called as code words of length n i.e. $n = k+r$.
- * In place of sending data words we send corresponding code words.

eg:: message = 00011011

$k=2$

dataword.

For $K=2$ bits and $r=1$ bit So dataword is of 2 bits and code word is of 3 bits i.e. $n=K+r$.

Dataword = K bits

\downarrow
 2^k combinations

Codeword = n bits

\downarrow
 2^n combinations

$(n > k)$ $2^n - 2^k =$ codewords that are not used \rightarrow invalid codewords.

| Dataword | Valid codeword | Codeword = 3 bits |
|---|-------------------|---|
| 00 | $\rightarrow 000$ | $000 \checkmark$ |
| 01 | $\rightarrow 011$ | $001 \times$ |
| 10 | $\rightarrow 101$ | $010 \times$ |
| 11 | $\rightarrow 110$ | $011 \checkmark$ $100 \times$ Invalid code word |
| $2^n - 2^k \rightarrow$ Invalid codewords | | $101 \checkmark$ |
| $2^n - 2^k = 4$ | | $: 110 \checkmark$ |
| 111 \times | | |
| <pre> graph TD Codeword --> ValidCodeword["Valid Codeword (2^k)"] Codeword --> InvalidCodeword["Invalid Codeword (2^n - 2^k)"] </pre> | | |

- * With k bits, we can create a combination of 2^k datawords.
- * With n bits, we can create a combination of 2^n valid codeword.
- * We know that $n > k$, there exist one to one correspondence b/w Codeword and Dataword
- * Hence $2^n - 2^k$ are invalid codeword
- * Hence 2^k are valid codeword.

Error detection using block code:

- If the following 2 conditions are met, the receiver can detect a change in the original codeword.
1. The receiver has a list of original codeword
 2. The original codeword has changed to invalid one

Each codeword sent to the receiver may change during transmission:

1. If the received codeword is the same as the one of the valid codeword, then word is accepted.
2. The received Codeword is not valid, it's discarded
3. The codeword is corrupted during transmission but the received word still matches a valid codeword, the error remains undetected.

Hamming Distance:

* Hamming distance between two binary strings of same size is the number of differences between corresponding bits. Hamming distance between two binary strings is denoted by $d(x,y)$

$$d(000, 011) = 2 \text{ (Hamming distance)}$$

$$d(10101, 11110) = 3 \text{ (Hamming distance)}$$

* Hamming distance can be easily be found if we apply XOR operation (\oplus) on the two words and count the number of '1's in the result.

* In the set of codewords, the minimum hamming distance is the smaller hamming distance between all possible pairs of codewords

e.g.: Valid code words

010 (a)

101 (b)

110 (c)

001 (d)

$$d(a,b) = 3$$

$$d(a,c) = 1$$

$$d(a,d) = 2$$

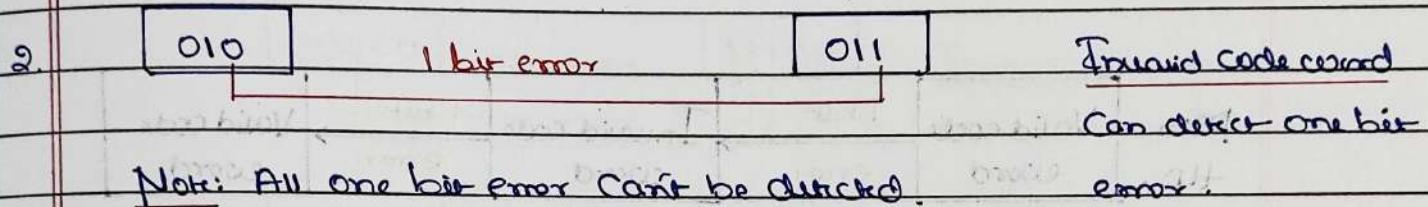
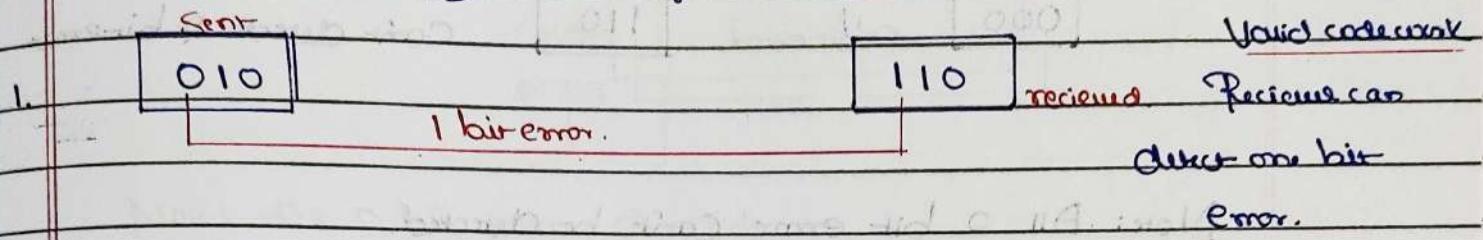
$$d(b,c) = 2$$

$$d(b,d) = 1$$

$$d(c,d) = 3$$

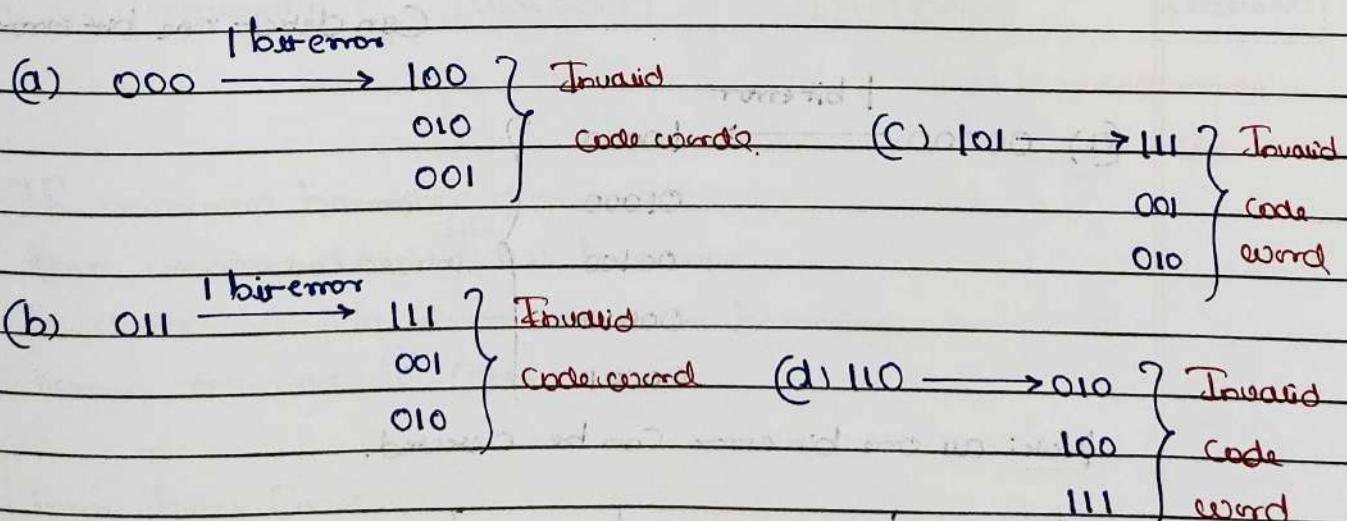
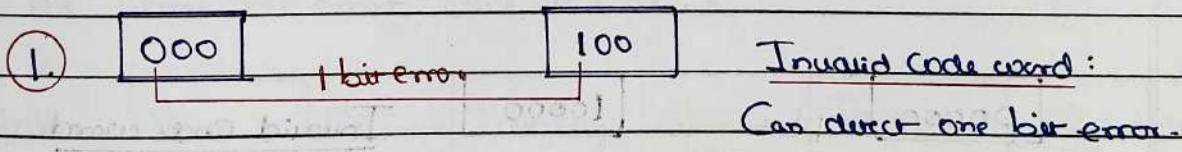
Minimum hamming distance = 1

Minimum Hamming Distance for error detection:



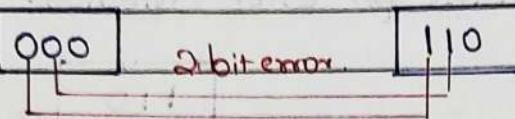
eg.: 2

| Valid code word | $d(a,b) = 2$ | Minimum Hamming distance = 2. |
|-----------------|--------------|-------------------------------|
| 000 (a) | $d(b,c) = 2$ | |
| 011 (b) | $d(c,d) = 2$ | |
| 101 (c) | $d(a,c) = 2$ | |
| 110 (d) | $d(a,d) = 2$ | |

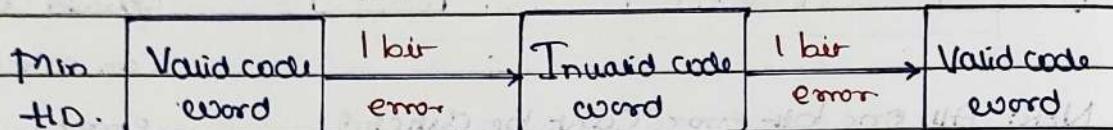


Note: all one bit error can be detected.

(2)

Valid code word

Can't detect 2 bit error.

Note: All 2 bit error Can't be detected.

Receiver can detect all one bit errors

eg:: 3. Valid code word

00000 (a)

01011 (b)

10101 (c)

11110 (d)

$d(a,b) = 3$

$d(a,c) = 3$

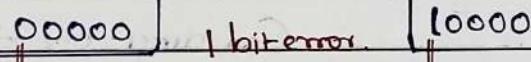
$d(a,d) = 4$

$d(b,c) = 4$

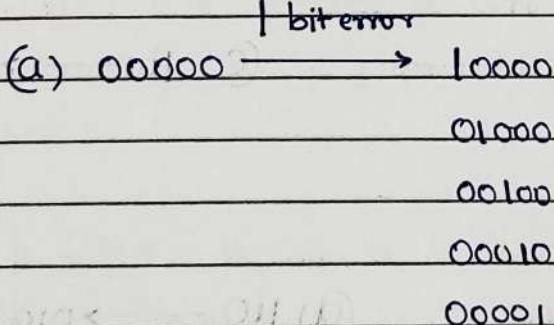
$d(b,d) = 3$

$d(c,d) = 3$

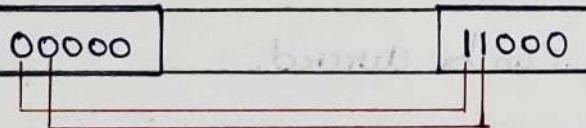
minimum Hamming distance = 3.

Invalid code word

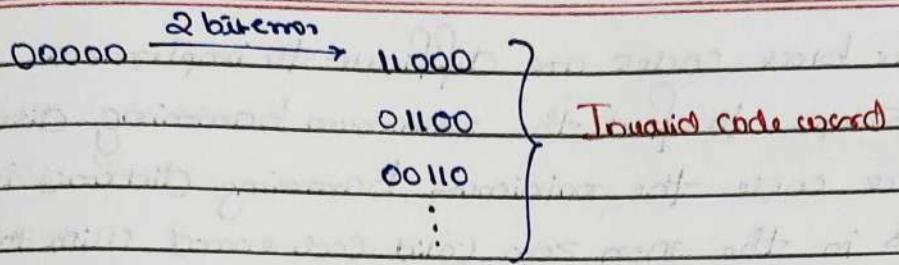
Can detect one bit error.



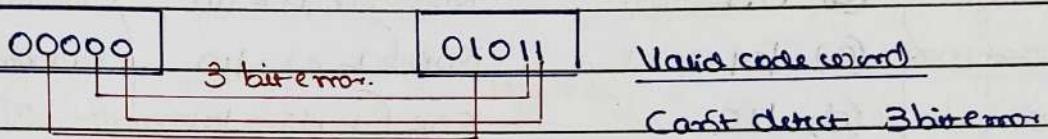
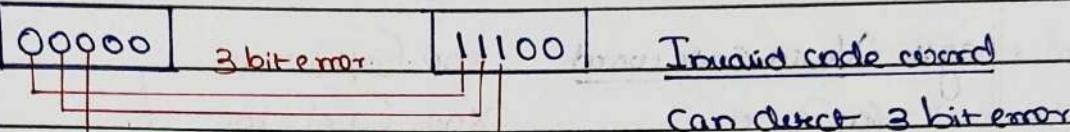
Invalid code word

Note: all one bit error Can be detected.Invalid code word

Can detect 2 bit error



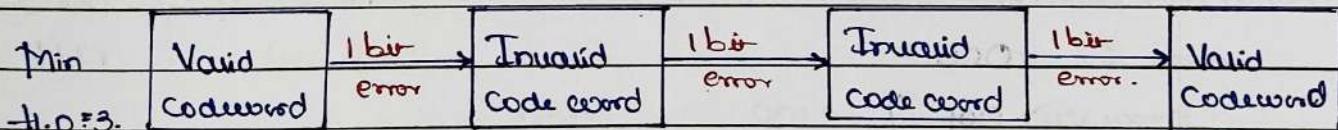
Note: All 2 bit error detected.



Note: All 3 bit error can't be detected.

* QF minimum hamming distance = 3

- * All one bit error detected
- * All two bit error detected
- * All three bit error can't be detected.



* If minimum hamming distance = d
then we can detect (d-1) bit errors.

To detect 'd' bit error minimum hamming distance required is (d+1)

Linear Block Codes:

- * A linear block code is a code in which the XOR of two valid code words creates another valid code word.
- * Today almost all error detection codes are linear block codes.

Non linear block codes are difficult to implement.

- * It is simple to find the minimum Hamming distance for linear block code - the minimum Hamming distance is the no. of 1's in the non zero valid code word with the smallest number of 1's.

eg:: Valid Code word

(a) 000

$$\text{XOR } (a, b) = 011$$

$$\text{XOR } (a, c) = 101$$

(b) 011

$$\text{XOR } (a, d) = 110$$

all valid code

(c) 101

$$\text{XOR } (b, c) = 110$$

excluded.

(d) 110

$$\text{XOR } (b, d) = 101$$

$$\text{XOR } (c, d) = 011$$

words.

* So above code word is linear block code.

- * Minimum Hamming Distance = 2 (min no. of 1's in the non zero code word).

Assume it is linear block code:

000 011 100 110

001 110 010 101

non zero code words

minimum no. of 1's = 1.

minimum Hamming Distance = 1

Minimum Hamming Distance for Error Correction:

| Min HD = 2 | Valid Codeword | 1 bit error | Invalid Codeword | 1 bit error | Valid codeword | Correct all one bit error |
|------------|----------------|-------------|------------------|-------------|----------------|---------------------------|
|------------|----------------|-------------|------------------|-------------|----------------|---------------------------|

Ex:

Valid code word

1001 } Minimum

1010 } Hamming dist = 2

Sent
① 1001

1 bit error.

Received

1011

Invalid code word

- Can detect one

bit error, not corr.

② 1010

1 bit error.

1011

Valid code word

It can detect one

bit error but

Cannot correct 1 bit error

Ex: 2

Valid code word

0000 } Min-Hamming

0011 } Distance = 2

Sent

0000

1 bit error.

Received

0010

Invalid code word

It can detect one bit error

but Cannot correct 1 bit error.

0011

1 bit error.

0010 Invalid code word

It can detect one bit, but

Cannot correct one bit error

Ex: 4.

Valid Code word

0000 } Min-Hamming

1111 } Distance = 4

Sent

0000

0001

Invalid code word

1 bit error.

It can detect and correct

all one bit error.

0000

0011

Invalid code word

It can detect two bit error

but cannot correct 2 bit error.

Note:

- To correct minimum one bit error minimum Hamming Distance required = $3 = 2 \times 1 + 1$
- To correct two bit error minimum Hamming Distance = $5 = 2 \times 2 + 1$
- To correct 'd' bit error minimum Hamming Distance required = $2 \times d + 1$

Problem Solving on Hamming Code

1. Consider a binary code that consists of only four valid code words 0000, 01011, 10101, 11110
 Let the minimum h.d. of the code be P and max no. of erroneous bits that can be corrected by the code q .
 Then the value of P and q .

Ans. Min. Hamming Distance = 3 (P)

Min. Hamming Distance to correct 1 bit error = $2d+1$
 $2d+1 = 3$

$$2d = 2, \quad 2d = 2$$

$$\therefore d = \frac{2}{2} = 1$$

2. What is the distance of the following code?

00000, 01010, 00111, 01100, 11111

Ans. Hamming Distance = 2 (minimum)

3. An error correcting code has the following code word: 00000, 0000111, 0101010, 1111000. What is the max. no. of bits that can be corrected?

Ans. Minimum Hamming Distance = 4

Min. H.D required to correct d bit error = $2d+1$

$$2d+1 = 4$$

$$2d = 4 - 1 = 3.$$

$$d = \frac{3}{2} = 1.5.$$

$$d = \underline{\underline{1}}$$

4. The minimum Hamming Distance to correct upto 5 bit error successfully = $2d+1 = 2(5)+1 = \underline{\underline{11}}$

5. The minimum Hamming Distance to detect upto 10 bit error is = $2d+1 = 10+1 = \underline{\underline{11}}$

Error ControlError detectionError Correction

1. Simple parity
2. 2-D parity
3. CRC
4. Checksum.

1. Hamming Code.

Simple Parity:

- * To the Simple parity concept one extra bit (Parity bit) is added to each data word.
- * Simple parity check can detect all single bit errors.
- * Simple parity check cannot detect an even no. of errors.
- * Simple parity check can detect an odd number of errors.

Simple parityEven parityOdd parity

No. of 1's must be even in each code word including the parity bit.

No. of 1's must be odd in each code word including the parity bit.

2D Parity:

- * Two dimensional parity check can detect and correct all single bit error and detect two or three bit error that occur anywhere in the matrix.
- * However, only some patterns with four or more errors can be detected.
- * In a 2D parity check code, the information bits are organised in a matrix consisting of rows and columns.

- * For each row and each column one parity check bit is calculated.

Original data:

| | | | | |
|---------------------|---------------------|---------------------|---------------------|---------------------|
| 010010 | 010101 | 100101 | 111011 | 001001 |
| 1 st row | 2 nd row | 3 rd row | 4 th row | 5 th row |

By using even parity

| | | | | | | |
|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 |

Row parity

Column Parity

No. of rows = 5

No. of columns = 6

Transmitted Data:

0100100 0101011 1001011 1110111 0010010 0100001.

One Error:

| | | | | | | |
|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 1 | 0 | 1 | 1 | 1 |
| 0 | 0 | 1 | 0 | 0 | 1 | 0 |

* One bit error detected as well as

Corrected

* One bit error after 2 parity

1 0 1 0 1 1 1 ←

Two Errors:

| | | | | | | |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 |

0 1 0 0 1 0 0

↑

* It can detect two bit errors but

0 1 1 0 0 1 1 ←

Can't correct two bit errors.

1 0 0 1 0 1 1

* 2 bit error will affect many bits.

1 1 1 0 1 1 1 ←

* 2 bit error will affect

0 0 1 0 0 1 0

minimum 2 bits.

0 1 0 0 0 0 1

↑ ↑

Three Error:

| | |
|-------------|--|
| 0 1 0 0 0 0 | 0 ← * 3 bit error detected but not corrected |
| 0 0 0 1 0 1 | 1 ← * 3 bit error will affect recursive. 6 |
| 1 0 0 1 0 1 | 1 Parity bits, and minimum 3 parity bits. |
| 1 1 0 0 1 1 | 1 ← |
| 0 0 1 0 0 1 | <u>Four Errors</u> |
| 0 1 0 0 0 0 | |
| ↑ ↑ ↑ | |

| | |
|-------------|-------------|
| 0 1 0 0 1 0 | 0 0 0 0 1 0 |
| 0 0 0 0 0 1 | 1 0 1 1 0 1 |
| 1 0 0 1 0 1 | 1 0 0 0 0 1 |
| 1 0 1 0 1 1 | 1 1 1 0 0 1 |
| 0 0 1 0 0 1 | 0 0 1 0 0 1 |
| 0 1 0 0 0 0 | 0 1 0 0 0 1 |

4 bit error can't be
detected

4 bit error detected

Note:

Disadvantage of 2D parity is that if we have a error in the parity then this scheme does not work fine.

Cyclic Code:

- * Cyclic code are special linear block code with one extra property.
- * In cyclic code, if a codeword is cyclically shifted (rotated) then the result is another codeword.

Linear Block Codes:

- * A linear block code is a code in which the XOR (+) of two valid Codewords Create another valid Codeword.

Today almost all error detecting codes are linear block codes: non-linear block codes are difficult to implement.

It is simple to find the minimum Hamming distance for linear block.

Code the minimum hamming distance is the number of 1's in a non-zero valid code word with the smallest number of 1's.

Introduction to CRC:

- * Length of the dataword = n
- * Length of the divisor = k
- * Append $(k-1)$ zeros to the original message
- * Perform modulo 2 division
- * Remainder of division = CRC
- * Codeword = $n+k-1$ (CRC must be $k-1$ bits)
- * Codeword = dataword with appended $(k-1)$ zeros + CRC.

Data = 1001001

Division or CRC generator = 1101

$$\begin{array}{r}
 1101) 1001001000 \\
 \underline{1101} \\
 100001000 \\
 \underline{1101} \\
 10101000 \\
 \underline{1101} \\
 0111000 \\
 \underline{1101} \\
 01000 \\
 \underline{1101} \\
 00001011 \rightarrow \text{CRC Remainder}
 \end{array}$$

Codeword = Dataword + CRC
 $= 1001001000 + 111$
 $= 1001001111$

If receiver received uncorrupted data:

1101) 1001001111

1101

100001111

1101

10101111

1101

1111111

1101

10111

1101

1101

1101

000

Syndrome = 0

* If syndrome to dataword is rejected or else accepted.

Polynomial Notation in CRC.

- * Dataword = $d(x)$
- * Codeword = $c(x)$
- * Generator = $g(x)$
- * Syndrome = $s(x)$
- * Error = $e(x)$

Applying CRC Step by Step:

1. Determine the degree 'n' of $g(x)$ (higher power)
2. Determine $x^n d(x)$
3. Determine the remainder by dividing $x^n d(x)$ by $g(x)$
4. Codeword = $x^n d(x) + \text{remainder}$.

e.g.: Dataword $d(x) = 1001001$

$$\begin{array}{r} 1001001 \\ x^6 x^5 x^4 x^3 x^2 x^1 x^0 \\ \hline \end{array} = x^6 + x^3 + 1.$$

Divisor 1101

$$x^2 x^1 x^0 = x^3 + x^2 + 1. \quad (\text{higher power} = x^3) \quad n=3$$

$$\begin{aligned} x^7 d(x) &= x^3 (x^6 + x^3 + 1) \\ &= x^9 + x^6 + x^3. \end{aligned}$$

$$\begin{array}{r} x^3 + x^2 + 1 \\ \times x^6 + x^3 \\ \hline x^9 + x^6 + x^3 \end{array}$$

$$\underline{x^9 + x^8 + x^6}$$

$$\begin{array}{r} x^9 \\ x^8 + x^3 \\ \hline \end{array}$$

$$\underline{x^8 + x^7 + x^5}$$

$$\underline{x^7 + x^5 + x^3}$$

$$\underline{x^7 + x^6 + x^4}$$

$$\underline{x^6 + x^5 + x^3}$$

$$\underline{x^6 + x^5 + x^3}$$

$$\begin{array}{r} x^4 \\ x^4 + x^3 + x \\ \hline \end{array}$$

$$\underline{x^3 + x}$$

$$\underline{x^2 + x^2 + x}$$

$$\underline{x^2 + x + 1}$$

$x^2 + x + 1$ - Remainder or CRC

Problem Solving on CRC

1. Consider the CRC based error detecting scheme having the generator polynomial $x^3 + x + 1$. Suppose the message = 11000 is to be transmitted. Check bits $C_2 C_1 C_0$ are appended at the end of the message by transmitter. The transmitted bit string is denoted by $mymzmmzmmymoC_2 C_1 C_0$. The value of sequence $C_2 C_1 C_0$ is

Ans Generator = $x^3 + x + 1$

$$= 1011 \quad 1011) 11000000$$

message = 11000

$$\begin{array}{r} 1011 \\ 1110000 \\ 1011 \\ \hline 101000 \end{array}$$

Ans = 100

$$1011$$

$$100 - \text{CRC}$$

2. Given the generator function $G(x)$ and the message function $m(x)$ as follows:

$$G(x) = x^4 + x + 1, \quad r=4$$

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

Calculate the transmission function $T(x)$

$$x^4 + x + 1 \overline{) x^{11} + x^{10} + x^8 + x^6 + x^5}$$

$$x^8 + x^7 + x^6 + x^5$$

$$x^{10} + x^7 + x^6 + x^5$$

$$x^{10} + x^7 + x^6$$

$$\text{Codeword} = x^{11} + x^{10} + x^8 + x^6 + x^5 + x^2 + x$$

$$x^8 + x^7 + x^6 = \text{Remainder}$$

$$(x^2 + x) \rightarrow \text{Remainder}$$

HW

3. The message 11001001 is to be transmitted using the CRC polynomial $x^3 + 1$ to protect it from error. The message that should be transmitted is:

4. A computer network uses polynomial over GF(2) for error checking using 8 bits as info bits and uses $x^3 + x + 1$ as generator. In this network the message 01011011 is transmitted as

$$\text{Generator} = x^3 + x + 1$$

$$= 1011$$

$$1011 \overline{) 01011011000}$$

$$\text{Transmitted data} = 01011011101$$

$$1011$$

$$011000$$

$$1011$$

$$1110$$

$$1011$$

$$0101$$

Cyclic Code Analysis

- * Dataword = $d(x)$
- * Codeword = $c(x)$
- * Generator = $g(x)$
- * Syndrome = $s(x)$
- * Error = $e(x)$

1. If $s(x) \neq 0$, one or more bit is corrupted
2. If $s(x) = 0$, either
 - (i) no bit is corrupted
 - (ii) Some bits are corrupted, but channel fails to detect them.

Received Code word = Sent Codeword + error

Received Codeword = $c(x) + e(x)$

1. If there is no error, $e(x) = 0$ then

$$\begin{aligned} \text{Received Codeword} &= c(x) \\ \frac{c(x)}{g(x)} &= 0 \end{aligned}$$

2. If there is error, $e(x) \neq 0$ then

$$\text{Received Codeword} = c(x) + e(x)$$

Received Codeword = $c(x) + e(x)$

$$\text{Received Codeword} = \frac{c(x)}{g(x)} + \frac{e(x)}{g(x)}$$

$\frac{c(x)}{g(x)} = 0$ According to the definition of Ccc. So Syndrome is actually the remainder of $\frac{e(x)}{g(x)}$

Either

$\frac{e(x)}{g(x)} = 0$ (i) Entire $e(x) = 0$ [no error] Ccc scheme is working fine

(ii) $e(x) \neq 0$, but we are getting $\frac{e(x)}{g(x)} = 0$ then it

means $e(x)$ is divisible by $g(x)$

Dataword = 1101001

Divisor = 1001

Sender 1001) 1101001000

1001

100001000

1001

101000

1001

1100

1001

0101

→ CRC or Remainder

Sent codeword = 1101001101

Received codeword = 1101000100

1001) 1101000100

1001

100000100

1001

100100

1001

000

Syndrome = 0

No error

Note: * Crc is not perfect scheme if $e(x)$ is divisible by $g(x)$ then that error can't be detected.

* Probability of such error is very less, hence error detection probability of Crc is very high.

$$\text{Received codeword} = \frac{c(x) + e(x)}{g(x)}$$

Syndrome = $s(x)$

1. If $s(x) \neq 0$, then code word is rejected and Crc Scheme is working fine.
2. If $s(x)=0$ and $e(x)=0$ then Codeword is accepted and Crc Scheme is working fine.
3. If $s(x)=0$ and $e(x) \neq 0$ [$e(x)$ is divisible by $g(x)$] then Codeword accepted and Scheme failed to detect error.

Note:

* Except for last bit error, Single bit error give even number so divisor must not be even. If divisor is also even then remainder will be zero, so we cannot catch single bit error.

* To detect all single bit error the last bit of the divisor must be 1, so that divisor becomes an odd number and hence all single bit error detected.

* If the generator has more than one term and co-efficients of x^i is 1, all single bit error can be detected.

* If a generator cannot divide $x^t + 1$ (t between 0 to $n-1$) then all isolated double error can be detected.

* A generator that contains a factor of $x+1$ ^{can} detect all odd numbered errors.

1. If the generator has more than one term and co-efficients of x^i is 1, all single bit error can be detected.

eg: Data: 1011

CRC generator = 1 (Generator is not valid)

eg.: Data = 1011

$$\text{CRC Generator} = x^4 + x^3 + x^2 + x + 1$$

10 | 10110

10

110

10

10

00

\rightarrow CRC or Remainder.

Received codeword

10010

10 | 10010

10

010

10

00 \rightarrow Syndrome = 0

No error, dataword accepted so it is not able to detect the error.

Note: Generators Should not contain '0'

eg.: Data = 1011

$$\text{CRC generator} = x^3 + 1 = 1 \cdot x^3 + 1 \cdot x^0 = 11$$

11 | 10110

1110

11

0010

11

01 \rightarrow Remainder

1011

11

11 | 10101

11

1101

11

01 \rightarrow Syndrome = 1

One bit error detected

Send codeword

Received Codeword

10111

10100

11 | 10100

11

1100

11

0000

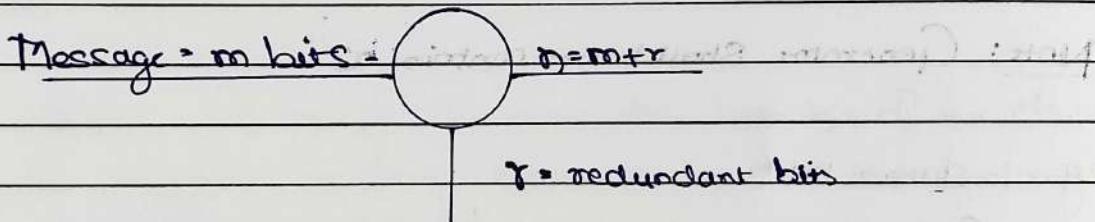
Syndrome = 0, two bit errors not detected.

A good Polynomial generator needs to have the following characteristics:

1. It should have atleast two terms.
2. The co-efficient of the term x^0 should be 1.
3. It should not divide $x^t + 1$ where t between 2 and $n-1$.
4. It should have the factor $x+1$.

Hamming Code:

- + Hamming code can correct 1 bit error
- + Hamming code can detect upto 2 bit error
- + Hamming code can be used for error correction.



According to the Hamming code, number of redundant bits
 $m+r+1 \leq 2^r$ where r = lower limitation.

e.g.: Data = 1010111, $m=7$

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

$$r=1 \rightarrow 7+1+1 \leq 2^1 \times$$

$$r=2 \rightarrow 7+2+1 \leq 2^2 \times$$

$$r=3 \rightarrow 7+3+1 \leq 2^3 \times$$

~~$$r=4 \rightarrow 7+4+1 \leq 2^4 = 16 \leq 16$$
 (Yes)~~

~~$$r=5 \rightarrow 7+5+1 \leq 2^5 = 32 \leq 32$$
 (Yes)~~

Choose the minimum value of r that satisfies
the condition.

$$n = m+r$$

$$= 7+4$$

~~$$= 11$$~~

Redundant bit position = $\frac{1}{2}$ (Gause 120)
or

Parity bits or Checkbits.

$$= 2^0, 2^1, 2^2, \dots$$

$$1, 2, 4, \dots$$

$$1, P_1, P_2, P_3, \dots$$

$$\begin{array}{ccccccccc} P_1 & P_2 & P_3 & P_4 & P_5 & P_6 & P_7 & P_8 & P_9 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{array}$$

$$\begin{array}{cccccc} P_1 & P_2 & P_3 & P_4 & P_5 & P_6 \\ 1 & 3 & 5 & 7 & 9 & 11 \\ \textcircled{1} & 0 & 0 & 1 & 1 \end{array}$$

$$\begin{array}{cccccc} P_2 & P_3 & P_4 & P_5 & P_6 & P_7 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ \textcircled{0} & 1 & 1 & 0 & 1 & 1 \end{array}$$

$$\begin{array}{cccccc} P_4 & P_5 & P_6 & P_7 \\ 4 & 5 & 6 & 7 \\ \textcircled{1} & 0 & 1 & 0 \end{array}$$

$$\begin{array}{cccccc} P_8 & P_9 & P_{10} & P_{11} \\ 8 & 9 & 10 & 11 \\ \textcircled{1} & 1 & 1 & 1 \end{array}$$

e.g.:

Transmitted data = 10110101111

If receiver received uncorrupted data

Received data = 10110101111

$$\begin{array}{cccccc} P_1 & P_2 & P_3 & P_4 & P_5 & P_6 \\ 1 & 3 & 5 & 7 & 9 & 11 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{array}$$

even $P_1=0$.

$$\begin{array}{cccccc} P_4 & P_5 & P_6 & P_7 & P_8 & P_9 \\ 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{array}$$

even $P_4=0$

$$\begin{array}{cccccc} P_2 & P_3 & P_4 & P_5 & P_6 & P_7 \\ 2 & 3 & 6 & 7 & 10 & 11 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{array}$$

even $P_2=0$.

$$\begin{array}{cccccc} P_8 & P_9 & P_{10} & P_{11} \\ 8 & 9 & 10 & 11 \\ 1 & 1 & 1 & 1 \end{array}$$

even ($P_8=0$)

$P_8 P_4 P_2 P_1$

$0 \ 0 \ 0 \ 0 \rightarrow \text{no error}$ (If non zero then error)

If receiver received corrupted bit.

Received data = 10110101011
 \downarrow 10^6 bits

| | |
|--|---|
| P_1 $\begin{matrix} 1 & 3 & 5 & 7 & 9 & 11 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{matrix} \rightarrow \text{odd } (P_1=1)$ | P_4 $\begin{matrix} 4 & 5 & 6 & 7 \\ 1 & 0 & 1 & 0 \end{matrix} \rightarrow \text{even } (P_4=0)$ |
| P_2 $\begin{matrix} 2 & 3 & 6 & 7 & 10 & 11 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{matrix} \rightarrow \text{even } (P_2=0)$ | P_8 $\begin{matrix} 8 & 9 & 10 & 11 \\ 1 & 0 & 1 & 1 \end{matrix} \rightarrow \text{odd } (P_8=1)$ |

P₈P₄P₂P₁

| 0 0 | \rightarrow Non zero means error

\hookrightarrow decimal value = 9

~~11 12 so 9th bit got corrupted~~

* If receiver received corrupted data: (2 bit error)

Received data = 10111101011

| | | |
|-------|---------------------------|--|
| P_1 | $1 \ 3 \ 5 \ 7 \ 9 \ 11$ | $1 \ 1 \ 1 \ 0 \ 0 \ 1 \rightarrow \text{even } (P_1=0)$ |
| P_4 | $4 \ 5 \ 6 \ 7 \ 8$ | $1 \ 1 \ 1 \ 0 \rightarrow \text{odd } (P_4=1)$ |
| P_2 | $2 \ 3 \ 6 \ 7 \ 10 \ 11$ | $0 \ 1 \ 1 \ 0 \ 1 \ 1 \rightarrow \text{even } (P_2=0)$ |
| P_8 | $8 \ 9 \ 10 \ 11$ | $1 \ 0 \ 1 \ 1 \rightarrow \text{odd } (P_8=1)$ |

P₈P₄P₂P₁

1100 → decimal value = 12

(Dro zero means empty)

Two bit error detected

Q1 If a 7-bit hamming code word received by the receiver is 1011011. Assume even parity state whether the received code word is correct or not? If not correct then locate the bit having error.

Ans

P₁ P₂ 3 P₄ 5 6 7

| P ₁ | 1 | 3 | 5 | 7 | |
|----------------|---|---|---|---|---------------------------|
| | 1 | 1 | 0 | 1 | → odd (P ₁ =1) |

| P ₂ | 2 | 3 | 6 | 7 | |
|----------------|---|---|---|---|---------------------------|
| | 0 | 1 | 1 | 1 | → odd (P ₂ =1) |

| P ₄ | 4 | 5 | 6 | 7 | |
|----------------|---|---|---|---|---------------------------|
| | 1 | 0 | 1 | 1 | → odd (P ₄ =1) |

P₄ P₂ P₁
1 1 1 → non zero remain error
decimal value = 7, so 7th bit got corrupted.

Q2 Assume that a 12-bit hamming code word consisting of 8-bit data and 4 check bits is d₇d₆d₅d₄d₃d₂d₁, c₈ c₇c₆c₅c₄ where data bits and check bits are:

Data bits Check bits

1 1 0 × 0 1 0 1
d₇ d₆ d₅ d₄ d₃ d₂ d₁,
c₈ c₇ c₆ c₅ c₄ c₃ c₂ c₁

Correct values of x and y are?

Ans:

1 2 3 4 5 6 7 8 9 10 11 12
0 1 1 0 0 1 0 4 x 0 1 1

C₁
1 3 5 7 9 11
0 1 0 0 x 1

C₄
4 5 6 7 12
0 0 1 0 1 → even

∴ The
values of
x and y
are odd &
even
respectively.

C₂. 2 3 6 7 10 11
1 1 1 0 0 1 → even.

C₈. 8 9 10 11 12
x y 0 1 1.

0 (for even parity),

Q3. Consider hamming code (Signal bit error detection and correction technique), the minimum parity bits needed for 60 bits data is _____

Ans.

$$m=60$$

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

$$\checkmark r=7, 60+7+1 \leq 2^7 \text{ (yes)}$$

Q4. For single bit error Correcting Hamming code, the code length for 12 data bit is _____

Ans

$$m=12$$

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

$$r=4 \rightarrow 12+4+1 \leq 2^4 \times$$

$$r=5 \rightarrow 12+5+1 \leq 2^5 \checkmark$$

$$\text{Code Length} = 12+5$$

$$= 17$$

HW

Q5. After encoding using hamming method, the pattern for 1010111 is

Ans

$$m=7, r=4, D=m+r$$

$$= 7+4=11 \text{ bit}$$

$$r=4 \rightarrow 7+4+1 \leq 2^4 \quad 12 \leq 16 \text{ (yes)}$$

| P ₁ | P ₂ | P ₃ | P ₄ | P ₅ | P ₆ | P ₇ | P ₈ | P ₉ | P ₁₀ | P ₁₁ |
|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|-----------------|-----------------|
| 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 |

| | |
|----------------|----------------|
| P ₁ | P ₄ |
| 1 3 5 7 9 11 | 4 5 6 7 |
| 1 0 1 0 1 1 | 1 1 0 0 1 1 0 |
| P ₂ | P ₈ |
| 2 3 6 7 10 11 | 8 9 10 11 |
| 1 0 1 0 1 1 | 1 0 0 0 1 1 |

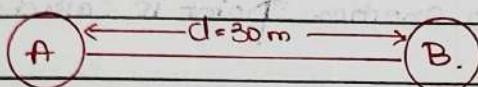
Note: Odd parity is preferably over even parity.

FLOW CONTROL

Delay in Computer Network.

Bandwidth: Bandwidth represent the rate at which number of bits placed on the link in one second.

Velocity: Velocity represent the rate at which distance covered in one second.



100 bits transfer from A to B.

$$B = 1 \text{ bps} = 1 \text{ bit/sec}$$

$$v = 10 \text{ m/sec}$$

$$\begin{aligned} \text{Total time} &= 100 \text{ sec} + 3 \text{ sec} \\ &= \underline{\underline{10.3 \text{ sec}}} \end{aligned}$$

Delay:

1. Transmission delay (T_d)
2. Propagation delay (P_d)
3. Queuing delay (Q_d)
4. Processing delay (P_{rd})

Transmission delay: Amount of time taken to transfer a packet on to the outgoing link is called as transmission delay.

e.g.: 1

Packet size = 1000 bits

$$\text{Bandwidth} = 2 \text{ bps} = 2 \text{ bits/sec}$$

$$T_d = \frac{1000 \text{ bits}}{2 \text{ bits/sec}}$$

$$= \underline{\underline{500 \text{ Sec}}}$$

| |
|---------------------|
| $T_d = \frac{L}{B}$ |
|---------------------|

e.g.: 2

Packet Size = 100 bits

$$\text{Bandwidth} = 10 \text{ bps} = 10 \text{ bits/sec}$$

$$\text{Transmission Delay} = \frac{100 \text{ bits}}{10 \text{ bits/sec}}$$

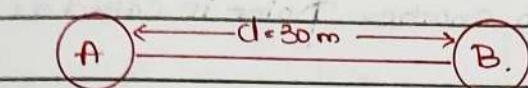
$$= \underline{\underline{10 \text{ sec}}}$$

FLOW CONTROL

Delay in Computer Network.

Bandwidth: Bandwidth represent the rate at which number of bits placed on the link in one second.

Velocity: Velocity represent the rate at distance covered in one second.



100 bit transfer
from A to B.

$$B = 1 \text{ bps} = 1 \text{ bit/sec}$$

$$v = 10 \text{ m/sec}$$

$$\begin{aligned} \text{Total time} &= 100 \text{ sec} + 3 \text{ sec} \\ &= \underline{\underline{103 \text{ sec}}} \end{aligned}$$

Delay:

1. Transmission delay (T_d)
2. Propagation delay (P_d)
3. Queuing delay (Q_d)
4. Processing delay (P_{rd})

Transmission delay: Amount of time taken to transfer a packet on to the outgoing link is called as transmission delay.

eg:: 1.

$$\text{Packet size} = 1000 \text{ bits}$$

$$\text{Bandwidth} = 2 \text{ bps} = 2 \text{ bits/sec}$$

$$T_d = \frac{1000 \text{ bits}}{2 \text{ bits/sec}}$$

$$= \underline{\underline{500 \text{ sec}}}$$

$$T_d = \frac{L}{B}$$

eg:: 2

$$\text{Packet Size} = 100 \text{ bits}$$

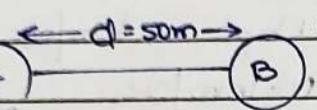
$$\text{Bandwidth} = 10 \text{ bps} = 10 \text{ bits/sec}$$

$$\text{Transmission delay} = \frac{100 \text{ bits}}{10 \text{ bits/sec}}$$

$$= \underline{\underline{10 \text{ sec}}}$$

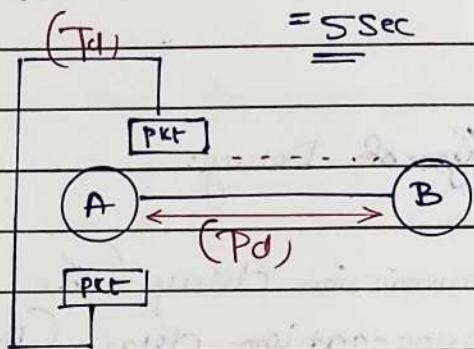
| | Data | Bandwidth |
|---|---|-----------|
| K | $1024 (2^{10})$ | 10^3 |
| M | $1024 \times 1024 (2^{20})$ | 10^6 |
| G | $1024 \times 1024 \times 1024 (2^{30})$ | 10^9 |

Propagation delay: Amount of time taken to reach a packet from one point to another point is called as propagation delay.

eg::  $d = 50m$, $v = 10mm/sec.$

$$\text{Propagation Delay} = \frac{d}{v} = \frac{50m}{10mm/sec.} = 5 \text{ sec}$$

$$Pd = \frac{\text{distance}}{\text{velocity}} = \frac{d}{v}$$



Total time taken to send a packet from A to B = $Td + Pd$

Queuing delay: Amount of time a packet will wait in the queue at the router before being taken up for processing is called as Queuing delay.

* $DLL \rightarrow \text{Node to Node or Hop to Hop}$

* $NI \rightarrow \text{Source host to Destination host}$

* $TL \rightarrow \text{Process to Process or end to end}$

OSI Layer.

Application Layer
 Presentation Layer
 Session Layer
 Transport Layer (TL)
 Network Layer (NL)
 Data Link Layer (DL)
 Physical Layer (PL)

TCP/IP

Application Layer
 Transport Layer
 Network Layer
 Data Link Layer
 Physical Layer.

Processing Delay: Processing delay is the time required for the router or a destination host to receive a packet from its input port, remove the header, perform an error detection procedure, and deliver the packet to the output port (in case of router) or deliver the packet to upper layer protocol (in case of destination host).

Q1. If the packet size is 1kb and channel size/capacity is 10^9 bits/sec what is the transmission time?

Ans

$$\text{Packet Size} = 1\text{KB} = 1024 \text{ Byte} = 1024 * 8 \text{ bits} \\ = 8192 \text{ bits}$$

$$\text{Bandwidth (B)} = 10^9 \text{ bits/sec}$$

$$T_d = \frac{L}{B} = \frac{8192}{10^9 \text{ bits/sec}} = 8.192 \times 10^{-6} \text{ sec} \\ = 8.192 \mu\text{s}$$

Q2. Consider two hosts x and y, connected by a single directed link of rate 10^6 bits/sec. The distance between the two hosts is 10,000 km and the propagation delay along the link is 2×10^{-8} m/sec. Host x sends a file of 50,000 bytes as one large message to host y continually. Let the transmission and propagation delay be p milliseconds and q (ms), the values of p and q are:

Ans

$$B = 10^6 \text{ bits/sec}, d = 10,000 \text{ km}$$

$$v = 2 \times 10^8 \text{ m/sec} \quad \text{packet size } (L) = 50,000 \text{ bytes} \times 8 \\ = 1,00,000 \text{ bits}$$

$$T_d = \frac{L}{B} = \frac{1,00,000}{10^6 \text{ bits/sec}}$$

$$10^6 \text{ bits/sec} = 400 \times 10^{-3} \text{ sec} \\ = \underline{\underline{400 \text{ msec}}}$$

$$P_d = \frac{d}{v} = \frac{10,000}{2 \times 10^8 \text{ km/sec}}$$

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

$$q = \underline{\underline{50 \text{ msec}}}$$

$$\therefore p = 400 \text{ msec} \text{ and } q = 50 \text{ msec.}$$

- Q3. Consider two computers x and y connected via a single bandwidth 512 Gbps . Suppose that both hosts are separated by distance T in meters, and propagation delay along with the link is $2 \times 10^9 \text{ meter/sec}$. Computer x has to send a packet of size 1 KByte to computer y . What will be the distance T such that the delay in propagation is equal to the delay in transmission?

Ans.

$$B = 512 \times 10^9 \text{ bits/sec}, \text{ Distance} = m \text{ bits}$$

$$v = 2 \times 10^9 \text{ m/sec}, L = 1 \text{ KB} = 1024 \text{ Bytes} = 8 \times 1024 \text{ bits}$$

$$P_d = T_d$$

$$\frac{d}{v} = \frac{L}{B} \quad \frac{T}{2 \times 10^9 \text{ m/sec}} = \frac{8 \times 1024 \text{ bits}}{512 \times 10^9 \text{ bits/sec}}$$

$$T = \frac{8 \times 1024 \times 2 \times 10^9}{512 \times 10^9} \text{ mtr}$$

$$T = \underline{\underline{32 \text{ mtr}}}$$

Q4 Consider a 100 Mbps link between an earth station (Sender) and a satellite (receiver) at an altitude of 2100 km. The signal propagates at a speed of 3×10^8 m/sec. The time taken (in ms) for the receiver to completely receive a packet of 1000 byte transmitted by the sender is _____

Ans

$$d = 2100 \text{ km}, v = 10^8 \text{ m/sec.}, u = 10^5 \text{ km/sec.}$$

$$T_d = \frac{d}{v} = \frac{2100 \text{ km}}{3 \times 10^5 \text{ km/sec}}$$

$$= 7 \times 10^{-3} \text{ sec}$$

$$= 7 \text{ ms}$$

pkt size = 1000 byte = 8000 bit

$$B = 100 \text{ Mbps} = 100 \times 10^6 \text{ bits/sec.}$$

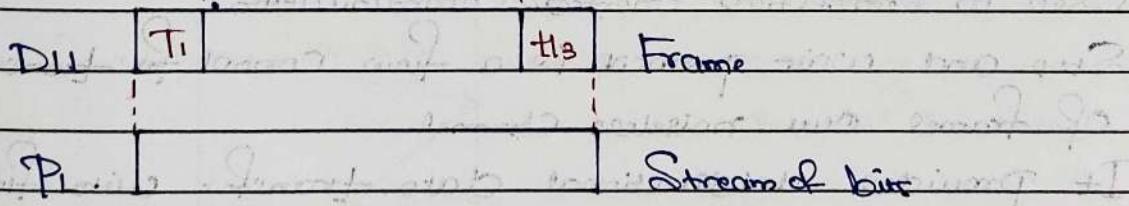
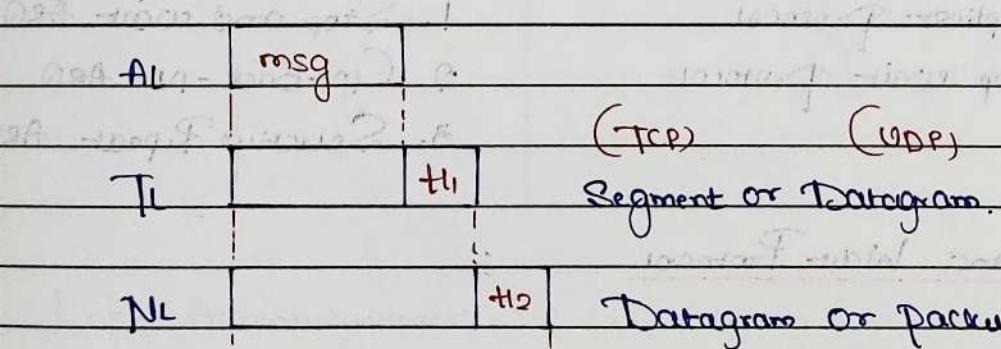
$$= 100 \times 10^8 \text{ bits/sec}$$

$$T_d = \frac{L}{B} = \frac{8000 \text{ bits}}{10^8 \text{ bits/sec.}} = 8 \times 10^{-5} \text{ sec}$$

$$= 0.8 \times 10^{-3} \text{ sec}$$

$$\therefore T_d + p_d = 17 + 0.8$$

$$= 17.08 \text{ ms}$$

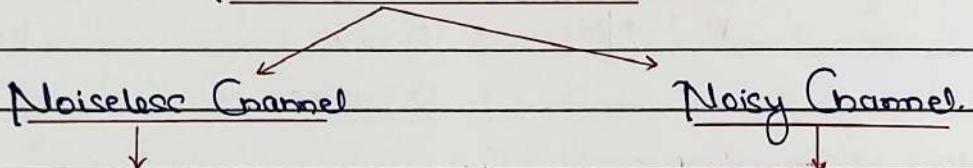
Flow Control

1. Flow control co-ordinate the amount of data can be sent before receiving the acknowledgement.
2. Flow control is a set of procedure that tells the sender how much data it can transmit before it must wait for an acknowledgement.

From the receiver.

3. Receiver has a limited speed at which it can process incoming data and limited amount of memory in which to store incoming data.
4. Receiver must inform the sender before limit is reached and request that the transmitter to send fewer frames or stop temporarily.
5. Since the rate of processing is often slower than the rate of transmission, receiver has a block of memory (buffer) storing incoming data until they are processed.

Flow Control Protocols



1. Simplex Protocol
2. Stop wait protocol.

1. Stop and wait ARQ
2. Go-back-N ARQ
3. Selective Repeat ARQ

Stop and Wait Protocol

- * Used in connection oriented communication.
- * Stop and wait protocol is a flow control for transmission of frames over noiseless channel.
- * It provides Unidirectional data transfer with flow control facilities without error control.
- * The idea of Stop and wait protocol is straight forward.
- * After transmitting one frame, the sender waits for an acknowledgement before transmitting the next frame.

Sender Side:

Rule 1: Send one data packet at a time

Rule 2: Send the next packet only after receiving the ACK for the previous packet.

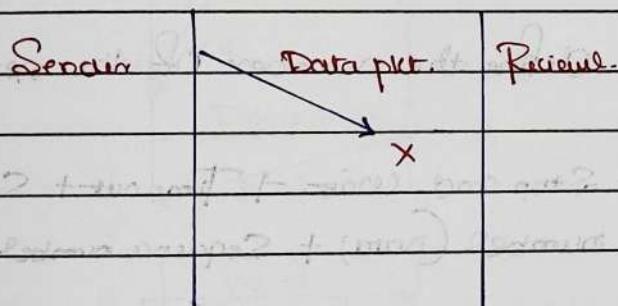
Receiver Side:

Rule 1: Receive and consume the data packet.

Rule 2: After Consuming Packet, acknowledgement needs to be sent.

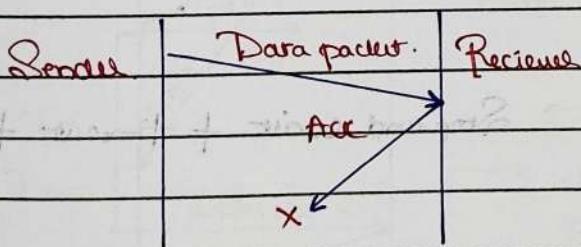
Problems of Stop and Wait Protocol

1. Lost data packet



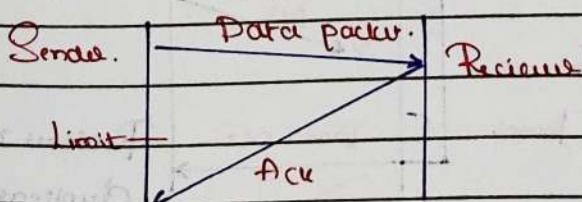
- * Sender wait for ACK for an infinite amount of time.
- * Receiver wait for data an infinite amount of time

2. Lost acknowledgement



- * Sender waits for the acknowledgement for an infinite amount of time.

3. Delay acknowledgement



- * Delay in acknowledgement might be wrongly considered as an ACK of some other packet.

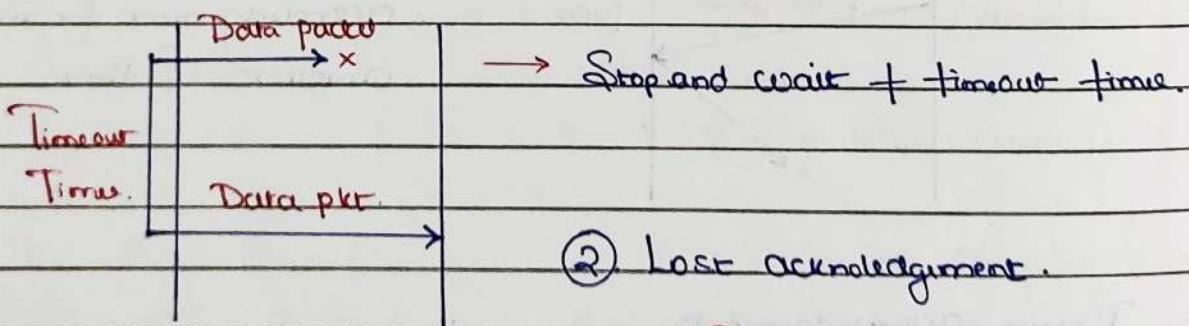
The above 3 problems are resolved by using Stop and wait ARQ (Automatic Repeat Request)

Stop and Wait ARQ.

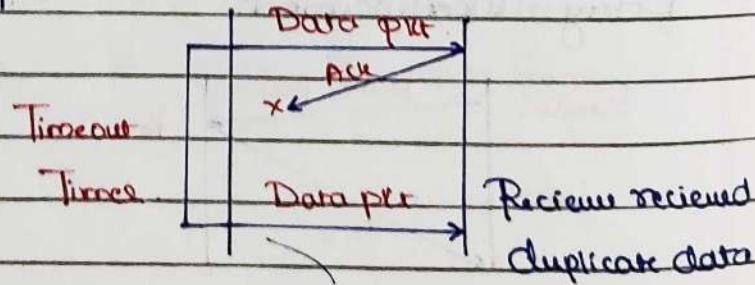
1. It provides both error control and flow control.
2. Error Control in Stop and wait ARQ is done by keeping a copy of sent frame until it receives an acknowledgement.
3. Sender Starts a timer when it sends a frame. If ACK is not found/received within the allocated time period, the Sender assumes that the frame was lost or damaged and resends it.
4. Receiver sends an acknowledgement to Sender if it received a frame correctly.
5. ACK number always defines the number of the next expected frame.
6. Stop and wait ARQ = Stop and Wait + Timeout + Sequence number (Data) + Sequence number (ACK).

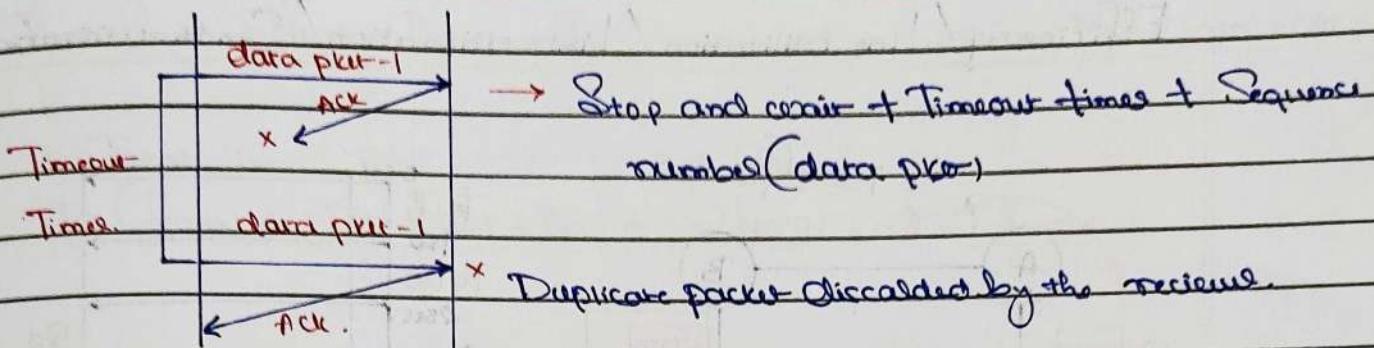
Solutions:

① Lost Data packet.

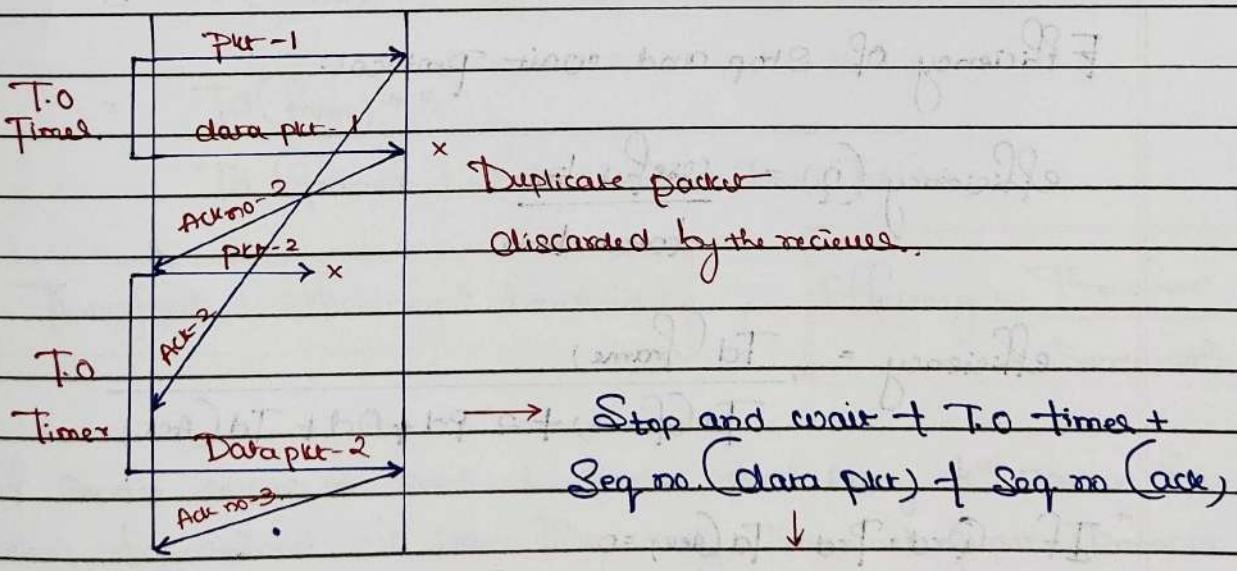
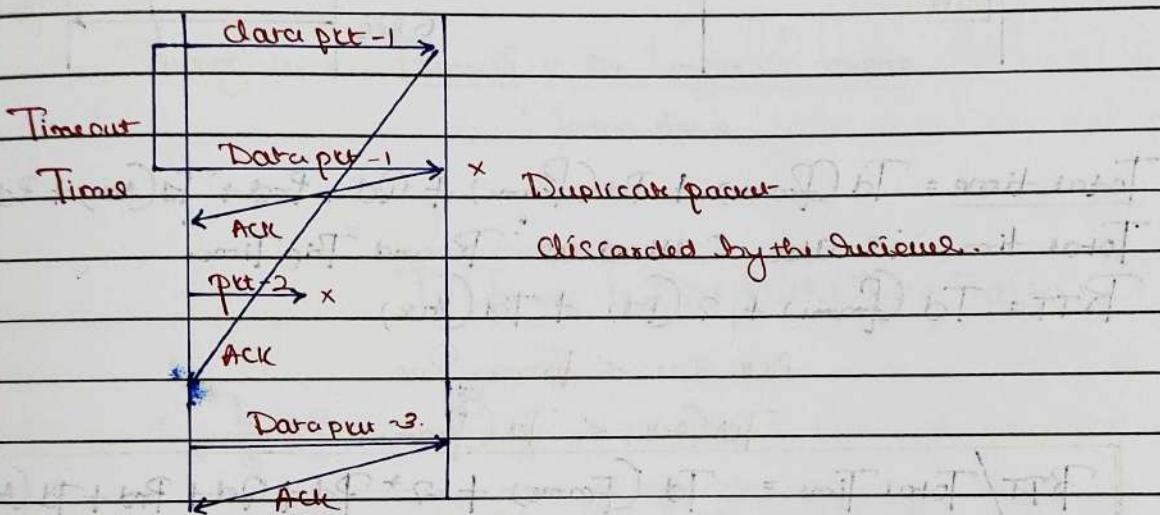


② Lost acknowledgement.

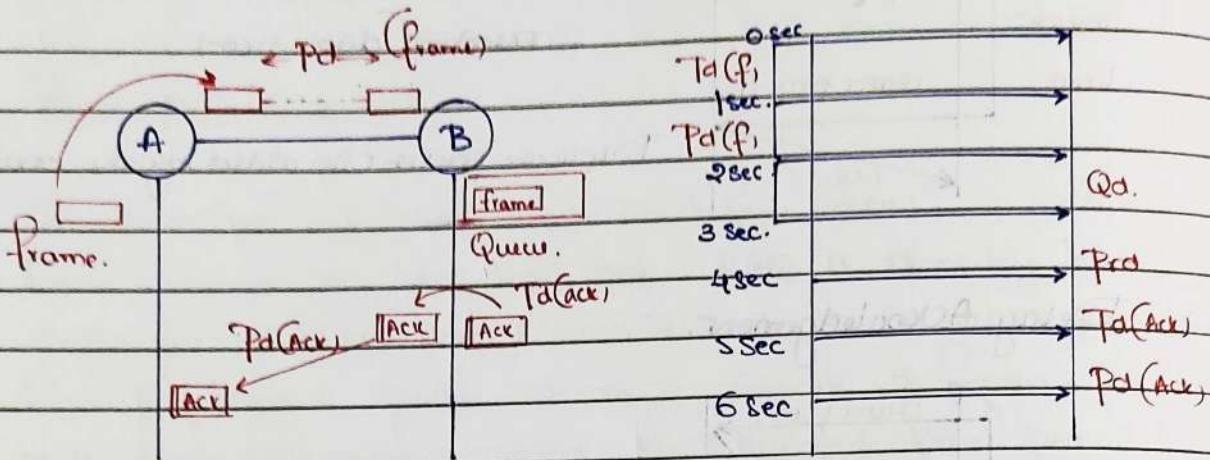




③ Delay acknowledgement.



Efficiency / Line utilization / Link utilization / Sender utilization:



$$\text{Total time} = T_d(\text{Frame}) + P_d(\text{Frame}) + Q_d + P_d + T_d(\text{Ack}) + P_d(\text{Ack})$$

Total time is also called as "Round Trip Time".

$$RTT = T_d(\text{Frame}) + 2 \cdot P_d + T_d(\text{Ack})$$

Ack Size < Frame Size

$$T_d(\text{Ack}) < T_d(\text{Frame})$$

$$\boxed{RTT/\text{Total Time} = T_d(\text{Frame}) + 2 \cdot P_d + Q_d + P_d + T_d(\text{Ack})}$$

Efficiency of stop and wait protocol:

$$\text{efficiency} (\eta) = \frac{\text{useful time}}{\text{total time}}$$

$$\text{efficiency} = \frac{T_d(\text{Frame})}{T_d(\text{Frame}) + 2 \cdot P_d + Q_d + T_d(\text{Ack})}$$

$$\star \text{ If } Q_d \cdot P_d = T_d(\text{Ack}) = 0$$

$$\text{then Total time} = T_d(\text{Frame}) + 2 \cdot P_d + Q_d + P_d + T_d(\text{Ack})$$

$$\text{Total time} = T_d(\text{Frame}) + 2 \cdot P_d$$

$$\text{efficiency} = \frac{\text{useful time}}{\text{total time}}$$

Throughput / Effective Bandwidth / Bandwidth utilization / Max. Data rate.

$$\text{Total time} \longrightarrow 1 \text{ Frame}$$

$$\frac{T_d(\text{frame}) + 2^* P_d + Q_d + P_{rd} + T_d(\text{Ack})}{10 \text{ Sec}} \longrightarrow 1 \text{ Frame}$$

$$10 \text{ Sec} \longrightarrow 1000 \text{ bits}$$

$$1 \text{ sec} \longrightarrow \frac{1000}{10} = 100 \text{ bits/sec}$$

$$\text{Throughput} = \frac{\text{Frame Size or Length of frame}}{\text{Total time}}$$

$$= \frac{L}{T_d(\text{frame}) + 2^* P_d + Q_d + P_{rd} + T_d(\text{Ack})}$$

$$= \frac{L}{B} \times B$$

$$T_d(\text{frame}) + 2^* P_d + Q_d + P_{rd} + T_d(\text{Ack})$$

$$= \frac{T_d(\text{frame}) + B}{T_d(\text{frame}) + 2^* P_d + Q_d + P_{rd} + T_d(\text{Ack})}$$

$$\boxed{\text{Throughput} = \text{efficiency} * \text{bandwidth}}$$

$$\boxed{\text{Efficiency} = \frac{\text{Throughput}}{\text{Bandwidth}}}$$

Q1. If sender want to send 10 packet and every 4th packet that is being transmitted is lost. By using Stop and wait protocol how many total transmission are required?

Ans 1 2 3 4 5 6 7 8 9 X 10

Total transmission = 13

No. of retransmission = 3.

Q2. If Sender want to send 500 packets on a link having a error probability 0.2. A Stop and wait protocol is used to transfer data across the link, then how many total transmission are required?

Ans.

$$n = 500 \quad P = 0.2$$

$$\frac{n}{500} + \frac{nP}{500(0.2)} + \frac{nP \cdot P}{100(0.2)} + \frac{nP \cdot P^2}{20(0.2)^2}$$

$$500 + 100 + 20 + 4 =$$

$$n \left[\frac{1}{1-P} \right] = \frac{n}{1-P}$$

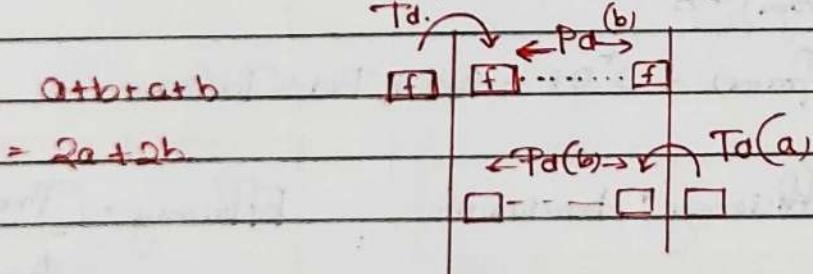
$$\text{Total transmission required} = \frac{n}{1-P}$$

$$= \frac{500}{1-0.2} = \frac{500}{0.8} = 625$$

Q3. Consider the Stop and wait protocol, if transmission time is 'a' at the source and propagation delay is 'b' then after what time the sender can send the second packet?

Consider the data packet and ACK packet of same size.

Ans.



Q4. A series of a 1000 bit frame is to be transmitted across a data link of 100 km in length with 20Mbps. If the link has a velocity of propagation 2×10^8 m/sec then the efficiency of stop and wait protocol is ____%.

Ans.

$$\text{Frame Size} = 1000 \text{ bits}$$

$$d = 100 \text{ km}$$

$$\text{Bandwidth} = 20 \text{ Mbps}$$

$$= 20 \times 10^6 \text{ bits/sec}$$

$$T_d(\text{frame}) = \frac{L}{B}$$

$$= \frac{1000 \text{ bits}}{20 \times 10^6 \text{ bits/sec}} = 0.05 \text{ sec}$$

$$V = 2 \times 10^8 \text{ km/sec.}$$

$$Pd \cdot \frac{d}{V} = \frac{100 \text{ km}}{2 \times 10^8 \text{ km/sec}} = 0.5 \text{ msec.}$$

$$\text{efficiency} = \frac{T_d(\text{frame})}{T_d(\text{frame}) + 2^* Pd + \text{Lat} + \text{Rdt} + T_d(\text{ACK})}$$

$$= \frac{0.05 \text{ msec}}{0.05 \text{ msec} + 2^* 0.5 \text{ msec}}$$

$$= \frac{0.05}{1.05} = \frac{5}{105} = 0.04761$$

$$\eta = \underline{47.61\%}$$

Q5 If the bandwidth of the line is 1.5 Mbps, RTT is 45 msec and frame size is 8192 bytes, then the efficiency in stop and wait protocol is ____ %.

$$\text{Ans } B = 1.5 \text{ Mbps} \\ = 1.5 \times 10^6 \text{ bytes/sec}$$

$$RTT = 45 \text{ msec}$$

$$T_d(\text{frame}) = \frac{8192 \text{ bytes}}{1.5 \times 10^6 \text{ bytes/sec}}$$

$$\eta = \frac{T_d(\text{frame})}{RTT} = \frac{5461.33 \times 10^{-6} \text{ sec}}{45 \text{ msec}} = \underline{5.461 \text{ msec}}$$

$$= \frac{5.461 \text{ msec}}{45 \text{ msec}} = 0.1213$$

$$\eta = \underline{12.13\%}$$

Q6. A sender uses the Stop and wait ARQ protocol for reliable transmission of frames. Frames are of size 1000 bytes and the transmission rate at the sender is 80 kbps. Size of an acknowledgement is 100 bytes and the transmission rate at the receiver is 8 kbps. The one way propagation delay is 100 milliseconds. Assuming no frame is lost, the sender throughput is 2500 bytes/sec.

$$\text{Frame size} = 1000 \text{ bytes} \\ = 8000 \text{ bits.}$$

$$\text{Ack size} = 100 \text{ Byte}$$

$$B = 80 \text{ kbps} = \frac{80 \times 10^3 \text{ bits/sec}}{8 \times 10^3 \text{ bits/sec}} = 10 \text{ sec.}$$

(Receiver)

$$Pd = 100 \text{ msec.} = \frac{100 \times 10^3}{10} \text{ sec.}$$

$T_d(\text{frame})$

$$= \frac{8000}{8 \times 10^3} \text{ bit/sec}$$

$$= \frac{1}{10} \text{ sec}$$

$$T_d(\text{Ack}) = \frac{800 \text{ bit}}{8 \times 10^3 \text{ bit/sec}}$$

$$= \frac{1}{10} \text{ sec}$$

$$\text{Throughput} = \frac{\text{Frame Size}}{T_d(\text{frame}) + 2 * P_d + Q_d + T_{\text{prop}} + T_d(\text{Ack})}$$

$$= \frac{8000 \text{ bit}}{10 \text{ sec} + 2 * \frac{1}{10} \text{ sec} + \frac{1}{10} \text{ sec}}$$

$$= \frac{8000}{10.2 \text{ sec}} = 20,000 \text{ bit/sec}$$

$$= \frac{1}{10} \text{ sec} + \frac{1}{10} \text{ sec} + \frac{1}{10} \text{ sec}$$

$$= \frac{1}{10} \text{ sec} = \frac{2000}{8} \text{ bit}$$

$$= \underline{250 \text{ byte/sec}}$$

Q7. The values of parameters for the Stop and wait ARQ protocol are given below:

Bit rate of the transmission channel = 1Mbps, Prop delay = 0.75ms

Time to process a frame = 0.25 ms

Number of byte in the information frame = 1980 (payload)

No. of overhead byte in the information frame = 20 (H)

No. of byte in the acknowledgement frame = 20

Assume no transmission error. Then the transmission efficiency of Stop and wait ARQ for the above parameters is

Ans.

$$B = 1 \text{ Mbps} = 10^6 \text{ bit/sec}$$

$$Ack = 20 \text{ byte} = 160 \text{ bit}$$

$$P_d = 0.75 \text{ msec}$$

$$P_d(\text{Ack}) = \frac{\text{Ack Size}}{\text{Bandwidth}}$$

$$P_{rd} = 0.25 \text{ msec}$$

$$\text{Bandwidth}$$

$$\text{Frame Size} = \text{data} + \text{header}$$

$$= \underline{160}$$

$$= 1980 + 20 = 2000 \text{ Byte}$$

$$10^6 \text{ bit/sec} = 0.16 \times 10^3 \text{ sec}$$

$$= 16,000 \text{ bytes}$$

$$= \underline{0.16 \text{ msec}}$$

$$P_d(\text{frame}) = \frac{\text{Frame Size}}{\text{Bandwidth}}$$

$$= \frac{16,000}{10^6} = 16 \times 10^{-3} = \underline{16 \text{ msec}}$$

$$\eta = \frac{T_d(\text{frame})}{T_d(\text{frame}) + 2^*pd + pd + Pd + T_d(\text{ack})}$$

$$= \frac{16}{16 + 2^*0.75 + 0.25 + 0.16}$$

$$= \frac{16}{17.91} = 0.8933$$

$$\eta = \underline{\underline{0.8933}}$$

Q8. A link has a transmission speed of 10^6 bits/sec. It uses data packets of size 1000 bytes each. Assume that the acknowledgement has negligible transmission delay, and its propagation delay is same as that of data propagation delay. Also assume that the processing delays at node are negligible. The efficiency of Stop and wait protocol in this setup is exactly 25%. The value of the one-way delay in msec is?

$$\text{Ans } B = 10^6 \text{ bits/sec}$$

$$\eta = 25\% = \frac{1}{4}$$

$$\text{Data packet size} = 1000 \text{ Byte} \\ = 8000 \text{ bits}$$

$$T_d(\text{frame}) = \frac{8000 \text{ bits}}{10^6 \text{ bits/sec}}$$

$$= 8 \times 10^{-3} \text{ sec} = \underline{\underline{8 \text{ msec}}}$$

$$\text{efficiency} = \frac{1}{4} = \frac{T_d(\text{frame})}{T_d(\text{frame}) + 2^*pd + pd + Pd + T_d(\text{ack})}$$

$$T_d(\text{frame}) + 2^*pd + pd + Pd + T_d(\text{ack})$$

$$\Rightarrow \frac{1}{4} = \frac{8}{8 + 2^*pd} = 8 + 2^*pd = 32$$

$$2^*pd = 32 - 8$$

$$2^*pd = 24 \text{ msec.}$$

$$pd = \frac{24}{2} \text{ msec.}$$

$$Pd = 12 \text{ msec.}$$

Q9. Suppose that the Stop and wait ARQ is used on a link with a bit rate of 64 kb/sec and 20 msec prop. delay. Assume that the transmission time for the acknowledgement and the processing time at node are negligible. Then the min frame size in bytes to achieve a link utilization of atleast 50% is

$$\text{Ans } B = 64 \times 10^3 \text{ bits/sec}, Pd = 20 \text{ msec}, \text{ Frame Size } L = ?$$

$$\text{efficiency} \geq 50\% \cdot \left(\frac{1}{2}\right)$$

$$\text{efficiency} = \frac{\text{useful time}}{\text{total time}} = \frac{1}{2}$$

$$\frac{T_d(\text{frame})}{T_d(\text{frame}) + T_d \cdot 2 + P_d + P_{rd} + T_d(\text{Ack})} \geq \frac{1}{2}$$

$$\frac{T_d C}{T_d + 2^* P_d} \Rightarrow 2^* T_d = T_d + 2^* P_d \\ T_d \geq 2^* P_d$$

$$\frac{L}{B} \geq 2^* P_d$$

$$L \geq 2^* P_d * B$$

$$L \geq 2^* 20 \times 10^3 \text{ sec} \times 64 \times 10^3 \text{ bits/sec}$$

$$L \geq 40 \times 64 \text{ bits}$$

$$L \geq \frac{40 \times 64^8}{8} \text{ bytes}$$

$$L \geq 320 \text{ Byte}$$

Frame Size.

Q10. A channel has a bit rate of 4 kbps and one-way propagation delay of 20 ms. The channel uses Stop and wait protocol. The transmission time of the acknowledgement frame is negligible. To get a channel efficiency of atleast 50%. the min frame size should be?

Ans

$$B = 4 \times 10^3 \text{ bits/sec}$$

$$L \geq 2^* P_d * B$$

$$P_d = 20 \text{ ms/sec}$$

$$L \geq 2^* 20 \times 10^3 \text{ sec} \times 4 \times 10^3 \text{ bits/sec.}$$

$$L \geq 160 \text{ bits}$$

Q11. On a wireless link, the probability of packet is 0.2. A stop and wait ~~ack~~ protocol is used to transfer data across the link. The channel condition is assumed to be independent from transmission to transmission. Avg no. of packet attempts required to transfer 100 packets?

Ans

$$P = 0.2 \quad \text{Total transmission} = ? = \frac{100}{1-P} = \frac{100}{1-0.2} = \frac{1000}{8} = \underline{\underline{125}}$$

Q12. A channel has a bit rate of 4 kbps and one way propagation delay of 10 ms. The channel uses Stop and wait protocol. The transmission time of the acknowledgement frame is negligible. To get a channel efficiency of atleast 75%, the min frame size?

Ans $B = 4 \times 10^3 \text{ bits/sec}$ $P_d = 10 \text{ m.sec} = 10 \times 10^{-3} \text{ sec}$

$$\text{efficiency} \geq 75\% \quad \left(\frac{3}{4}\right)$$

$$\text{efficiency} \geq \frac{3}{4}$$

$$T_d(\text{frame})$$

$$\geq \frac{3}{4}$$

$$T_d(\text{frame}) + 2 \cdot P_d + Q_d + P_{\text{ack}} + T_d(\text{Ack})$$

$$T_d(\text{frame}) \geq \frac{3}{4}$$

$$T_d(\text{frame}) + 2 \cdot P_d \geq \frac{3}{4}$$

$$L_p \cdot T_d(\text{frame}) \geq 3 \cdot T_d(\text{frame})$$

$$T_d(\text{frame}) \geq 6 \cdot P_d$$

$$\frac{L}{B} \geq 6 \cdot P_d$$

$$L \geq 6 \cdot P_d \times \text{Bandwidth}$$

$$L \geq 6 \cdot 10 \times 10^3 \text{ sec} \times 4 \times 10^3 \text{ bits/sec}$$

$$L \geq 240 \text{ bits (frame size)}$$

Q13. Consider a wireless link, where error probability is 0.6 to transfer data across the link, Stop and wait protocol is used, the channel condition is assumed to be independent from transmission to transmission. The average no. of transmission attempts to transfer a packet is 500. The value x is

Ans

$$\text{Avg no. of transmission for 'n' pkt} = \frac{n}{1-P}$$

$$\frac{500}{1 - 0.4} = \frac{x}{0.4}$$

$$\text{Avg no. of transmission for 'x' pkt} = \frac{x}{1-P}$$

$$x = 500 \cdot 0.4$$

$$\frac{500}{1 - 0.6} = \underline{\underline{x}}$$

$$\underline{\underline{x}} = 200$$

Q14. Consider Stop and wait ARQ for flow control, data transfer rate of channel is 32 kbps, One way end to end propagation

delay is 16 ms and frame size is 32 bytes then efficiency percentage is

Ans

$$B = 32 \text{ Mbps}$$

$$= 32 \times 10^3 \text{ bits/sec}$$

$$Pd = 16 \text{ ms sec}$$

$$\text{Frame size} = 32 \text{ byte}$$

$$= 32 \times 8 \text{ bits}$$

$$= 256 \text{ bits}$$

$$T_d(\text{frame}) = \frac{\text{Frame size}}{\text{bandwidth}}$$

$$= \frac{32 \times 8 \text{ bits}}{32 \times 10^3 \text{ bits/sec}} = 8 \times 10^{-3} \text{ sec} = 8 \text{ msec}$$

$$\text{efficiency} = \frac{T_d(\text{frame})}{T_d(\text{frame}) + 2^* Pd + Qd + Prot + T_d(\text{Ack})} = \frac{8}{8 + 2^* 16} = \frac{8}{40} = \frac{1}{5}$$

$$\text{efficiency} = 20\%$$

Q15 Consider packet size is 1000 Bytes, distance between two hosts is 2000 Km, 1 Mbps link with 2×10^8 meter/sec. Signal speed, if Stop and Wait protocol is used then throughput is — (Mbps)

Ans.

$$\text{Packet size} = 1000 \text{ Bytes}, D = 2000 \text{ Km}$$

$$= 8000 \text{ bits}$$

$$V = 2 \times 10^8 \text{ m/sec}$$

$$V = 2 \times 10^5 \text{ km/sec}$$

$$B = 1 \text{ Mbps} = 10^6 \text{ bits/sec}$$

$$\text{efficiency} = \frac{T_d(\text{frame})}{T_d(\text{frame}) + 2^* Pd + Qd + Prot + T_d(\text{Ack})} = \frac{8000}{10^6 \text{ bits/sec}} = 8 \times 10^{-3} \text{ sec} = 8 \text{ msec}$$

$$Pd = \frac{D}{V} = \frac{2000 \text{ Km}}{2 \times 10^5 \text{ km/sec}} = 10 \times 10^{-3} \text{ sec}$$

$$= 10 \text{ msec}$$

$$\text{efficiency} = \frac{T_d(\text{frame})}{T_d(\text{frame}) + 2^* Pd}$$

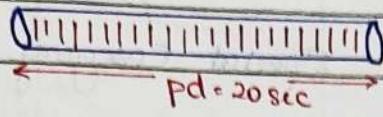
$$= \frac{8}{8 + 2^* 10} = \frac{8}{28}$$

$$\text{Throughput} = \text{efficiency} \times B$$

$$= \frac{8}{28} \times 1 \text{ Mbps}$$

$$= 0.285 \text{ Mbps}$$

Capacity of Link/wire/Channel



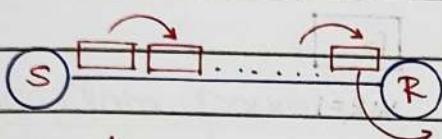
$$B = 1 \text{ bps} = 1 \text{ bit/sec}$$

$$\text{Capacity of Line} = 1 \text{ bit/sec} * 20 \text{ sec}$$

$$\text{Capacity of Link} = 20 \text{ sec bit}$$

$$\text{Capacity of the Link} = B * pd$$

eg::



$$B = 1 \text{ bit/sec}$$

$$pd = 10 \text{ sec}$$

$$\text{Capacity of the Link} = 1 \text{ bit/sec} * 10 \text{ sec}$$

$$\text{Capacity of Link} = B * pd$$

Q1. Bandwidth = 1Mbps and pd = 1 sec and packet size = 1000 bits, then how many packets can be transit at a time?

Ans $\text{Capacity of Link} = B * pd$

$$= 10^6 \text{ bits/sec} * 1 \text{ sec}$$

$$= 10^6$$

$$\text{no. of packets} = \frac{10^6}{10^3} = 10^3 \text{ packets can be in transit}$$

Q2. If bandwidth = 1Mbps and propagation delay is 10sec and packet size is 100 bits/sec. Find the no. of packets needed to maximally pack the link..?

Ans $(\text{Capacity of the link})$

$$\text{Capacity of Link} = B * pd$$

$$= 10^6 \text{ bits/sec} * 10^3 \text{ sec}$$

$$= 10^9 \text{ bits} = 1000 \text{ bin.}$$

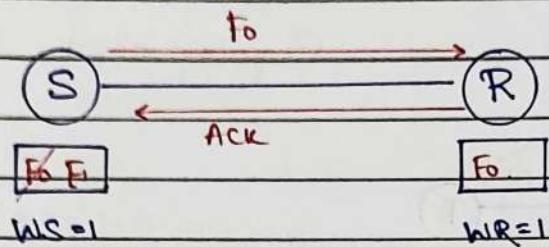
$$\text{No of packets}$$

$$= \frac{1000}{100}$$

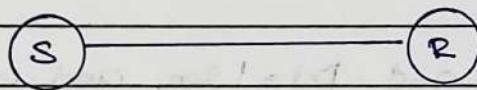
$$= 10 \text{ packets}$$

Important point about Stop and wait protocol

- Stop and wait Protocol is a Special Category of Protocols where window size = 1 Always.



- Stop and wait Protocol uses two Sequence number i.e. 0 and 1, irrespective of number of packet Sender is having

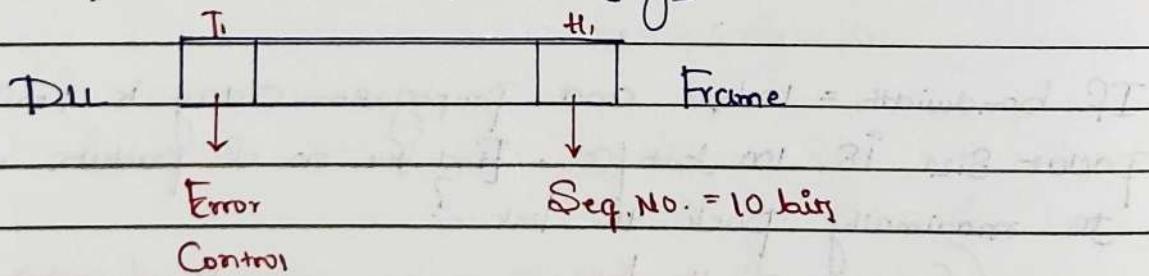


Sender wants to send 1000 frames to receiver.

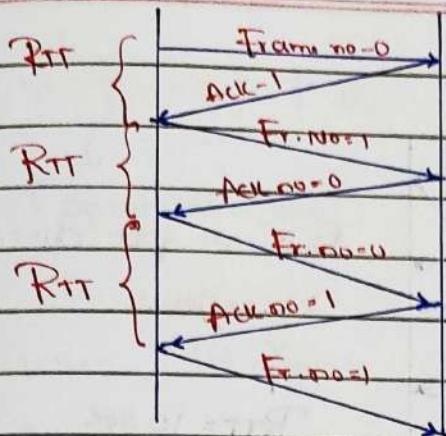
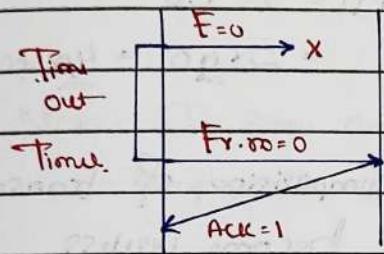
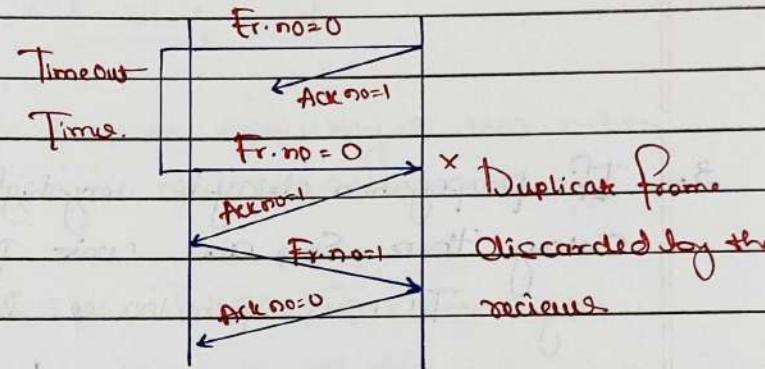
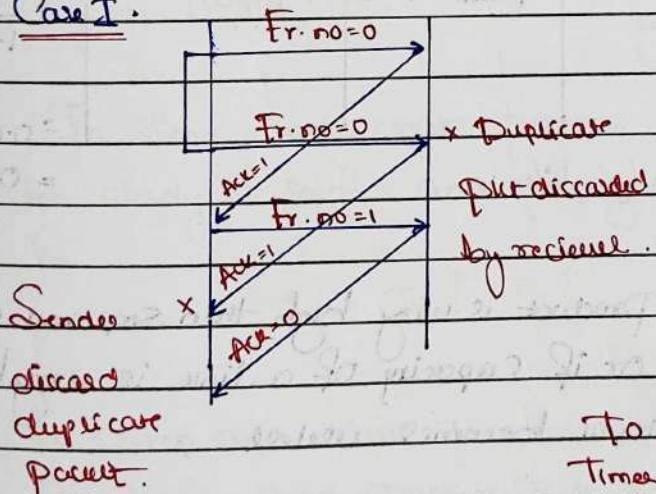
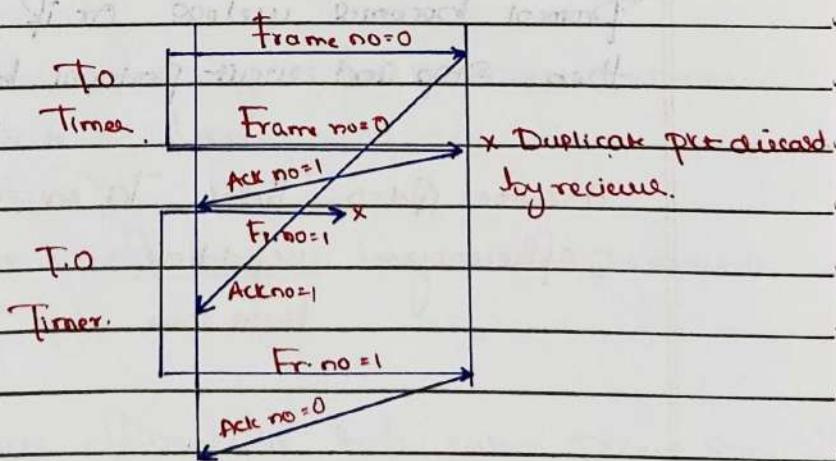
Fo F1 F2 F3 5999
0 1 2 3 999

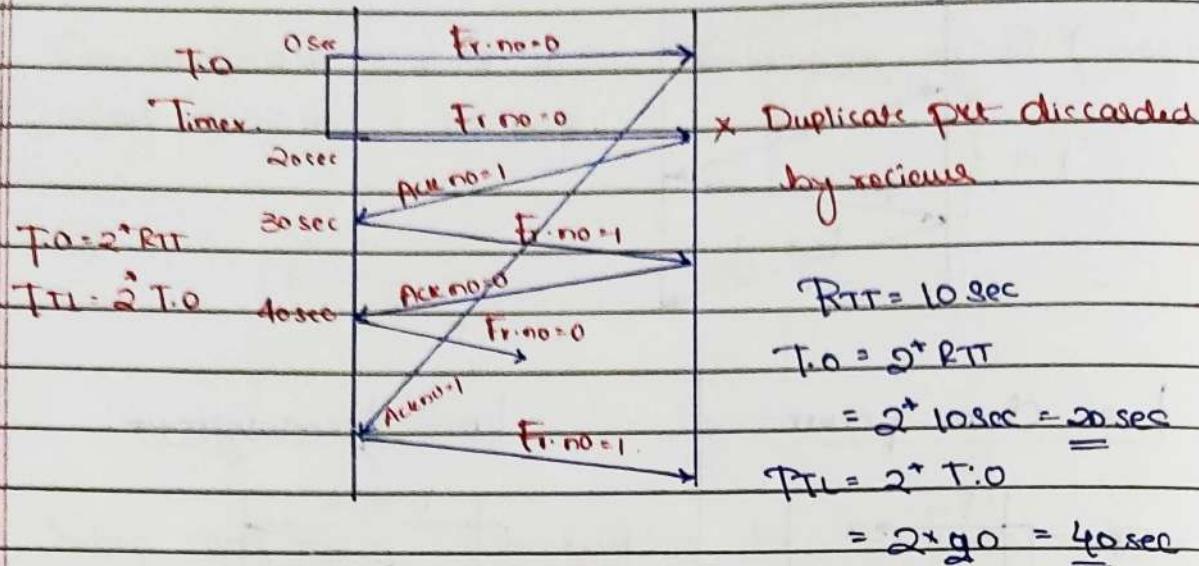
Total Sequence number required = 1000

No. of bits required = $\lceil \log_2 1000 \rceil = 10 \text{ bit}$.



10 bits overhead for one byte. To send 1000 frames
total overhead = $10 * 1000 = 10,000 \text{ bits}$.

Lost Data packet.Lost Acknowledgement.Delay in acknowledgement.Case I.Case II

Case III

3. If propagation delay is very high in comparison of transmission delay then Stop and wait protocol become useless.

e.g.: $T_d = 1 \text{ sec}$, $P_d = 100 \text{ sec}$, $Q_d = 0$, $P_{rd} = 0$, $T_d(\text{Ack})$

$$\begin{aligned}\text{efficiency} &= \frac{T_d(\text{frame})}{T_d(\text{frame}) + 2^* P_d} \\ &= \frac{1}{1 + 2^* 100} \\ &= \frac{1}{201} = 0.0049 \\ &= \underline{\underline{0.49\%}} (\leq 1\%) \end{aligned}$$

| $T_d = 1 \text{ sec}$ | $P_d = 100 \text{ sec}$ | $\eta = \frac{\text{useful time}}{\text{total time}}$ |
|------------------------|----------------------------------|--|
| Waiting time = 200 sec | $P_d = 100 \text{ sec}$ (Ack) | $= \frac{1}{1+200} = \underline{\underline{0.0049}}$ $= 0.49\%$ |

4. If (bandwidth and delay) Product is very high then stop and wait protocol become useless or if capacity of a link is very high then stop and wait protocol becomes useless.

Assume $Q_d = 0$, $P_{rd} = 0$, $T_d(\text{Ack}) = 0$

$$\text{efficiency} = \frac{\text{useful time}}{\text{total time}} = \frac{P_d}{T_d + 2^* P_d} = \frac{T_d}{T_d \left[1 + 2^* \frac{P_d}{T_d} \right]}$$

$$\eta = \frac{1}{1 + 2^{\frac{P_d + B}{L}}} - \uparrow \text{ then } \eta \downarrow.$$

↓

Capacity of a link

4. $T_d = 1 \text{ sec}$, $P_d = 100 \text{ sec}$, $Q_d = 0$, $P_{rd} = 0$, $T_d(\text{Ack}) = 0$

$$\eta = \frac{T_d}{T_d + 2^{\frac{P_d + Q_d + P_{rd} + T_d(\text{Ack})}{L}}}$$

$$\eta = \frac{T_d}{T_d + 2^{\frac{P_d}{L}}}$$

$$\eta = \frac{1}{1 + 2^{\frac{P_d}{L}}} = \frac{1}{2^{10}} = 0.0049 = 0.49\%$$

Note: In Stop and wait protocol efficiency is low when propagation delay is high and transmission delay is low.

5. $T_d = 100 \text{ sec}$, $P_d = 1 \text{ sec}$, $Q_d = 0$, $P_{rd} = 0$, $T_d(\text{Ack}) = 0$

$$\begin{aligned} \eta &= \frac{T_d}{T_d + 2^{\frac{P_d}{L}}} \\ &= \frac{100}{100 + 2^{10}} = \frac{100}{102} = 0.9830 = 98.30\% \end{aligned}$$

In Stop and wait protocol efficiency is high when transmission delay is high and propagation delay is low.

$P_d \downarrow T_d \uparrow \eta \uparrow$

6. To stop and wait protocol efficiency is low when distance is high and packet size is less.

7. To stop and wait protocol efficiency is low when distance is high and bandwidth is high

8. To stop and wait protocol efficiency is high when packet size

is high and Distance is low.

Q.

$$\eta = \frac{T_d}{T_d + 2^* P_d} = \frac{T_d}{T_d \left[1 + 2^* \frac{P_d}{T_d} \right]}$$

$$\eta = \frac{1}{1 + 2^* \frac{d}{v} + \frac{B}{L}}$$

$v \rightarrow$ Fixed
 $B \rightarrow$ Fixed

$d \uparrow \quad \eta \downarrow$: η is good for LAN

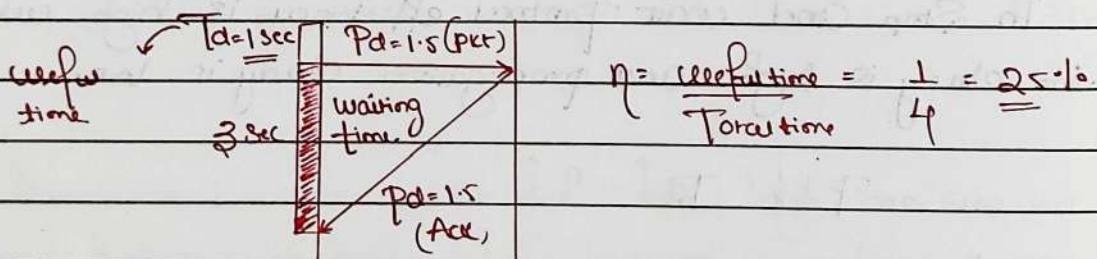
$L \uparrow \quad \eta \uparrow$: η is good for Large packet.

Q. Suppose two hosts are connected by a point-to-point link and they are configured to use Stop and Wait protocol for reliable data transfer. Identify in which of the following scenarios, the link utilization is the lowest.

Ans Longer link length and higher transmission rate.

e.g. $T_d = 1 \text{ sec}$, $P_d = 1.5 \text{ sec}$, $\eta = ?$

$$\eta = \frac{T_d}{T_d + 2^* P_d} = \frac{1}{1 + 2^* 1.5} = \frac{1}{4} = 25\%$$



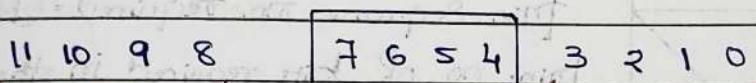
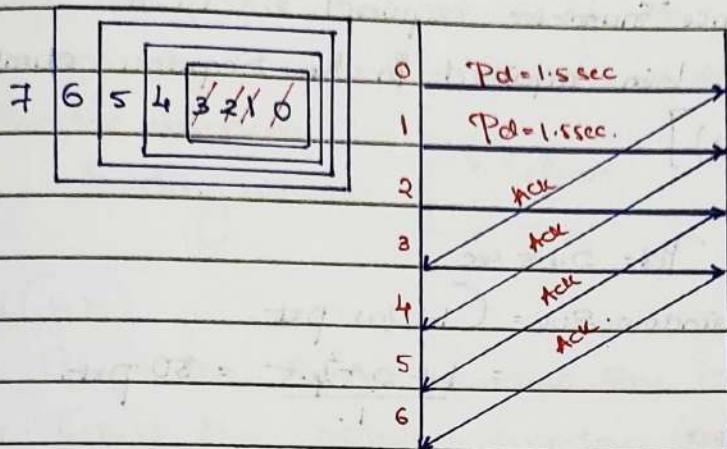
e.g.: $T_d = 1 \text{ sec}$, $P_d = 1.5 \text{ sec}$

$$\text{maximum window size} = (1 + 2^a) \text{ pkt}$$

$$= 1 + 2^* \frac{1.5}{1}$$

$$= 4 \text{ pkt}$$

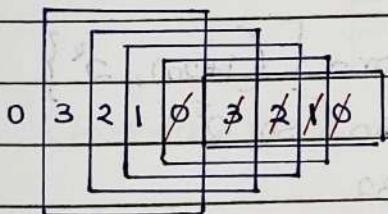
Sliding Window



New to be transmitted & not acknowledged

e.g.:

$$\begin{aligned} T_d &= 1.8 \text{ sec}, P_d = 1.5 \text{ sec} \\ \text{max window size} &= (1+2\alpha) \text{ pkt} \\ &= 1+2 \times \frac{1.5}{1} = 4 \text{ pkt} \end{aligned}$$



This no. of bits required in the Sequence no. field = 2 bits

$$\begin{aligned} \{00, 01, 10, 11\} \\ = [\log_2 (1+2\alpha)] \end{aligned}$$

$$= [\log_2 4]$$

$$= [\log_2 2^2] = 2 [\log_2 2] = 2 \text{ bits}$$

Maximum window size = $(1+2a)$ pkt.

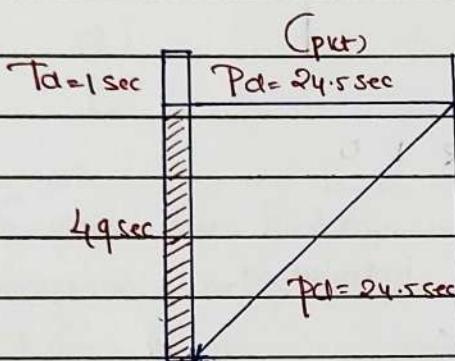
Minimum sequence number required = $(1+2a)$

Minimum no. of bits required in the sequence number field
 $= \lceil \log_2 (1+2a) \rceil$

e.g.: $T_d = 1$ sec, $P_d = 24.5$ sec

$$\text{Max. window size} = (1+2a) \text{ pkt}$$

$$= 1 + 2^{\frac{2}{24.5}} = 50 \text{ pkt.}$$



$$\text{Min sequence no. required} = (1+2a) = 50$$

min. no. of bits required in the sequence

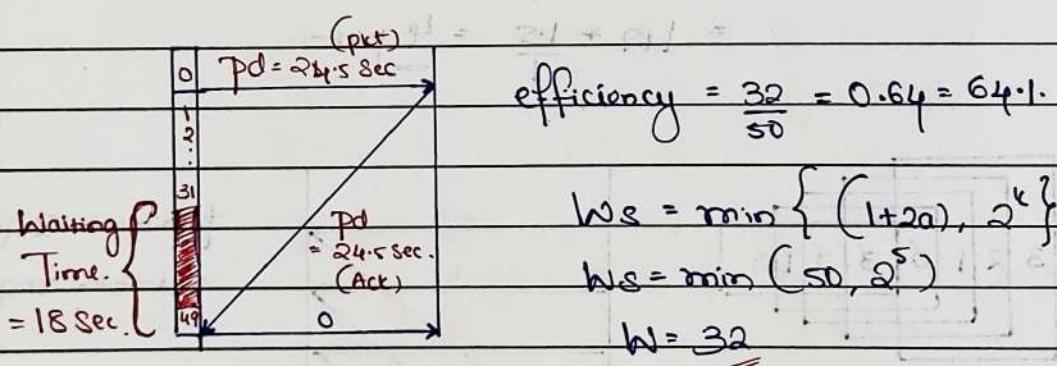
$$\text{number of fields} = \lceil \log_2 (1+2a) \rceil$$

$$= \lceil \log_2 50 \rceil$$

$$= 5.67 = 6 \text{ bits.}$$

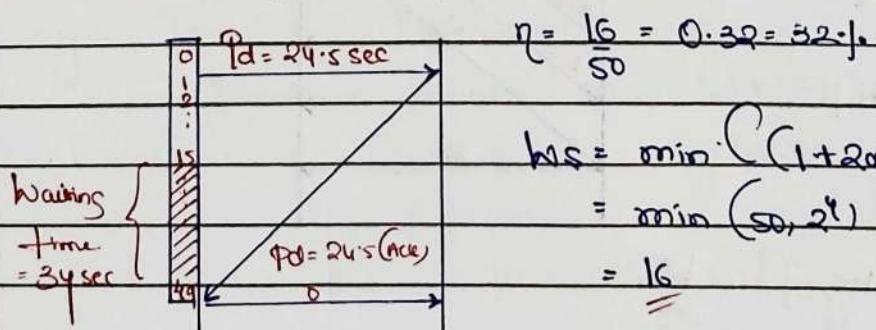
Case I: Sequence no. (k) = 5 bit

$$\text{Total Sequence No.} = 2^5 = 32 \quad (0-31)$$

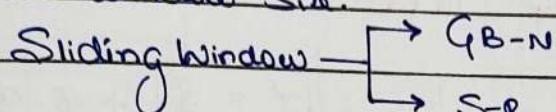


Case II: Sequence no. (k) = 4 bit

$$\text{Total Sequence number} = 2^4 = 16 \quad (0-15)$$

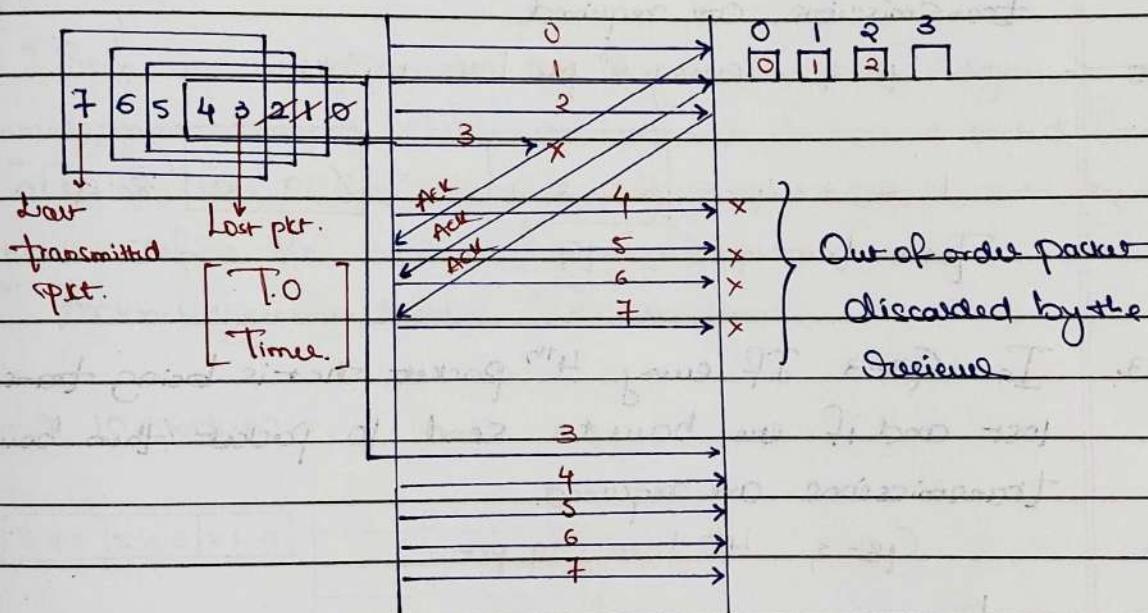


Sliding Window: In the Sliding window concept instead of sending one packet and wait for the acknowledgement, we send 'w' packets and wait for the acknowledgement, where 'w' is the Sender window size.

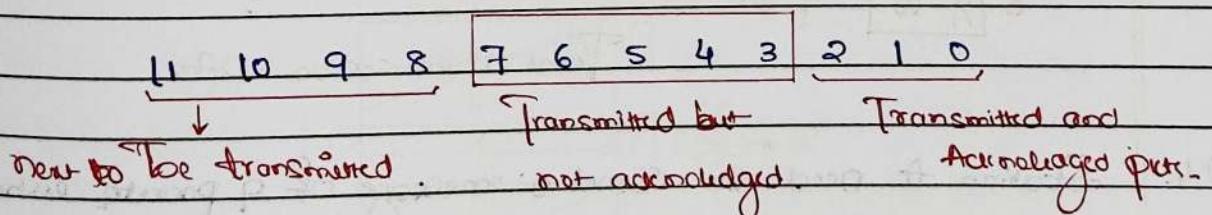


GB-N ($N \geq 1$)

1. In the GB-N the Sender window size is N itself.
2. In the GB-N the receiver window size is equal to one always ($W_r = 1$)



Note: * Go-back-N is from last transmitted packet



- * Out of order packet is not retransmitted by the receiver.
- * Timer is maintained only for the first frame (rightmost) in the window because if timer expires then sender assumes that rest of the frames are not received by the receiver (because Out of order packet is rejected).

Q1. In GB-3, if every 5th packet that is being transmitted is lost and if we have to send 10 packets, then how many transmissions are required.

Ans.

GB-3, 5th lost, 10 pkt.

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|--|---|----|
| 1 | 2 | 3 | 4 | ↙ | 6 | 7 | 5 | 6 | ↗ | 8 | 9 | 7 | 8 | ↗ | 10 | | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|--|---|----|

Total transmission = 18

Q2. In GB-4, if every 6th packet that is being transmitted is lost and if we have to send 10 packets then how many total transmissions are required.

Ans.

GB-4, every 6th per lost, 10 pkt

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|--|---|---|----|
| 1 | 2 | 3 | 4 | 5 | ↙ | 7 | 8 | 9 | 6 | 7 | ↗ | 8 | 9 | 10 | | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|--|---|---|----|

Total transmission = 17

Q3. In GB-3 If every 4th packet that is being transmitted is lost and if we have to send 10 packets then how many transmissions are required.

Ans.

GB-3, 4th lost, 10 pkt.

↓

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|----|---|---|---|----|---|---|---|---|---|---|---|---|---|---|---|---|---|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 4 | ↙ | 6 | 7 | 5 | 6 | 7 | 8 | 6 | ↗ | 8 | 9 | 7 | ↗ | 9 | 10 |
| 8 | ↙ | 9 | 10 | | | 9 | 10 | | | | | | | | | | | | | | |

Total transmission = 27.

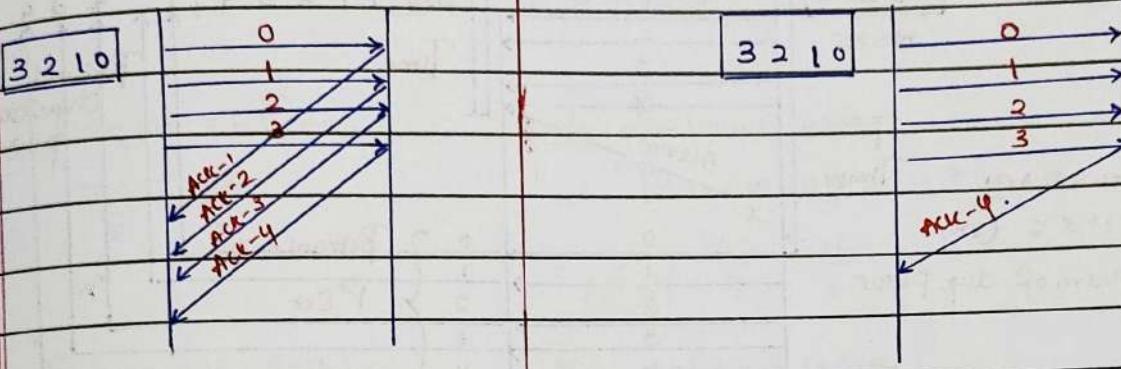
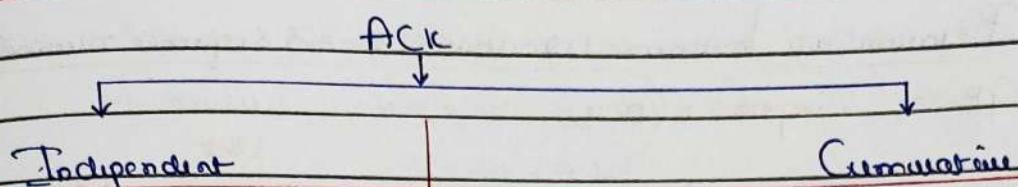
Q4. Station A needs to send a message of 9 packets where send window = 3. All packets are ready and immediately available for transmission. By using CBRN strategy, if 5th packet get lost, what will be the total transmission?

Ans.

WS=3, 5th lost, 9 packets

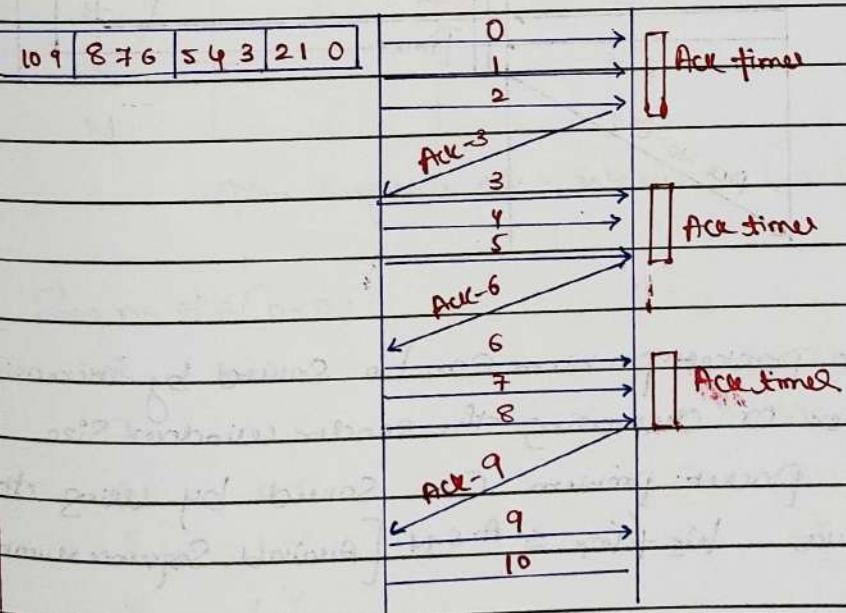
| | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|--|---|--|
| 1 | 2 | 3 | 4 | ↙ | 5 | 6 | 7 | 5 | 6 | ↗ | 7 | 8 | 9 | 7 | 8 | ↗ | 9 | | 9 | |
| | | | | | ↑ | | | ↑ | | | | | | | | | | | | |

Total transmission = 16

Note:

- * Stop and wait Protocol uses independent acknowledgement and acknowledgement number defines the number of next expected frame.
- * GB-N uses Cumulative acknowledgement and acknowledgement number defines the number of next expected frame.
- * Acknowledgement time < Time out time.

→ GB-3, 10 packets



$$\text{efficiency} = \frac{10 \times 5}{5 + 2^*25 + 2 + 0.5}$$

$$= \frac{50}{57.5} = 0.8695$$

$$\therefore \eta = 86.95\% \\ \underline{\underline{= 87\%}}$$

- Q4 Assume a sender send 6 packet (0-5). The sender receives an acknowledgement with ACKNO=3. What is the interpretation if the system is using GB-N
 Ans It means packet 0, 1, 2 have received uncorrupted and receiver expected packet 3.

Q5 In a Sliding window ARQ scheme, the transmitter's window size is n and the receiver's window size is m . The min no of distinct sequence numbers required to ensure correct operation of the ARQ scheme is.

$$\text{Ans } m+n$$

Q6 Consider packet size is 1000 bits. And distance between the two hosts is 5 Km, 1 Mbps link with signal speed 2ms/km is used, the efficiency is %. If N is set to 7 in GB-N

$$\text{Ans } \text{pk size} = 1000 \text{ bits} \quad B = 1 \text{ Mbps} = 10^6 \text{ bits/sec.}$$

$$d = 5 \text{ Km.}$$

$$\text{Propagation time} = 5 \times 2 \text{ ms.}$$

$$= 10 \text{ ms}$$

$$\text{Speed } v = 2 \text{ ms/km.}$$

$$T_d(\text{frame}) = \frac{1000 \text{ bits}}{10^6} = 10^{-3}$$

$$\eta = \frac{N \times T_d(\text{frame})}{T_d(\text{frame}) + 2^*p_d + Q_d + T_d(\text{Ack})}$$

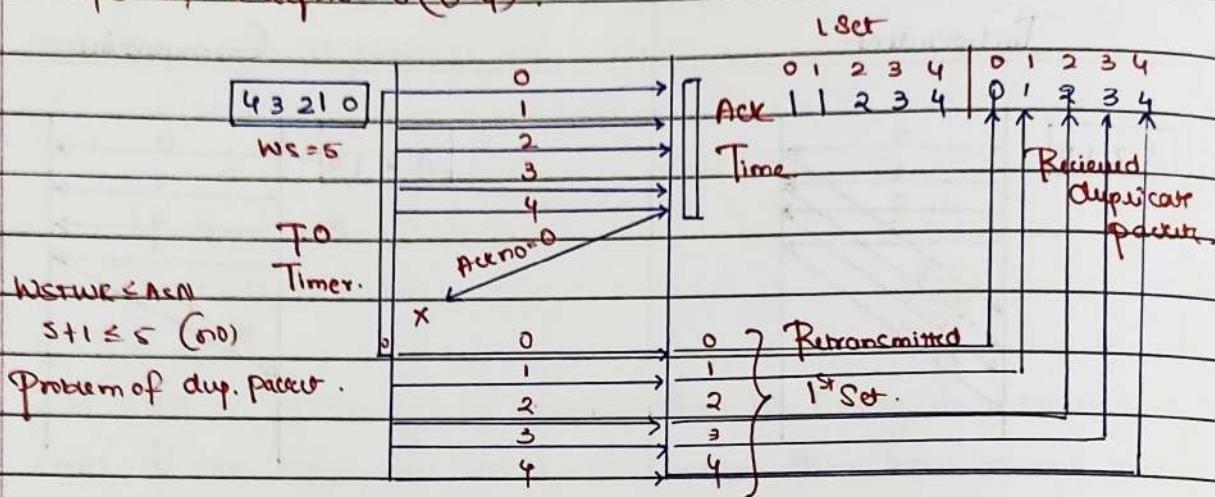
$$10^6 \cdot - 1 \text{ ms}$$

$$= \frac{7 \times 1}{1 + 2 \times 10} = \frac{7}{21} = \frac{1}{3} = \underline{\underline{33.33\%}}$$

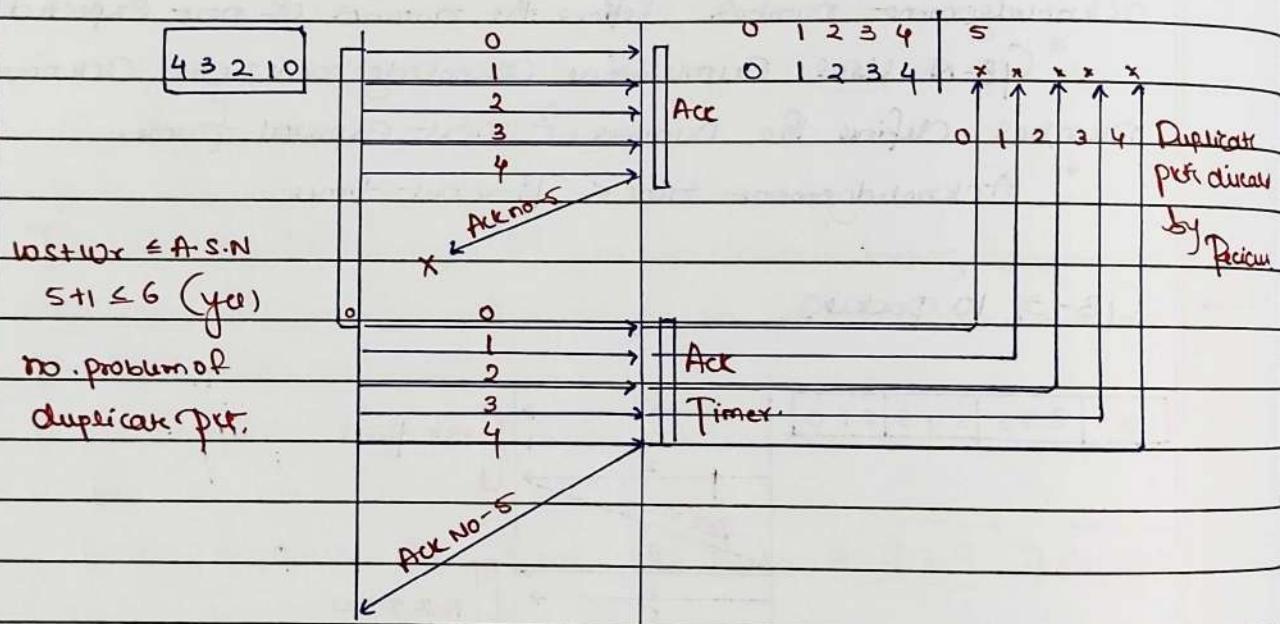
- Q7 In GB-N protocol the packet size is 1000 bytes transmission time for one packet is 1ms. If distance between hosts is 10km

Relationship between window size and sequence number

GB-5, Seqno = 5 (0-4).



GB-5, Sequence No = 6 (0-5)



Note:

- * Duplicate packet problem can be solved by increasing the Sequence Number or decreasing the sender window size.
- * Duplicate packet problem can be solved by using the following formula $WS + WR \leq A.S.N$ [Available Sequence Number]

WR Size = In GB-N the window receiver size is equal to one away irrespective of window sender size ($WR=1$)

And Signal Speed is 5ms Per Km ($\frac{m}{sec}/km$) and frame Sequence Number are 6 bit long in frame format thus throughput is 7Mbps is.

Ans

$$\text{Pkt Size} = 1000 \text{ Byte} = 8000 \text{ bits} \quad \text{Prop. time for } 1 \text{ Km} = 5 \text{ ms}$$

$$T_d = 1 \text{ msec} = 10^{-3} \text{ sec} \quad " " 10 \text{ Km} = 50 \text{ ms}$$

$$d = 10 \text{ Km}$$

$$\text{Seqno} = 6 \text{ bit}$$

GB-N

$$\text{Seqno} = k \text{ bit}$$

$$B = ?$$

$$\frac{w_s}{w_r} = \frac{w_s}{1} \quad T_d = \frac{L}{B}$$

$$2^k - 1 \quad 1$$

$$\frac{10^{-3} \text{ sec}}{1} = 8000 \text{ bits}$$

$$= \frac{63}{2^k - 1} \quad 1$$

$$B = \frac{8000}{10^{-3}} = 8 \times 10^6 \quad = 8 \text{ Mbps}$$

$$\text{efficiency} = \frac{63 \times 1}{1 + 2^k \times 50}$$

$$= \frac{63}{101}$$

$$\text{Throughput} = 2 \times B$$

$$= \frac{63 \times 8}{101} \text{ Mbps}$$

$$= 4.99 \text{ Mbps}$$

$$\approx 5 \text{ Mbps}$$

Q8 Host A is sending data to host B over a full duplex link. A and B are using S-W protocol. The $w_s = w_r = 5$ packets each. Data packets (sent only from A to B) are all 1000 byte long and transmission time for such a packet is 50μsec. acknowledgement packets (sent from B to A) are very small and negligible. The propagation delay over the link is 200μsec. What is max achievable throughput?

Ans.

$$w_s = 5, w_r = 5$$

$$\text{Throughput} = 5 \times 1000 \text{ Byte}$$

$$\text{Pkt size} = 1000 \text{ byte}$$

$$T_d(\text{frame}) + 2^k \cdot p_d + Q_d \cdot p_d + T_d(\text{ack})$$

$$T_d(\text{frame}) = 50 \mu\text{sec}$$

$$= 5000 \text{ byte}$$

$$p_d = 200 \mu\text{sec}$$

$$50 \mu\text{sec} + 2^k \cdot 200 \mu\text{sec}$$

$$= 5000 \text{ byte}$$

$$4.5 \times 10^{-5} \times 10^6 \text{ sec}$$

$$= 11.1 \times 10^6 \text{ byte/sec}$$

Q9. Consider GBN ARQ is used for flow control, frame size is 4000 bits, data transfer rate of channel is 1Mbps and one way propagation delay is 18ms, then what should be the window size of the sender, window size and min. number of bits required for sequence number field for max utilization is:

Ans. Frame size = 4000 bits, $B = 1 \text{ Mbps} = 10^6 \text{ bits/sec}$

$$T_d = 18 \text{ msec.}$$

$$T_d(\text{frame}) = \frac{L}{B} = \frac{4000}{10^6} = 4 \text{ msec}$$

$$\eta = \frac{N * T_d(\text{frame})}{T_d(\text{frame}) + 2^k P_d + Q_d + P_{dt} + T_d(\text{acc})} = \frac{1}{1 + \frac{N * 4}{4 + 2^k * 18}}$$

$$N = \frac{40}{4} = 10.$$

$$\text{Min. Seq. no required} = 10 + 1 \\ = 11.$$

$$2^k = 11.$$

$$2^k = 2^4, K = 4$$

Q10. Consider a network connecting two systems located 8000 km apart. The bandwidth of the network is $500 \times 10^6 \text{ bits/sec}$. The propagation speed of the media is $1 \text{ km } \mu \text{sec/sec}$. It is needed to design GBN sliding window protocol for this network. The average pkt size is 10^7 bits . The network is used to be used at its full capacity. Assume that processing delay at nodes are negligible, the min. size in bits of seq. no. field has to be.

Ans. $d = 8000 \text{ km}$, $B = 500 \times 10^6 \text{ bits/sec}$

$$v = 4 \times 10^8 \text{ m/sec}$$

$$\text{pkt size} = 10^7 \text{ bits.}$$

$$T_d(\text{frame}) = \frac{d}{v} = \frac{10^7}{500 \times 10^8} = 0.02 \text{ sec}$$

$$P_d = d = \frac{8000}{v} = 2 \text{ sec}$$

$$4 \times 10^8 \text{ km/sec}$$

$$\eta = \frac{N * T_d(\text{frame})}{T_d(\text{frame}) + 2^k P_d + Q_d + P_{dt} + T_d(\text{acc})}$$

$$\frac{1}{1} = \frac{N * 0.02}{0.02 + 2^k * 2}$$

$$N: 4.02 \cdot N = 402 = 201$$

$$\frac{0.02}{2}$$

Minimum Sequence no. required = $201 + 1$
 $= 202$

$$2^k = 202 \therefore k = \underline{8 \text{ bit}}$$

Q11 Consider a 512×10^3 bits/second Satellite Communication link using one way Propagation delay of 150 m.sec GBN Protocol is used on this link to send data with a frame size of 1KB. ACK size is 64 byte, and frame processing time is 5 ms. Then window size should be min window size

$$B = 512 \times 10^3 \text{ bits/sec}$$

$$Pd = 150 \text{ msec.}$$

$$\text{Frame Size} = 1 \text{ Kbyte}$$

$$= 1024 \times 8 \\ = \underline{8192 \text{ bit}}$$

$$\text{Ack Size} = 64 \text{ byte}$$

$$\begin{aligned} Pcl &= 5 \text{ msec} \\ &= 8 \times 64 \text{ bit} \\ &= 512 \text{ bit.} \end{aligned}$$

$$T_d(\text{frame}) = \frac{L}{B} = \frac{8 \times 10^3 \text{ bit}}{512 \times 10^3 \text{ bit/sec}} = \underline{16 \times 10^{-3} \text{ sec}} \\ = 16 \text{ msec.}$$

$$Pd = \frac{d}{v} = \underline{150 \text{ msec.}}$$

$$T_d(\text{ACK}) = \frac{\text{Ack Size}}{B} = \frac{512}{512 \times 10^3} = \underline{1 \text{ msec.}}$$

$$\text{efficiency} = \frac{N \cdot Pd_{\text{frame}}}{T_d(\text{frame}) + 2 \cdot Pd_{\text{ACK}} + Pd_{\text{PCL}} + T_d(\text{ACK})}$$

$$1 = \frac{N \cdot 16}{16 + 2 \cdot 150 + 5 + 1} \Rightarrow 1 = \frac{N \cdot 16}{322} = \frac{322}{16}$$

$$N = 20.125$$

$$N = \lceil 20.125 \rceil = \underline{\underline{21}}$$

Q12 The distance between two stations M and N is 1 km. If the frame size is K bits long. The propagation delay/km is t' seconds. Let B bits/second be channel capacity. Assuming that the processing delay is negligible, the min. no. of bits for the sequence number field in a frame for maximum utilization, when the Sliding Window protocol is used is.

Ans

$$d = 1' \text{ km.}$$

$$\text{Frame size} = K \text{ bits, } B = R \text{ bits/sec.}$$

Propagation delay for 1 km = t' sec
 $- \text{For } 1' \text{ km} = t \text{ sec.}$

$$T_d(\text{frame}) = \frac{L}{B} = \frac{L}{R} \text{ sec.}$$

$$\text{efficiency} = \frac{W + T_d(\text{frame})}{T_d(\text{frame}) + 2^k P_d + Q_d + P_d + T_d(\text{frame})}$$

$$T_d(\text{frame}) + 2^k P_d + Q_d + P_d + T_d(\text{frame})$$

$$= \frac{W_s + \frac{L}{R}}{\frac{L}{R} + 2^k L T_p} = 1 = \frac{W_s R}{R} \times \frac{R}{K + 2^k L T_p}$$

$$W_s = \frac{K + 2^k L T_p}{R}$$

$$\text{min seq. no required} = K + 2^k L T_p$$

$$\text{no. of bits required in the seq. no field} [\log \frac{K + 2^k L T_p}{R}]$$

Q13. Consider two hosts are connected via direct link having data transfer rate 10 Mbps and signal speed 300 m/sec per km, distance between them is 6km and pkt size is 5000 Byte. The seq. no field in frame format is 3 bit long and GB-N protocol, the max amount of time the sender remain idle is.

Ans

$$B = 10 \text{ Mbps} = 10 \times 10^6 \text{ bit/sec}$$

$$\text{pkt size} = 5000 \text{ bytes}$$

$$\text{propagation time for } 6\text{ km} = 18 \text{ msec.}$$

$$= 8 \times 50,000$$

$$\text{Seq. no} = 3 \text{ bit}$$

$$= 40,000 \text{ bits}$$

$$\text{Seq. no} = k \text{ bit}$$

$$\frac{W_s}{2^k - 1} \quad \frac{W_R}{1} \quad \frac{W_s}{2^k - 1} \quad \frac{W_R}{1}$$

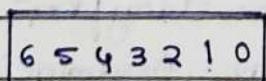
$$N = 7 \quad (\text{Sender window size in GB-N})$$

$$P_d(\text{sec}) = \frac{E_s}{B}$$

$$\text{Bandwidth} = 40,000 \text{ bits} = 4 \times 10^{-3} \text{ sec.}$$

$$10^7 \text{ bits/sec} = 4 \text{ msec}$$

$$P_d = 18 \text{ msec}$$



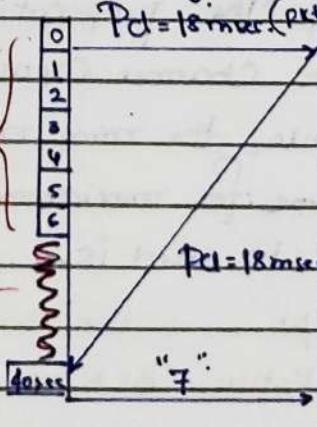
$$W_s = 7$$

$$28 \text{ msec.}$$

$$\text{Waiting Time} \leftarrow$$

$$= 40 \text{ msec} - 28 \text{ msec}$$

$$= 12 \text{ msec}$$



Max amount of time the sender remains idle = Total time - useful time

$$\text{Total time} = N + T_d$$

$$= 40 \text{ msec} + 4 \text{ msec}$$

$$= 40 \text{ msec} + 28 \text{ msec}$$

$$= \underline{12 \text{ msec}}$$

$$\text{Total time} = T_d(\text{frame}) + 2^* pd + Qd + Rd + T_d(\text{ACK})$$

$$= 4 \text{ msec} + 2^* 18 \text{ msec}$$

$$T_{RTT} = \underline{40 \text{ msec}}$$

Q14 A 1 mbps Satellite link connects two ground stations. The altitude of the satellite is 36,504 km and speed of the signal is 3×10^8 m/sec. What should be the packet size for a channel utilization of 25.1% for Satellite link usage Go-back-127 Sliding window. Assume that the acknowledgement packets are negligible in size and there are no errors during communication.

Ans

$$B = 1 \text{ mbps} = 10^6 \text{ bits/sec}$$

$$V = 3 \times 10^8 \text{ m/sec} = 3 \times 10^5 \text{ km/sec}$$

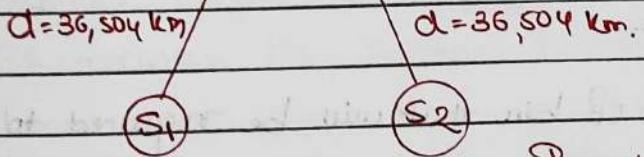
$$\text{Distance} = 2 \times 36,504$$

$$= 73,008 \text{ Km.}$$

$$\text{Packet size} = ?$$

$$Q = 25.1 = \frac{1}{4}, \quad \text{GBN-127}$$

$$N = 127$$



$$T_d = \frac{d}{V} = \frac{73,008 \text{ Km}}{3 \times 10^5 \text{ km/sec}} = 243.26 \times 10^{-5} \text{ sec.}$$

$$T_d = N + T_d(\text{frame})$$

$$\frac{1}{4} = T_d(\text{frame}) + 2^* pd + Qd + Rd + T_d(\text{ACK})$$

$$= \frac{1}{4} = \frac{127 \times T_d}{T_d + 2^* pd} \Rightarrow 127 + 4 \times T_d = T_d + 2^* pd$$

$$127 T_d = T_d + 2^* pd$$

$$126 T_d = 2^* pd$$

$$T_d = \frac{2^* pd}{126}$$

$$T_d = \frac{2 \times 243.26 \text{ sec}}{126}$$

$$\frac{L}{B} = \frac{2 \times 243.26 \text{ sec}}{126}$$

$$L = \frac{2 \times 243.26 \text{ sec} \times 10^6 \text{ bits/sec}}{126}$$

$$L = 960 \text{ bits} = \frac{960}{8}$$

$$L = \underline{120 \text{ Bytes}}$$

Q15. Frames of 1000 bits are sent over a 10^6 bps duplex link b/w two hosts. The propagation time is 25 ms. Frame are to be transmitted into this link to maximally pack them in transit. What will be max. number of bits (I) that will be required to represent the sequence numbers distinctly? Assume that no time gap needs to be given between transmission of two frames.

Ans

$$\text{Frame Size} = 1000 \text{ bit}$$

$$B = 10^6 \text{ bits/sec}$$

$$\text{Propagation time} = 25 \text{ ms}$$

$$\text{Capacity of Link} = B * p$$

$$= 10^6 \text{ bits/sec} \times 25 \times 10^{-3} \text{ sec}$$

$$= 10^3 \times 25 \text{ bits}$$

$$= 25,000 \text{ bits}$$

Capacity of Link (in frames)

$$= (\text{Capacity of Link}) \text{ bit} = 25,000 \text{ bit}$$

$$(\text{Frame Size}) \text{ bits}$$

$$1000 \text{ bits}$$

$$\begin{aligned} \text{No of frames} &= 25 & 2^k &= 25 \\ &\quad \curvearrowright & k &= 5 \text{ bits} \\ I &= k & \underline{\underline{}} \end{aligned}$$

Let 'I' be the min. no of bits that will be required to represent the sequence numbers distinctly assuming that no time gap needs to be given between transmission of two frame.

Suppose that SW protocol is used with the sender window size of 2^I , where I is the no. of bits earlier and acknowledgements are piggybacked. After sending 2^I frames, what will be the min. time sender will have to wait before starting transmission of the next frame?

Ans

$$\text{Sender window size} = 2^I = 2^5 = 32$$

min. time sender have to wait before starting transmission

of next frame = Total time - useful time

$$= \text{Total time} - N * T_d(\text{fram})$$

$$= 52 \text{ msec} - 32 * 1 \text{ msec}$$

$$= 20 \text{ msec}$$

$T_d(\text{fram})$

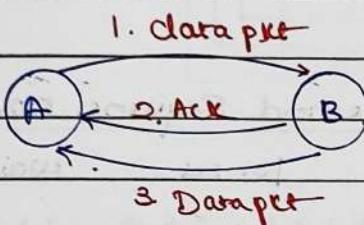
$$= \frac{1000}{10^6}$$

$$10^3$$

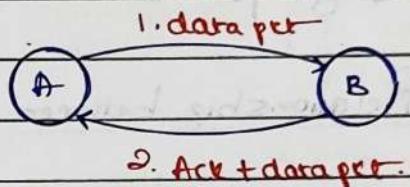
$$= \frac{1}{10} \text{ sec} = 1 \text{ msec}$$

$$\begin{aligned}
 \text{Total time} &= T_d(\text{frame}) + 2^* p_d + Q_d + P_d + T_d(\text{ACK}) \\
 &= 1\text{ msec} + 2^* 2.5 + 1 \\
 &= \underline{\underline{52\text{ msec}}}
 \end{aligned}$$

General Approach.

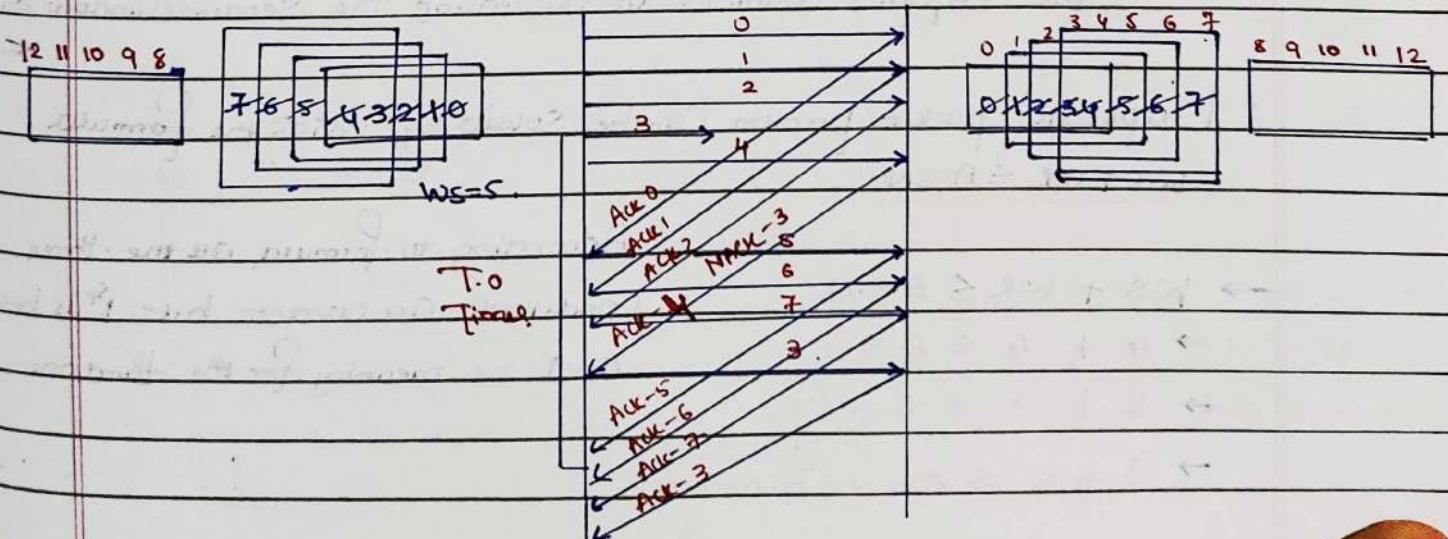


Piggy Backed



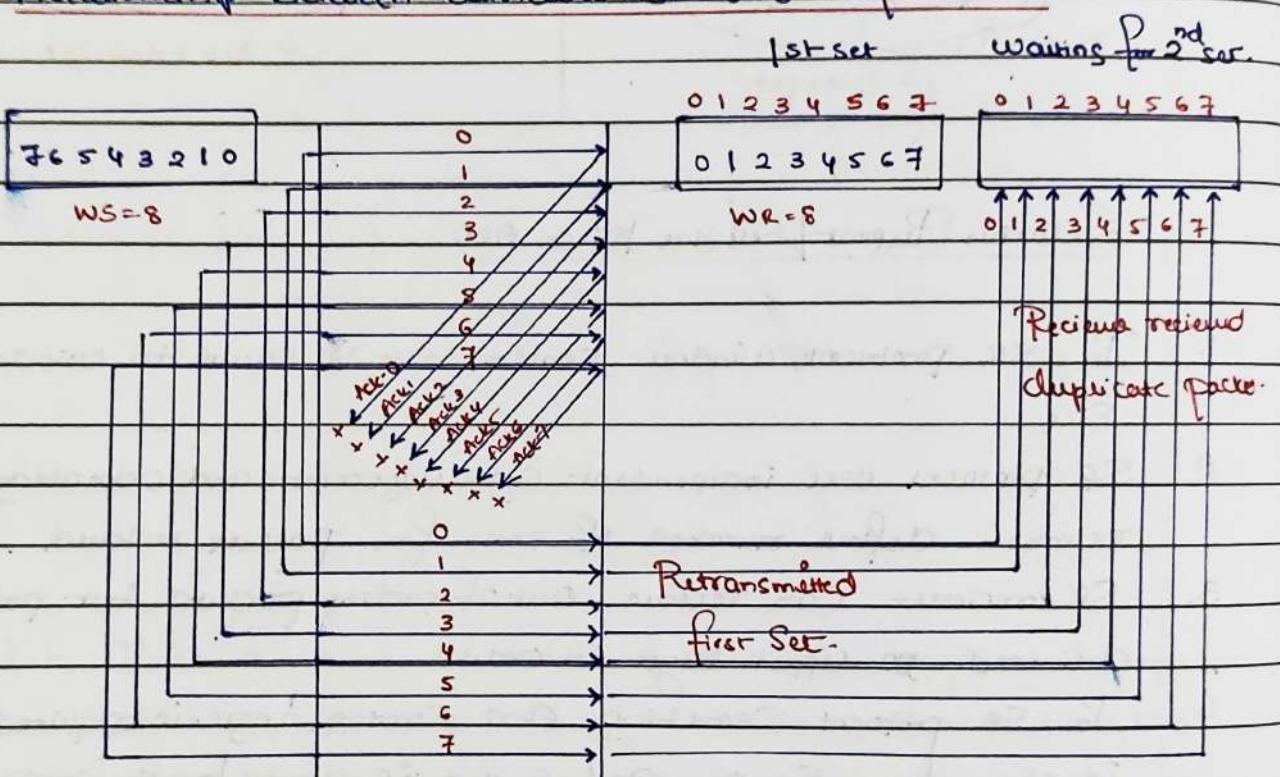
Selective Repeat / Selective Reject ARQ.

1. In SR protocol window sender size is equal to window receiver size
2. SR protocol uses independent acknowledgement and acknowledgement-number defines number of error free packets received.
3. SR receiver can receive out-of-order packets but packets are delivered to upper layer in order
4. In SR protocol searching and sorting logic is required. Searching is done by sender and sorting is done by the receiver
5. Timer is maintained for each and every frame in the window at sender side.



- For 1st Out of order delivery or if packet received is corrupted then NAK for respective packet is sent by receiver to sender.
- When sender receive NAK-3 then it will search in the window for packet-3 and immediately packet-3 is retransmitted even though its timer is not expired.

Relationship between window size and Sequence no.



Note: * Duplicate packet problem can be solved by increasing the sequence number or decreasing the sender window size.

* Duplicate packet problem can be solved by using the formula WS + WR ≤ A.S.N.

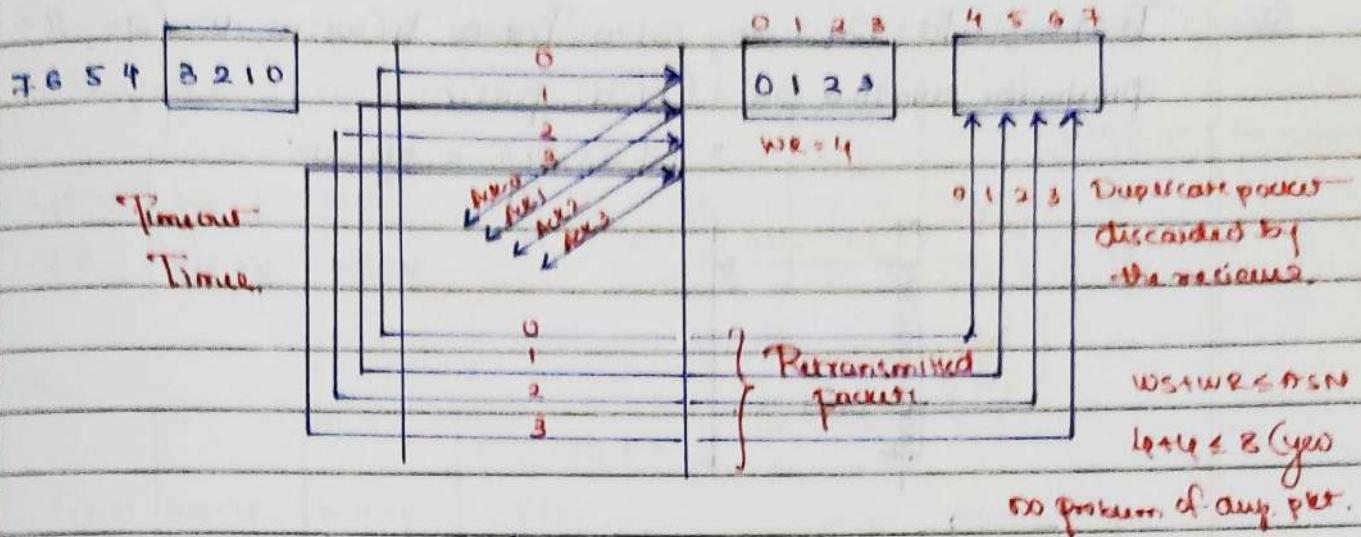
$$\rightarrow WS + WR \leq ASN$$

$$\rightarrow 4 + 4 \leq ASN$$

$$\rightarrow 5 + 3 \leq ASN \text{ (you)}$$

$$\rightarrow 3 + 5 \leq ASN \text{ (remaining)}$$

According to formula, all the three conditions are correct but 1st is best and no meaning for the third one.



1. Sequence no = 8 (0-7)

WS WR
4 4

4. Seq no = 3 bit

Total seq no = $2^3 = 8$ (0-7)

WS WR
4 4

2. Sequence No = 16 (0-15)

WS WR
8 8

5. Seq No = 4 bit

Total sequence no = $2^4 = 16$ (0-15)

WS WR

$8 [2^{4-1}] \quad 8 (2^{4-1})$

3. Seq No = N (0-N-1)

WS WR
 $N/2$ $N/2$

6. Seq no = k bit

WS WR

$2^{k-1} \quad 2^{k-1}$

7. WS WR.

| | |
|-----|-----|
| 4 | 4 |
| 8 | 8 |
| N | N |

Min. Sequence no required.

8

16

$2N$

Seq no = 8 (0-7)

WS WR

4 4 ✓

5 3 ✓

1 $2 \times WS > 1$ in SR

1 1 ✗ Stop & wait

Q. $T_d = 1 \text{ sec}$, $P_d = 24.5 \text{ sec}$, $Q_d = 0$, $P_{rd} = 0$, $T_d(\text{ACK}) = 0$, $W_S = 25$, $\eta = ?$

maximum window size = $(1+2a) \text{ packets}$

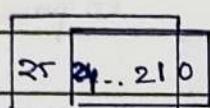
$$= 1 + 2 \times \frac{24.5}{21} = \underline{\underline{50 \text{ packets}}}$$

$T_d = 1 \text{ sec}$

$\left\{ \begin{array}{l} 49 \\ \text{sec} \end{array} \right\}$

$P_d = 24.5 \text{ sec}$

$P_d = 24.5 \text{ sec}$



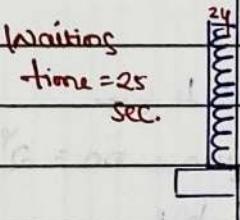
$P_d = 24.5 \text{ sec (pkt)}$

0
1
2
3
⋮

$WR = 50$

$$\text{Efficiency} = \frac{25}{50} = \frac{1}{2} = \underline{\underline{50\%}}$$

Waiting time = 25 sec.



$$\eta = \frac{25 \times 1}{1 \text{ sec} + 2 \times 24.5 \text{ sec} + 0 + 0 + 0}$$

$$\eta = \frac{1}{2} = \underline{\underline{50\%}}$$

$$\boxed{\text{Efficiency} = W_S + T_d(\text{frame})}$$

$$T_d(\text{frame}) + 2^+ P_d + Q_d + P_{rd} + T_d(\text{ACK})$$

Q. $\eta = \frac{1}{2}$, Bandwidth = 40 Mbps, Throughput = ?

Throughput = efficiency \times bandwidth

OR

$$\text{Throughput} = \frac{1}{2} \times \frac{20}{2} \text{ Mbps}$$

$$\boxed{\text{Throughput} = \frac{W_S \times \text{Frame Size}}{\text{Total Time}}} = \underline{\underline{20 \text{ Mbps}}}$$

1. SR protocol required more Sequence number in comparison of GBN.

(i) Seq.no = 8 (0-7)

(ii)

Min. seq.no required.

| | | | | | | |
|------|------|------|-----|------|------|----|
| GB-N | WS=7 | WR=1 | GBN | WS=7 | WR=1 | 8 |
| SR | WS=4 | WR=4 | SR | WS=7 | WR=7 | 14 |

(iii)

min seq.no

| | | | |
|------|------|------|-----|
| GB-N | WS=N | WR=1 | N+1 |
| SR | WS=N | WR=N | 2N |

2. SR protocol required more buffer space in comparison of GBN.

| | WS | WR | Buffer Space |
|-----|----|----|--------------|
| GBN | N | 1 | N+1 |
| SR | N | N | 2N |

3. Traffic is very high in SR protocol because SR protocol uses independent acknowledgement.

| | Stop and wait | GBN | SR |
|-----------------|--|--|---|
| Efficiency. | $\eta = \frac{T_d}{\text{Total time}}$ | $\eta = \frac{N + T_d}{\text{Total time}}$ | $\eta = \frac{W_s \times T_d}{\text{Total time}}$ |
| Throughput. | $R^* B$ | $R^* B$ | $R^* B$ |
| Buffer | 1+1 | N+1 | N+N |
| Seq.no. | 2(0 & 1) | N+1 (0-N) | 2N (0-2N-1) |
| Seq.no = k bits | - | WS WR 2^{k-1} 1. | WS WR 2^{k-1} 2^{k-1} . |
| Total time. | Same for all | Same for all | Same for all |

Q1. The maximum window size for data transmission using SR protocol with n -bit frame sequence no. is

Ans. $2^{(n-1)}$

Q2. If sender window size is 7s. What will be the sequence no. required in GBN and SR protocol?

Ans. Sender window size = N.

$$\text{min Seq. no in Gen} = N+1 (0-N)$$

$$\text{" " " " } \text{SR} = N+N = 2N (0-2N-1)$$

$$\therefore \text{GBN} = 76 (0-75)$$

$$\text{SR} = 150 (0-149)$$

Q3. If 'N' is the maximum sequence number then window size in GBN and SR is.

Ans. Seq. no = 8 ($0, 1, 2, 3, 4, 5, 6, 7$)

GBN

SR

WS WR

7 1.

WS WR

4 4

$\therefore \text{Ans} = N, \frac{N+1}{2}$

$\frac{N+1}{2}, 1.$

$\frac{N+1}{2}, \frac{N+1}{2}$

Q4. Suppose Sliding window ARQ is used for flow control and Optimal window size for maximum utilization of link is 5. If Stop and wait ARQ is used instead of Sliding window then link utilization (in percent) is. 20%.

Ans.

$$\eta_{\text{sliding window}} = N * \eta_{\text{stop & wait}}$$

$$\eta_{\text{stop & wait}} = \frac{1}{N} \times \text{Sliding Window}$$

$$\therefore \eta_{\text{stop & wait}} = \frac{1}{5} \times 1 = 20\%$$

Qs. Consider minimum number of bits required for sequence number field in SR-ARQ for maximum utilization are 4, then efficiency of Stop & wait - ARQ is

Ans

$$\eta_{\text{sliding window}} = N * \eta_{\text{Stop & wait}}$$

N - Send window size.

$$\eta_{\text{Stop & wait}} = \frac{1}{N} * \eta_{\text{sliding window}}$$

 $\text{Seq.no} = 4 \text{ bit}$

$$= \frac{1}{8} * 1 = 0.125$$

$$\begin{array}{ll} \text{WS.} & \text{WR.} \\ 2^{4-1} & 2^{4-1} \\ = 8 & = 8 \end{array}$$

Qs. Assume we need to design a protocol for a network in which B is 1 Mbps and average distance b/w sender & receiver is 5000 Km. Assume that avg. pkt size is 5000 bits. Propagation speed in the media is $2 \times 10^8 \text{ m/sec}$. If window sender size is 8 and process delay is 0.5 msec. and $q_d = 2 \text{ msec}$. $\eta = ?$

Ans. $B = 10^6 \text{ bits/sec}$, $d = 5000 \text{ km}$

$$V = 2 \times 10^8 \text{ m/sec.}$$

$$\text{Pkt size} = 5000 \text{ bits.}$$

$$V = 2 \times 10^8 \text{ Km/sec.}$$

$$Pd = \frac{d}{V} = \frac{5000 \text{ km}}{2 \times 10^8 \text{ Km/sec}}$$

$$T_d(\text{frame}) = \frac{L}{B} = \frac{5000 \text{ bits}}{10^6 \text{ bits/sec}}$$

$$= 25 \times 10^{-3} \text{ sec} = 25 \text{ msec.}$$

$$= 5 \times 10^{-3} \text{ sec} = 5 \text{ msec}$$

$$\text{WS} = 8, Q_d = 2 \text{ msec}, P_d = 0.5 \text{ msec.}$$

$$\eta = \frac{W_c \times T_d(\text{frame})}{T_d(\text{frame}) + 2 * P_d + Q_d + P_d + T_d(\text{ack})} = \frac{8 \times 5}{5 + 2 * 25 + 2 + 0.5}$$

$$= \frac{40}{5 + 50 + 2.5} = 0.6956$$

$$\approx 69.56\%$$

H/W

Q3. In selective repeat ARQ, packet size is 2000 byte transmission time for one packet is 1 ms. If distance b/w hosts is 10 km & signal speed is 4 m/s/km. And frame sequence are 6 bits long in frame format then throughput (in Mbps) = . 6.32 Mbps.

- Q8. Suppose you are designing a SW Protocol for a 1mbps point-to-point link to the moon, which has a one way latency (delay) of 1.25 sec. Assuming that each frame carried 1KB of data, the min no. of bits you need for the sequence number.
- for RWS = 1 (GBN) and
 - for SWS = RWS (sr) is.

$$B = 10^6 \text{ bits/sec}$$

$$Pd = 1.25 \text{ sec.}$$

$$\text{Frame Size} = 1 \text{ KB}$$

$$= 1024 \times 8 = 8192 \text{ bit.}$$

$$Td(\text{frame}) = \frac{8192 \text{ bit}}{10^6 \text{ bit/sec}} \\ = 0.008192 \text{ sec.}$$

$$\text{efficiency} = \frac{N + Td(\text{frame})}{Td(\text{frame}) + 2 * Pd + Qd + Pd + Td(\text{frame})}$$

$$1 = \frac{N + 0.008192}{0.008192 + 2 * 1.25}$$

$$0.008192 \times 2 * 1.25$$

$$N = \frac{0.008192 + 2 * 1.25}{0.008192}$$

$$N = 306.17$$

$$N = \lceil 306.17 \rceil = \underline{\underline{307}}$$

| Sliding Window | GB-N | Sr |
|-------------------------------------|----------------------------|--|
| Minimum sequence no. required = 307 | Min SeqNo required in GB-N | Min. seq no. required in SR is. |
| $2^k = 307$ | $= 307 + 1 = 308$ | $= 2N + 1$ |
| $k = 9 \text{ bit.}$ | $2^k = 308$ | $= 614 +$ |
| | $k = 9 \text{ bit.}$ | $= 615$ |
| | | $\therefore 2^L = 615$ |
| | | $L = \underline{\underline{10 \text{ bit}}}$ |

HW

$$\therefore \text{Ans} = 9, 10$$

- Q9. Consider a 128×10^3 bit/second satellite communication link with one way pd = 150 msec. SR protocol is used on this link to send data with a frame size of 1KB. Neglect the transmission time of acknowledgement. The min no. of bits required for the sequence no.

Field to achieve 100% utilization is

Ans.

$$B = 128 \times 10^3 \text{ bits/sec}$$

$$T_d = 150 \text{ msec}$$

$$\text{Frame size} = 1 \text{ KB}$$

$$= 1024 \times 8$$

$$= 8192 \text{ bits}$$

$$T_d = \frac{L}{B} = \frac{8192 \times 2}{128 \times 10^3}$$

$$= 64 \times 10^{-3} \text{ sec.}$$

$$= 64 \text{ msec}$$

$$\eta = N * T_d(\text{frame})$$

$$T_d(\text{frame}) + 2^{*}pd + Qd + Pd + T_d(\text{acc})$$

$$I = W_s \times 64 \quad W_s = \frac{264}{64}$$

$$W_s = 5.68$$

$$W_s = [5.68]$$

$$\text{Min. sequence no.} = 6 + 6 = 12$$

$$2^k = 12$$

$$k = 4 \text{ bits}$$

Q10. A 3000 Km long trunk operating at 1.536 Mbps is used to transmit 64 byte frame and user supp. If propagation speed is 64 km/sec then the number of bits should the sequence number is.

$$\text{Ans. } d = 3000 \text{ Km}, \quad B = 1.536 \times 10^6 \text{ bits/sec.} \quad \text{Frame size} = 64 \text{ Byte}$$

$$\text{prop. time for 1 Km} = 6 \text{ msec}$$

$$\text{propagation time for 3000 Km} = 512 \text{ bits}$$

$$= 3000 \times 6 \text{ msec} = 18000 \text{ msec.}$$

$$T_d(\text{frame}) = \frac{L}{B} = \frac{512 \text{ bits}}{1.536 \times 10^6 \text{ bits/sec}}$$

$$= 333.33 \times 10^{-6}$$

$$= 333.33 \text{ msec.}$$

$$\eta = N * T_d(\text{frame})$$

$$T_d(\text{frame}) + 2^{*}pd + Qd + Pd + T_d(\text{acc})$$

$$= N \times 333.33 \text{ msec.}$$

$$333.33 \text{ msec.} + 2^{*}18000 \text{ msec.}$$

This sequence no is

$$2^k = 100$$

$$k = 7 \text{ bits}$$

$$N = 109.00108$$

$$N = [109.00108] = 100$$

Q11. Consider Selective repeat ARQ is used for flow control, frame size is 4000 bits, data transfer rate of channel is 1 Mbps and one way propagation delay is 18 msec then minimum no. of bits required for sequence number field for maximum utilization is

Ans

$$L = 4000 \text{ bits}$$

$$T_d(\text{frame})$$

$$B = 1 \text{ Mbps} = 10^6 \text{ bits/sec.}$$

$$= \frac{4000}{10^6} = 4 \text{ msec}$$

$$P_d = 18 \text{ msec.}$$

$$\eta = \frac{W_s \times T_d(\text{frame})}{T_d(\text{frame}) + 2 \times P_d + Q_d + P_d(\text{ack})}$$

$$= \frac{W_s \times 4 \text{ msec}}{4 \text{ msec} + 2 \times 18 \text{ msec}}$$

$$= W_s = \frac{40}{4} = 10$$

$$\begin{aligned} \text{Min Sequence no} &= W_s + 10 \\ &= 10 + 10 \\ &= 20. \end{aligned}$$

$$2^k = 20$$

$$2^k = 20 \therefore k = 5 \text{ bits}$$

Q12. Suppose A uses 32 bytes packets to transmit message to station B using a sliding window protocol. The round trip delay between A and B is 80 msec and bottleneck bandwidth on the path between A and B is 128 kbps what is the optimal window size A should use?

Ans

$$Pkt \text{ size} = 32 \text{ B}$$

$$RTT = 80 \text{ msec}$$

$$= 32 \times 8 = 256 \text{ bits}$$

$$B = 128 \times 10^3 \text{ bits/sec.}$$

$$T_d(\text{frame}) = 256$$

$$128 \times 10^3 \text{ bits/sec.}$$

$$\eta = \frac{T_d(\text{frame})}{RTT} = \frac{2 \text{ msec} \times W_s}{80 \text{ msec.}}$$

$$= 2 \times 10^3 \text{ sec} = 2 \text{ msec}$$

$$W_s = \frac{80 \text{ msec}}{2 \text{ msec}} = 40$$

AD Steps to solve SWP Problem.

1. Calculate RTT

2. Based on given bandwidth and RTT calculate no. of bits we can

able to transfer units in RTT and equate it as window to terms of bits (W_{bin}) = $B^* RTT$.

$$3. W_{pkt} \text{ or } W_p = \frac{W_{bin}}{\text{Packet size}}$$

(Packet size)

$$4. \text{Minimum Sequence no required} = W_p^*$$

$$5. 2^k = W_p$$

Where $k = \text{no. of bits required in the sequence no field}$.

Q13 Consider two nodes A and B round trip delay between those is 80 ms and bottleneck bandwidth of link between A and B is 512 Kbps, the optimal window size (in packets) if the packet size is 64 Byte.

$$\text{Ans. } RTT = 80 \text{ msec} = 80 \times 10^{-3} \text{ sec}, \quad B = 512 \text{ Kbps} = 512 \times 10^3 \times 8 \text{ bits/sec}$$

$$\text{Packet size} = 64 \text{ byte} = 64 \times 8 \text{ bits}$$

AD Rule:

$$1. RTT = 80 \text{ msec.}$$

$$2. W_{bin} = B \times RTT = 512 \times 10^3 \times 8 \text{ bits/sec} \times 80 \times 10^{-3} \text{ sec} = 512 \times 8 \times 80 \text{ (bits)}$$

$$3. W_{pkt} = \frac{W_{bin}}{\text{packet size}} = \frac{2^3 \times 512 \times 8 \times 80}{64 \times 8} = 640 \text{ pkts}$$

$$T_d(\text{frame}) = L = \frac{64 \times 8}{B} = \frac{64 \times 8}{512 \times 10^3 \times 8} = \frac{1}{8} \times 10^3$$

$$2 = \frac{W_S \times T_d(\text{frame})}{RTT}$$

$$W_S = \frac{RTT}{T_d(\text{frame})} = \frac{80 \text{ msec}}{\frac{1}{8} \text{ msec}}$$

$$= \frac{1}{8} \times 10^3$$

$$= 80 \times 8 = 640 \text{ pkts.}$$

IPv4 header and Fragmentation.

IPv4 header.

| | | | | | |
|---------------|---------------------------|------------|--------------------|-----------------|---|
| | VER 4. | TTL 4. | Service 8 | Total Length 16 | $\rightarrow 32 \text{ bit} = 4 \text{ Byte}$ |
| 20 Byte fixed | Identification No. 16. | Flags 3 | Fragm. Offset 13. | | $\rightarrow 32 \text{ bit} = 4 \text{ Byte}$ |
| | Time-to-Live 8 | Protocol 8 | Header Checksum 16 | | $\rightarrow 32 \text{ bit} = 4 \text{ Byte}$ |
| | | | | | $\rightarrow 32 \text{ bit} = 4 \text{ Byte}$ |
| 40 B Variable | Source IP Address 32 | | | | $\rightarrow 32 \text{ bit} = 4 \text{ Byte}$ |
| | Destination IP Address 32 | | | | $\rightarrow 32 \text{ bit} = 4 \text{ Byte}$ |
| | Options (0-40 Byte) | | | | $5 \times 4 \text{ B} = 20 \text{ Byte}$ |

Minimum header size = $20 \text{ B} + 0 \text{ B} = 20 \text{ B}$.

Maximum header size = $20 \text{ B} + 40 \text{ B} = 60 \text{ B}$.

Header Length = (4 bits)

$$\hookrightarrow \text{max. no} = 1111 = 15.$$

Max. header size = 60 Byte.

$$\frac{60}{4} = 15.$$

S.F. $\rightarrow \frac{60}{4}$

$$\frac{60}{4} = 15$$

(SF) $\rightarrow \frac{60}{4}$

Header Size

$$\frac{20 \text{ B}}{4} = 5$$

TILF

0101

$$\frac{40 \text{ B}}{4} = 10$$

1010

Header Size

TILF

$$\frac{30 \text{ B}}{4} = 7.5 \times$$

TILF

Header Size

$30 \text{ B} + 2 \text{ B}$

$$= \frac{32}{4} = 8.$$

\downarrow

dummy byte \rightarrow Options

1000

$$1010 = 10$$

$$1100 = 12$$

$$1000 = 8$$

$$1111 = 15$$

TILF (5-15)

$$10 \times 4 = 40 \text{ Byte}$$

$$12 \times 4 = 48 \text{ Byte}$$

$$8 \times 4 = 32 \text{ Byte}$$

$$15 \times 4 = 60 \text{ Byte}$$

Header size (20-60 B)

padding = 2 byte

Version (4 bit) : It is used to indicate IPv4 or IPv6.

(0100)

(0110)

Services : In this interpretation the first 3 bits can called precedence bit (Priority bit) and next 4 bits can called types of service bits and last bit not used.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| P | P | P | D | T | R | C | X |

Priority type of service not used.

D : minimum delay

T : maximize throughput

R : high reliability

C : minimum cost.

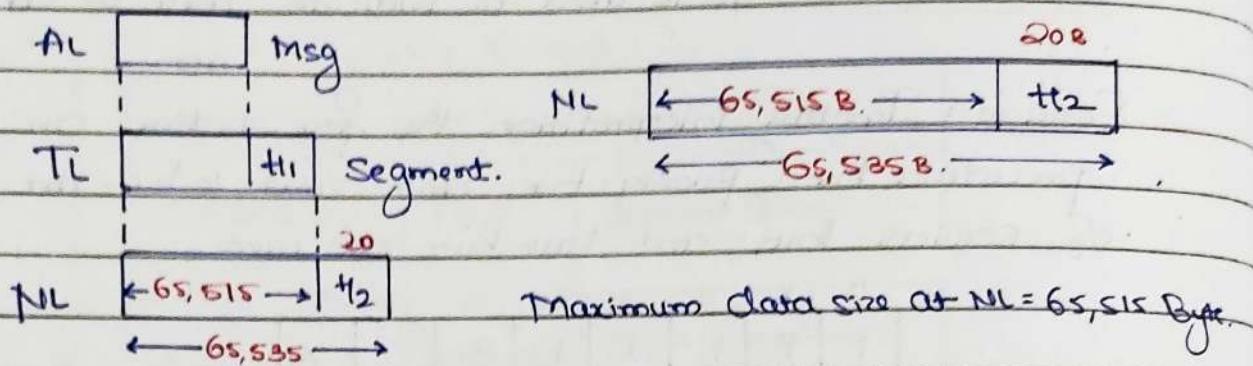
Priority : It is a 3 bit subfield ranging from 0-7 (000 to 111 in binary). Priority field is needed if router is congested need to discard some datagram, those datagram that have the lowest priority are discarded first.

Type of Service : It is a 4 bit subfield. Each bit having a special meaning although a bit can be 0 or 1. One and only one of the bits can have the value 1 in each datagram.

| D | T | R | C | |
|---|---|---|---|------------------|
| 0 | 0 | 0 | 0 | Default |
| 1 | 0 | 0 | 0 | minimum delay |
| 0 | 1 | 0 | 0 | Max. throughput |
| 0 | 0 | 1 | 0 | High reliability |
| 0 | 0 | 0 | 1 | Min. cost. |

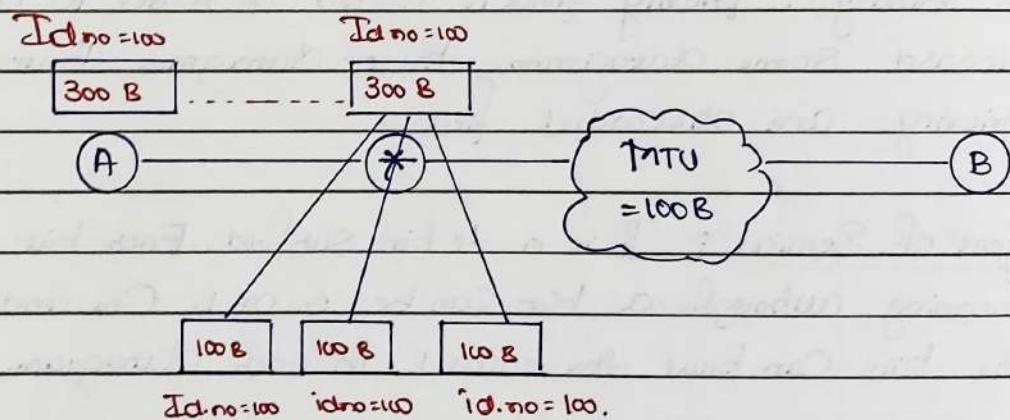
Total Length (16 bit)

Total Length = Data + Header, 16 bit \rightarrow max no. $2^{16}-1$.



Identification Number or Datagram Number (16 bit)

1. Each datagram is associated with a sequence no. is called as datagram no. or identification no.
2. It is used to identify all the fragments of same datagram.
3. All the fragment of same datagram will have the same identification number.



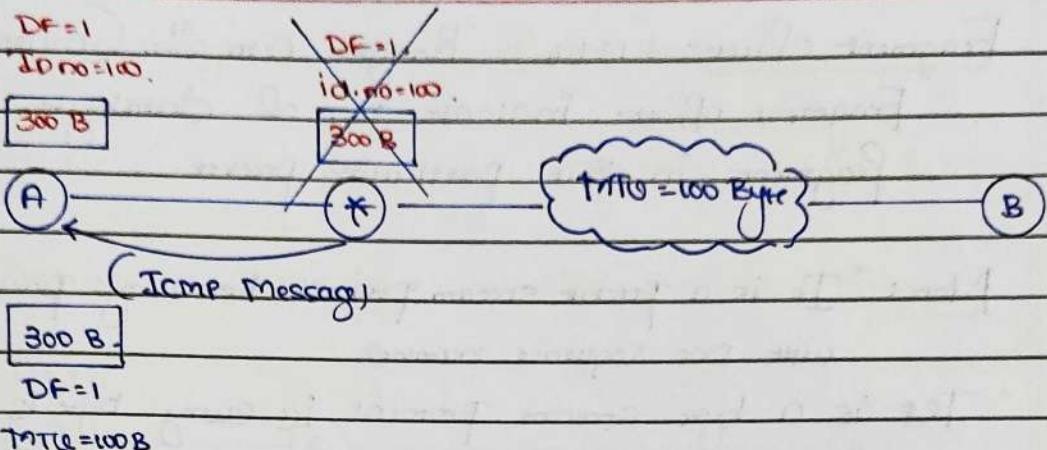
Flags: It is a 3 bit field as shown in the figure.

| | | | | |
|-----------------|----------|----------|----------|--|
| Not Used | X | D | M | 2nd bit is called Don't Fragment |
| | | F | F | 3rd bit is called more fragment |

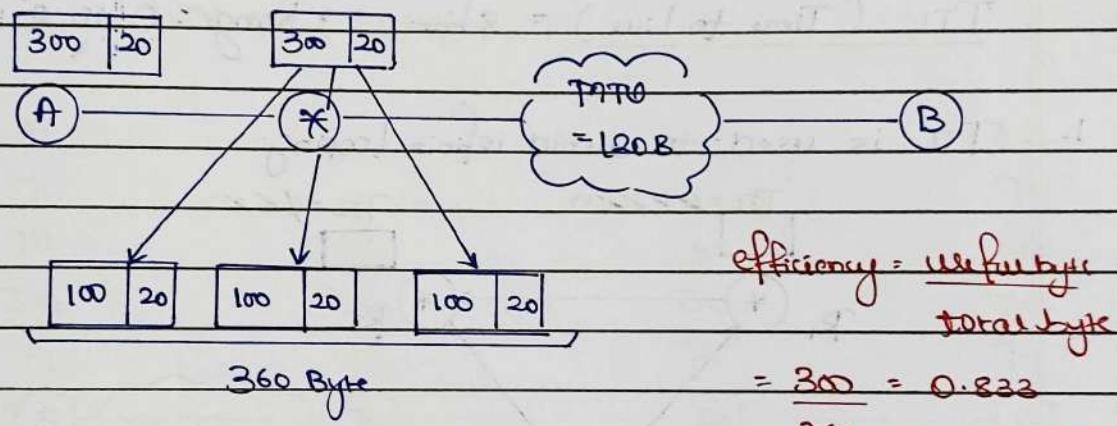
DF (Don't Fragment)

DF = 1 means datagram can't be fragmented

DF = 0 means datagram can be fragmented



T0 = 100 SF = 0 T0 = 100 DF = 0.



$$\text{efficiency} = \frac{\text{useful byte}}{\text{total byte}}$$

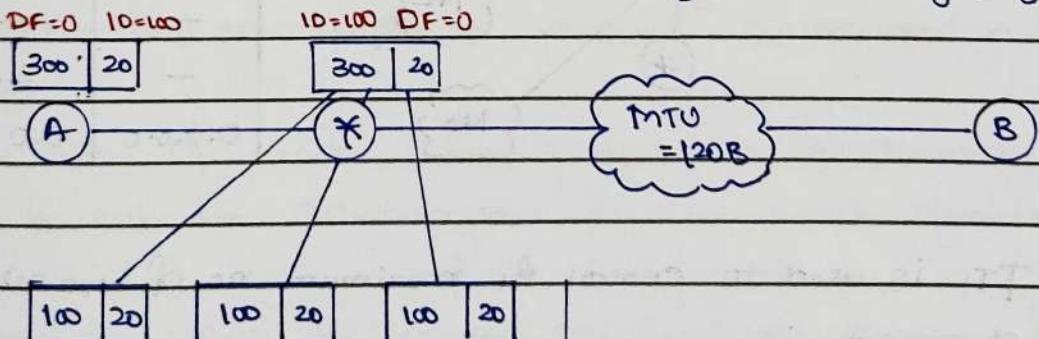
$$= \frac{300}{360} = 0.833$$

$$= \underline{\underline{83.33\%}}$$

More Fragment (MF)

MF = 1 → means this is not the last fragment, there are more fragments than this fragment.

MF = 0 → means this is the last fragment, or only fragment.



| 100 | 100 | 100 | ID.no |
|-----|-----|-----|-------|
|-----|-----|-----|-------|

| | | | |
|---|---|---|----|
| 0 | 1 | 1 | MF |
|---|---|---|----|

| | | | |
|-----|-----|---|-----------------|
| 200 | 100 | 0 | Fragment Offset |
|-----|-----|---|-----------------|

Fragment Offset: (13 bit) Range $0 \text{ to } 2^{13}-1$ ($0 \text{ to } 8191$)

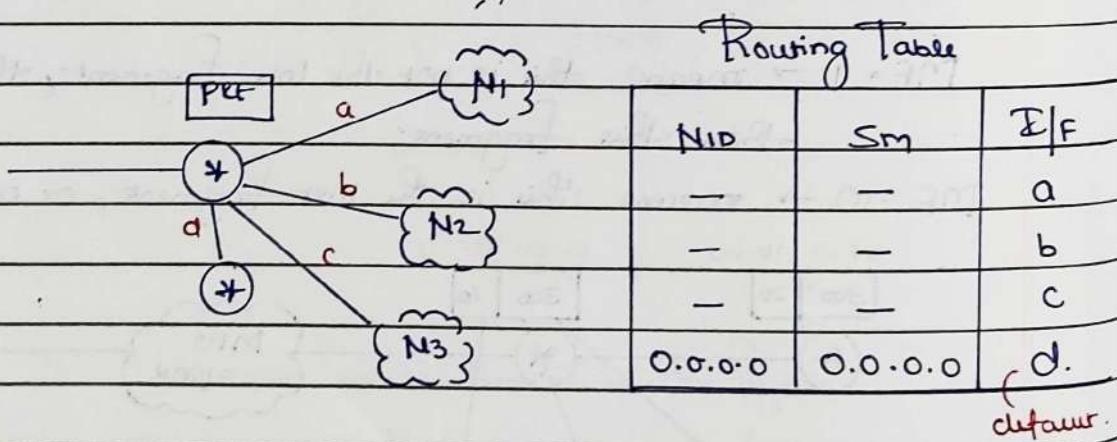
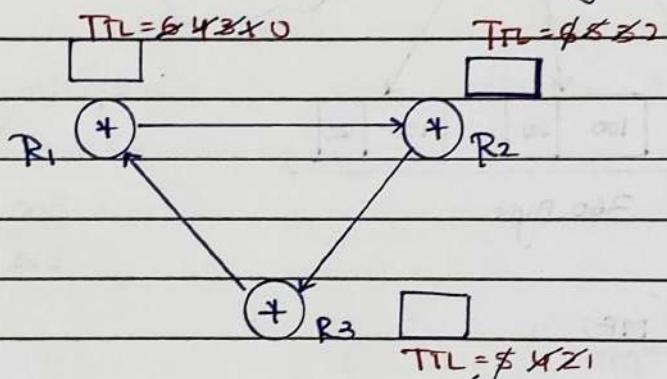
Fragment offset indicate no. of databyte ahead of the fragment in that particular packet.

Note: * IP is a packet stream protocol i.e every packet is associated with one sequence number.

* TCP is a byte stream protocol ie every byte is associated with one sequence number.

TTL (Time to Live) = 8 bit \rightarrow Range: $0 \text{ to } 2^8-1 = 0 \text{ to } 255$

1. TTL is used to avoid infinite looping.



2. TTL is used to control the maximum no. of hops waited by datagram.
3. When a source host sends a datagram, it stores a number in this field. Each router that process the datagram decrements this number by one. If TTL field reaches zero before the datagram arrives at its destination, then datagram is discarded and

an ICMP message is sent back to sender.

$$TTL = 4 \quad TTL = 3$$

$$TTL = 2$$

$$TTL = 1$$

$$TTL = 3$$

$$TTL = 2$$

$$TTL = 1$$

$$TTL = 0$$

$$TTL = 2$$

$$TTL = 1$$

$$TTL = 0$$

accepted

(S)

(R₁)

(R₂)

(D)

Discarded.

ICMP msg (TTL expired)

AL

T_L

N_L

D_L

P_L

S

N_L

D_L

P_L

R₁

N_L

D_L

P_L

R₂

AL

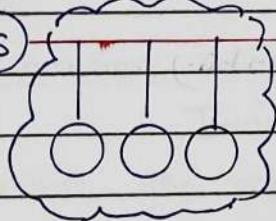
T_L

N_L

D_L

P_L

D



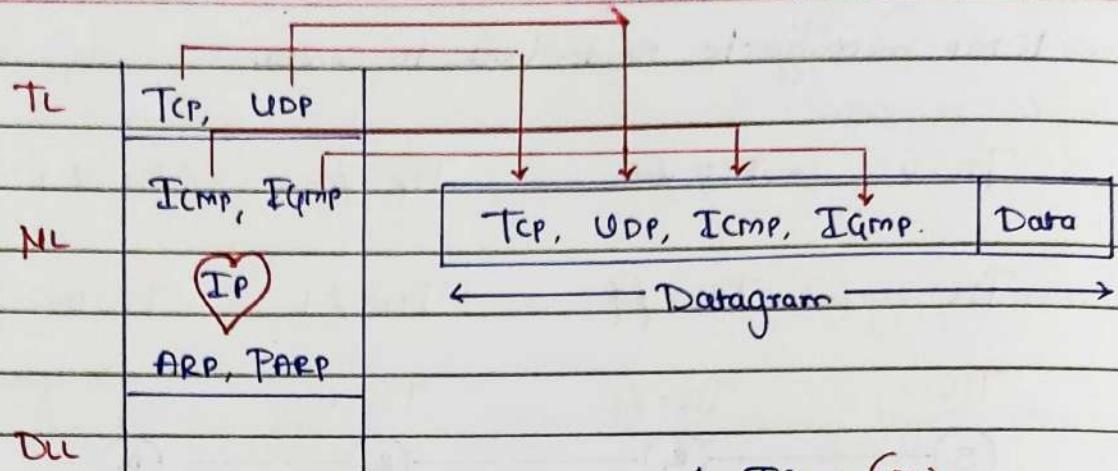
LAN-1

TTL never decrements to LAN.

Protocol (8bit)

1. This 8 bit field tells us which protocol is encapsulated in the IP packet.
2. At the time of traffic, some packets must be discarded, in this case it will be advantageous to know which protocol data is contained.
3. The order in which the router eliminates the datagram from buffer is:

ICMP > IGMP > UDP > TCP

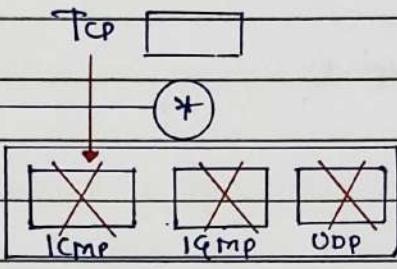


1. ICMP (01)

2. IGMP (02)

3. UDP (17)

4. TCP (06)



OSPF → (89)

Checksum. (4 bit, 8 bit, 16 bit, 32 bit)

(TCP/IP)

Let us assume Checksum = 4 bit.

Data = 0111 | 1011 | 1100 | 0000 | 0110

7 11 12 0 6

Checksum = $7+11+12+0+6 = 36$.

Checksum = 4 bit.

| | |
|----------------------|----|
| 01111011110000000110 | 3c |
|----------------------|----|

| | |
|----------------------|------|
| 01111011110000000110 | - 36 |
|----------------------|------|

 $36 - 36 = 0$ (No error)

Checksum = 4 bit Max. no. → 1111 : 15.

Checksum = $36 = \boxed{100100}$

$\downarrow +10$

$\begin{array}{r} 16 \\ \text{Complement} \end{array} \begin{array}{r} 0110 \rightarrow 6 \\ 1001 \rightarrow 9 \end{array}$

Transmitted Data.

Checksum.

011110111100000006110

1001

Received data.

| | | | | | |
|------|------|------|------|------|------|
| 0111 | 1011 | 1100 | 0000 | 0110 | 1001 |
| 7 | 11 | 12 | 0 | 6 | 9 |

$7+11+12+0+6+9 = 45 : \boxed{101101}$

$\downarrow 10$

$\begin{array}{r} 16 \\ \text{Complement} \end{array} \begin{array}{r} 1111 \\ 0000 \rightarrow \text{no error} \end{array}$

Header Checksum: (16 bit)

It is calculated only for header part not the data because the rest of the component in packet already covered by TCP Checksum.

Header Checksum is calculated for each and every router because related to IP header maybe change when packet is moving from one router to another.

Every router makes one modification i.e TTL so header checksum is calculated at every Router. Fragment offset, mf, total length, Option all may be changed at Router.

An msg

Tl msg th1 Segment

NL

{ th2 } → Check.

TTL = 7

00000111

S

TTL = 6

00000110

R₁

TTL = 5

00000101

R₂

TTL = 4

00000100

R

TTL = 320 Offset = 0

MF = 0 10 = 100

300 20

A

300 20

*

B

MTU
= 120B

100 20 100 20 100 20

100 100 100 1000

0 1 1 1 MF

200 100 0 Offset

120 120 120 TTL

| VER | TTL | Service | Total Length | Id.no |
|--------------------|--------|------------------|--------------|----------------------------|
| 0100 0101 10010010 | 16 bit | 1001101001001000 | 16 bit | 1000100000110101 16 bit |

1010 0010 0100 1000 | 1001001110100001
 Flag and Fragment Offset. TTL Protocol

Header Checksum.

SIP = 32 bit

DIP = 32 bit

0000000000000000 | 100100..... | 0100100.....

All 16 bit will be

Zero initially

Source Address: This 32 bit defines the IP address of the source. This field remains unchanged during the time IPX datagram travel from source to destination.

Destination Address: This 32 bit defines the address of the destination. This field remains unchanged during the time IPX datagram travel from source to destination.

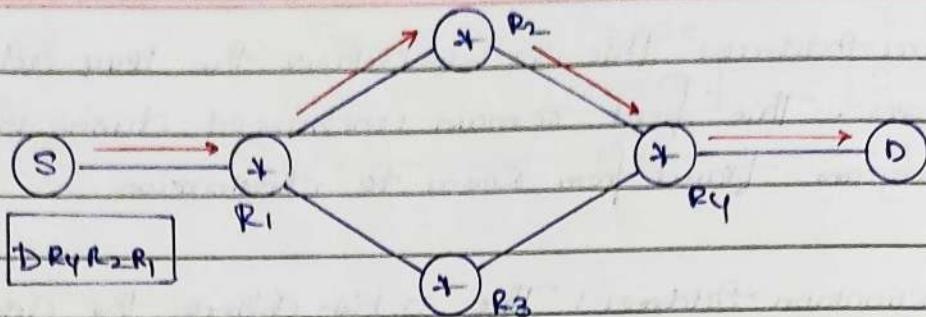
| Not Changed | May be changed | Definitely changed |
|-----------------------|-----------------------|--------------------|
| 1. VER | Total length | TTL |
| 2. TTL | TMF | Header checksum, |
| 3. Service | Fragment offset | |
| 4. Identification no. | TIL (if option found) | |
| 5. DF | Options | |
| 6. Protocol | | |
| 7. SIR | | |
| 8. DIP. | | |

Option: The header of IPX datagram is made of two parts a fixed part and a variable part. The fixed part is 20 Byte long and variable part can be maximum of 40 Byte.

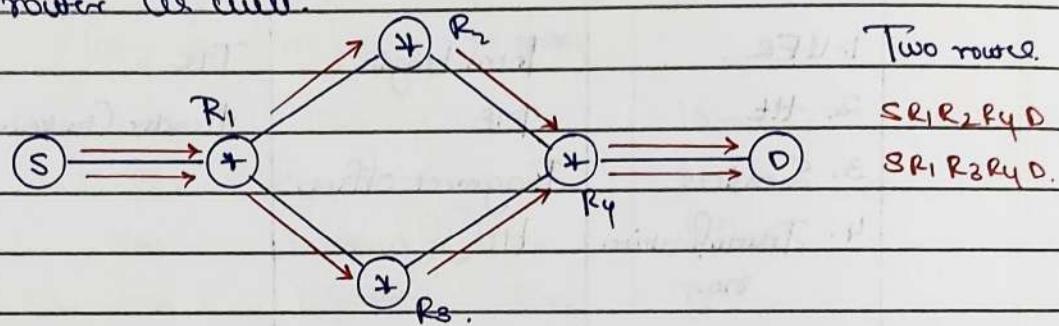
There are 5 Options:

1. Strict Source routing { Source will decide the route
2. Loose Source routing { Router will decide the route
3. Record routing { Router will decide the route
4. Timestamp
5. Padding

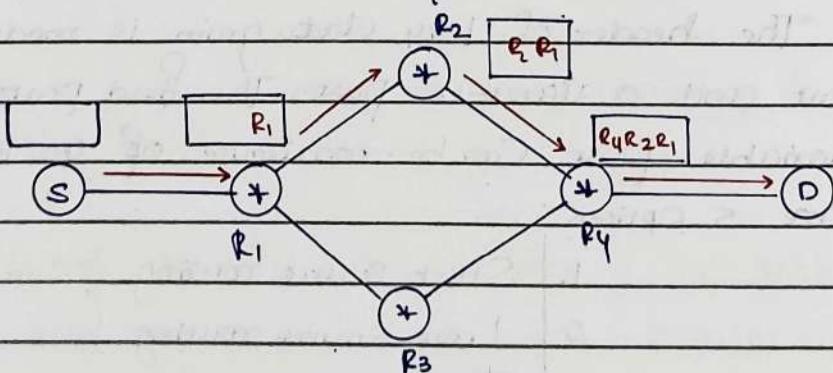
Strict Source Routing: A strict source routing is used by the source to predetermine a route for datagram to travel through the internet.



2. Loose Source Routing: A loose source route option is similar to strict source route but it is less rigid. Each router in the list must be visited, but the data gram can visit other routers as well.

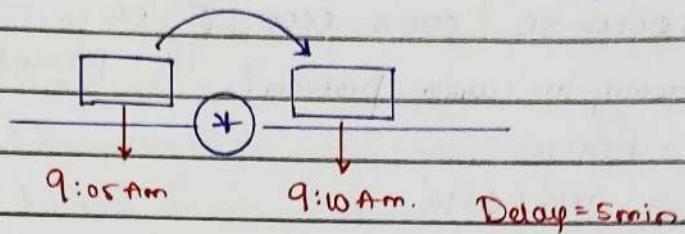


3. Record Routing: A record route option is used to record the internet routers that handle the data gram. It can list up to 9 router address. All the routers are supposed to record their IP address on their IP packet.



Note: First 16 bits (2 Byte) are reserved for Option type (8 bit) and length (8 bit). Out of 40 Byte only 38 bytes are remaining for storing IPv4 address. In 38 bytes we can store 9 IPv4 address. As each IPv4 address is of 4 byte.

4. Timestamp: It is used to find our delays at each router. Every router should record incoming and outgoing time.



- Q1. In an IPv4 packet the value of TLEN is $(100)_2$. How many bytes of options are being carried by this packet?

$$\text{Ans} \quad \text{TLEN} = (100)_2 = 12$$

$$\begin{aligned} \text{Header Size} &= 12 \text{ bytes} \\ &\quad - 20 \text{ bytes (options)} \\ &\quad \underline{28 \text{ bytes}} \end{aligned}$$

- Q2. In an IPv4 packet, the value of TLEN is 5, and the value of Total Length field is $(0048)_{16}$. How many bytes of data are being carried by this packet?

$$\text{Ans} \quad \text{TLEN} = 5$$

$$\begin{aligned} \text{TL} &= (0048)_{16} \\ &= 4 \times 16 + 8 \times 16^0 \\ &= 64 + 8 = 72 \end{aligned}$$

$$\text{TL} = D + \text{header}$$

$$\begin{aligned} \text{Data} &= \text{TL} - \text{header} \\ &= 72 - 20 = 52 \end{aligned}$$

- Q3. An IPv4 packet has arrived with first few hexadecimal digits as shown
~~(4500|00 5C000 30000 | 5906 . . .)₁₆~~

How many hops does this packet take before being dropped?

$$\text{Ans} \quad \text{TTL} = (59)_{16}$$

$$= 5 \times 16 + 9 \times 16^0 = \underline{\underline{89}}$$

- Q4. In an IPv4 packet the value of TLEN is $(100)_2$, how many bytes of options are being carried by this packet?

Qs. An IPv4 packet has the first few hexa decimal digits as shown below

45 0000 5C | 0003 0000 | 59 06

TTL Protocol.

The above belong to which protocol?

Ans. Protocol = (06)16

$$= 0 \times 16 + 6 \times 16^0$$

$$= 06 \quad \therefore \text{TCP}$$

Qs. In an IPv4 packet the value of TTL is 10 and value of total length field is '0084' hexa decimal, how many byte of data are being carried by this packet?

Ans. TTL = 10

T_L = (0084)₁₆

$$\text{Header Size} = 10 \times 4 = 40 \text{ Byte}$$

$$= 8 \times 16 + 4 \times 16^0$$

$$T_L = D + H$$

$$= 132$$

$$D = T_L - H = 132 - 20$$

$$= 92$$

Q7. For which one of the following reasons does internet protocol (IP) use TTL field in IP Datagram header?

Ans. Prevent packet from looping indefinitely.

Q8. One of the header fields in a IP Datagram is the TTL field. Which of the following statements best explain the need of this field?

Ans. It can be used to prevent packet looping.

Q9. In the TCP/IP protocol suite, which one of the following is not part of IP header?

Ans. Destination port number.

Q10. Which of the following fields of an IP header is not modified by a typical IP router?

Ans Source Address.

Q11. 'A' host (on TCP/IPV4 network A) sends an IP datagram D to host 'B' (also on TCP/IPV4 network B). Assume that no error occurred during the transmission of D. When D reaches B which of the following IP header fields (i) may be different from that of the original datagram D?

(i) TTL (ii) Checksum (iii) Fragment offset.

Ans All of the above

Q12 Which of the following statements is TRUE?

Ans Ethernet frame includes a CRC field and IP packet includes Checksum field.

HW

Q13 Which can be possible header size (in bytes) in IPv4 datagram?

(I) 20. (II) 30. (III) 50. (IV) 60.

Q14 Which can be possible header size (in bytes) in IPv4 datagram?

Ans Header size can be between 20 to 60B

But always multiple of 4. so one is 20, 60.

Q15 An IPv4 packet has the first few hexadeciml digits as shown below.

450000 5C000 30000 590C.

What is the size of data packet

Ans.

$$T_L = (\text{Data})_{16}$$

$$= 5 + 16 + 0 + 12 + 16^0 = 92.$$

$$\text{Header Size} = 5 \times 4$$

$$= 20$$

$$\therefore \text{Data} = 92 - 20 = 72$$

Q16 In IP datagram TCP segment is present header length field of IP datagram is 10 total length of IP datagram is 1000 byte. Header length field in TCP header is 15. then what is the

Sum of TCH data present in the datagram.

Ans.

TPL header = 10

TL = 100010

* TCP Header Lengths

TL : 11

$960 + 60$ [Segment]

960

44

$960 + 40$ [Datagram]

1000

* TCP data size = Total Length (TL) - IP(h) - TCP(h)

$$= 1000100010 - 60$$

$$= 994.$$

Q11. An IPNU packet has arrived with the first 16 bits as [010010110000], the receiver discard this packet. Why?

Ans.

$$Ver = (0100)_2 = 4$$

$$TLEN = (0010)_2 = 2.$$

$$\text{Header Size} = 2^4 = 8$$

$$\text{Min header Rto} = 20 \text{ Bits}$$

$$\text{Min TLEN field} = 20 - 8$$

$$= 4$$

\therefore Invalid TLEN

Q12. An IPNU packet has first few hexadecimal digits as shown below

450000 5C1000 30000 | 59060000 | 0A000E05
 1st row 2nd row 3rd row 4th row

What is the Source IP address in the last part?

Ans.

$$SIP = (\text{DA}, \text{OC}, \text{OE}, \text{OS})$$

$$= 10^{16} = 10 + 12^{16} = 12 \quad 14^{16} = 14 \quad 5 \times 16 = 16$$

$$= 10, 12, 14, 16.$$

Q13. Which of the following value is/are not possible of the TL in a datagram?

Ans.

TPL = 8 bits

TPL value cannot be zero

Range = 0 to 2^8

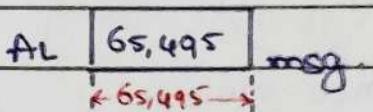
= 0 to 256

\therefore TPL value cannot be 0 and 301

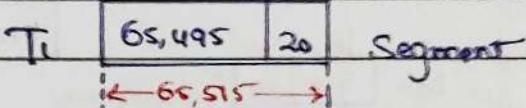
Note:

- * If there is no option field (in IP header) then the value not change when packet is moving from one router to another.
- * If there is a option field present in IP header then the field maybe changed when packet is moving from one router to another router.

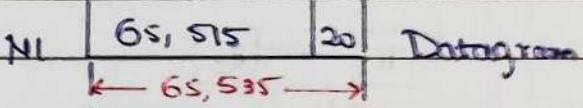
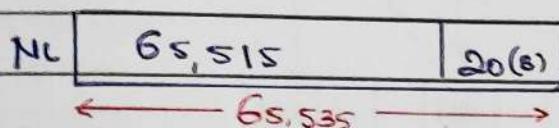
→ Total length = 16 bit.



$$\text{Max. size} = 2^{16} - 1 = 65,535$$



Total length = Data + Header.



Data.

Hd Frame

→ AL can pass any size of data to transport layer.

1480

AL



Data.

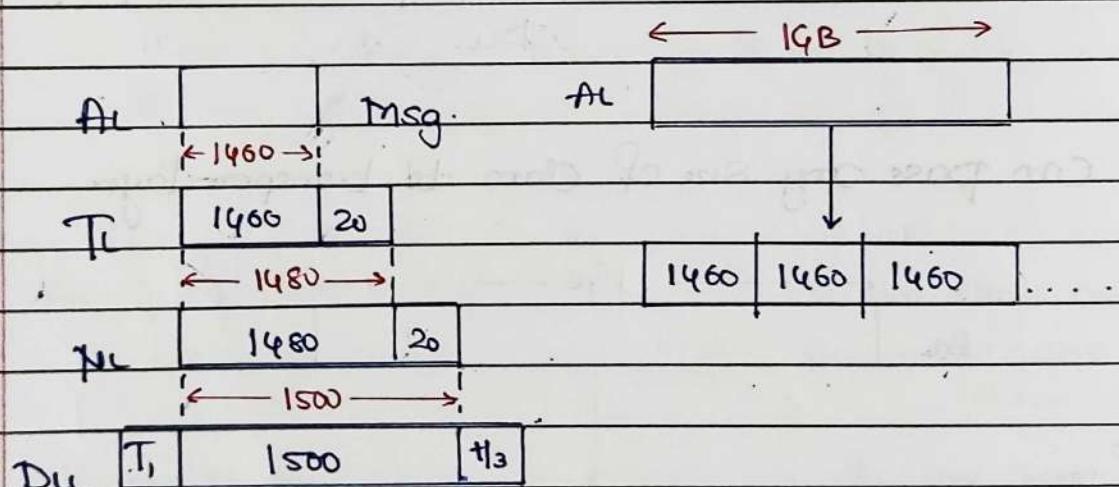
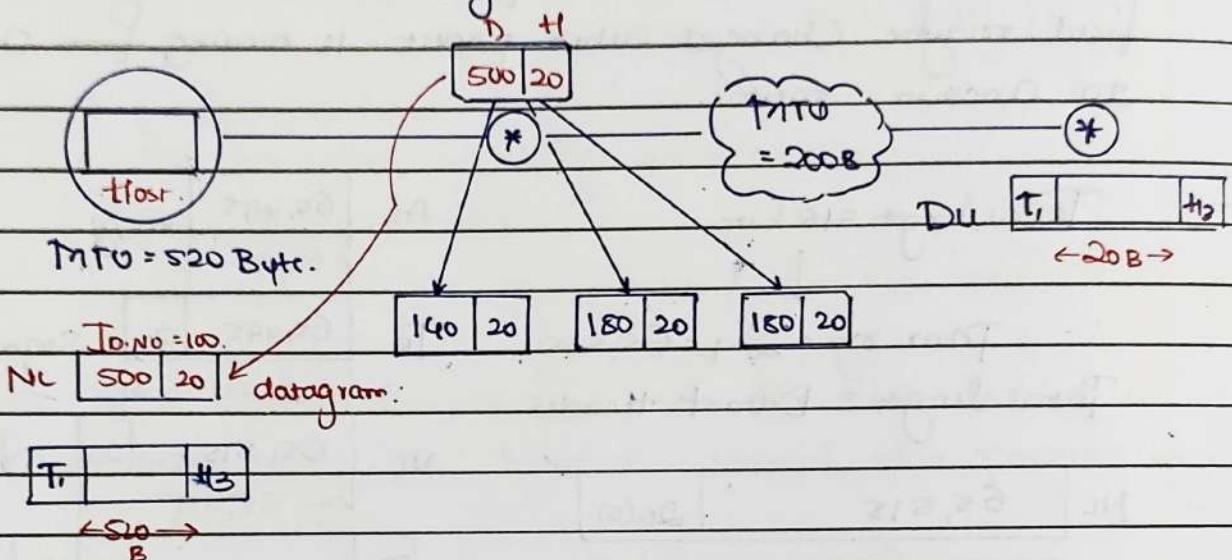
Hd.



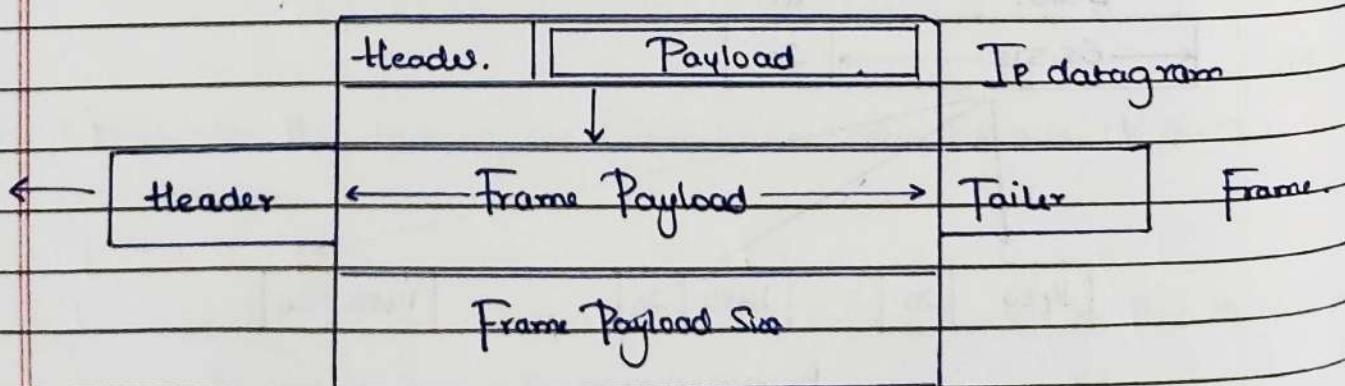
Fragmentation

Fragmentation at Router.

MTU = Maximum amount of data that can be stored in any Data Link layer.

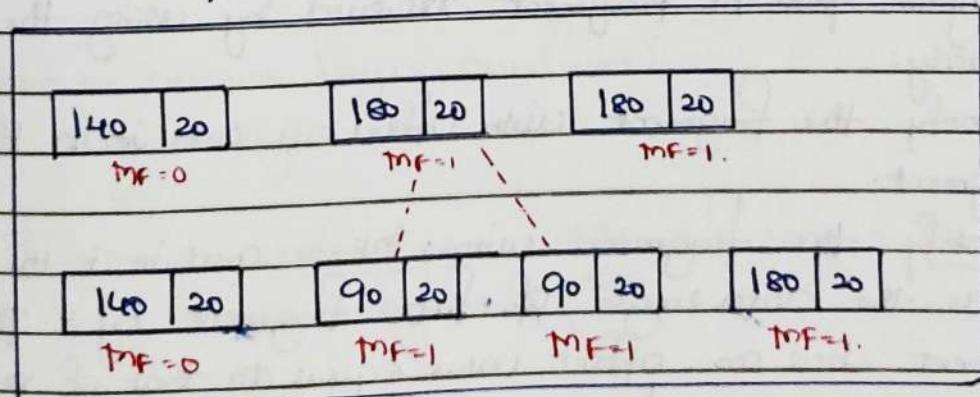
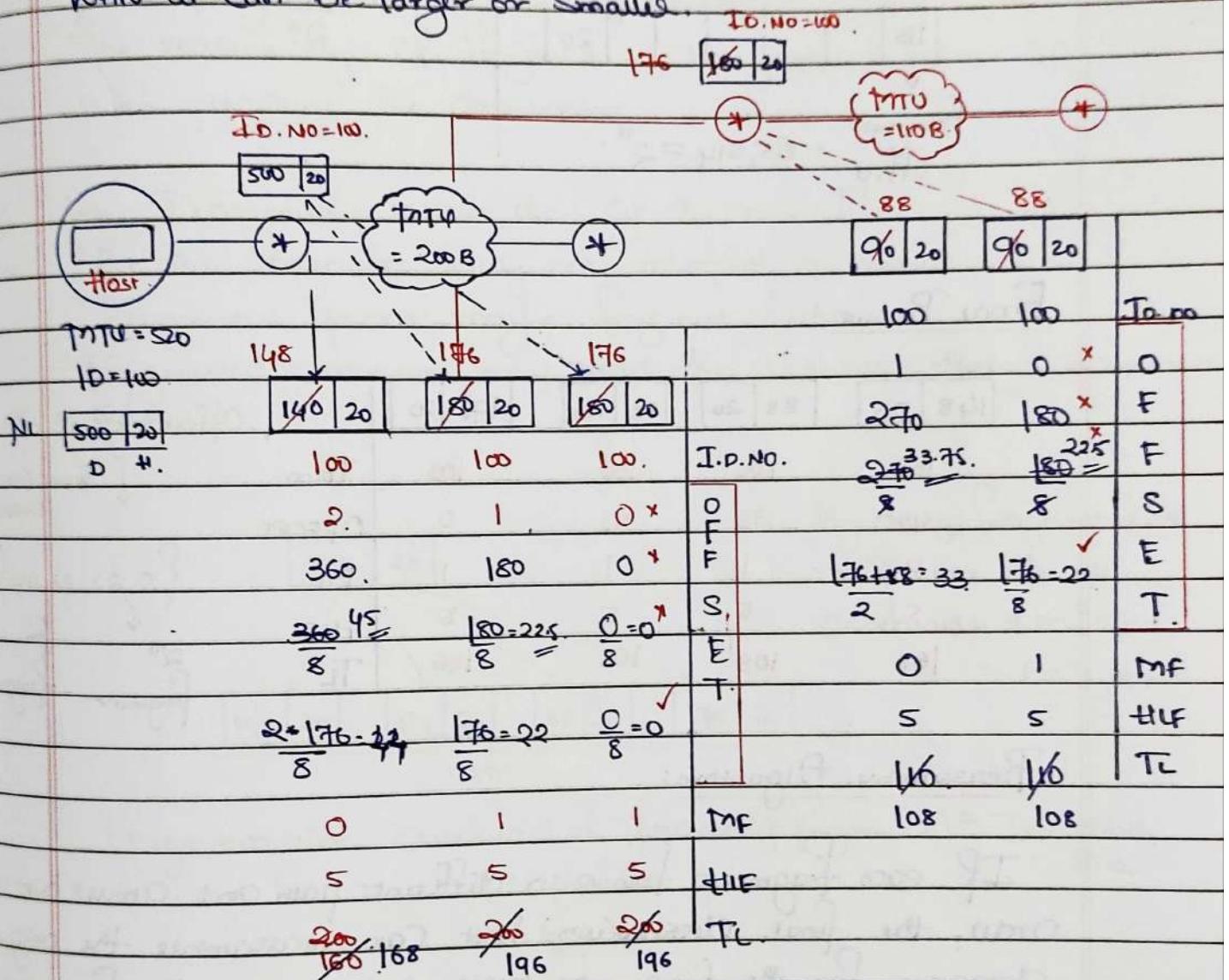


Maximum Transfer Unit (MTU)



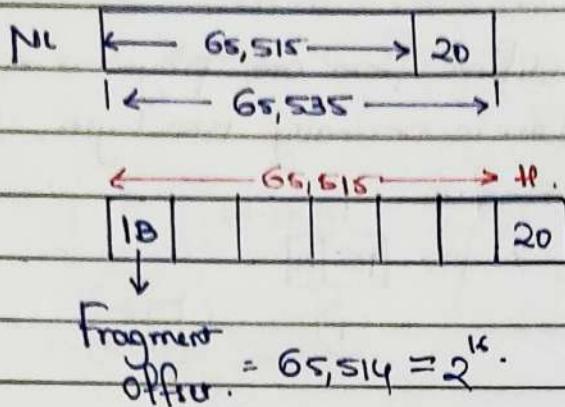
* When a datagram is encapsulated in a frame, the total size of the datagram must be less than the maximum size of the frame payload.

* The value of the MTU differs from one physical network. For example, the value of a LAN is normally 1500 bytes, but for a WAN it can be larger or smaller.



Total Length = 16 bit.

Maximum. no = $2^{16}-1 = 65,535$.



Fragment Offset = 12 bit.

Maximum. no = $2^{12}-1 = 4095$.

$$\underline{2}^{16} = \underline{2}^{13}$$

S.F. \leftarrow 2

$$\frac{\underline{2}^{16}}{\underline{2}^3} = \underline{2}^{16-3} = \underline{2}^{13}$$

Final Result:

| | | | | | | | | |
|-----|-----|-----|-----|-----|-----|-----|-----|--------------------------|
| 148 | 20 | 88 | 20 | 88 | 20 | 176 | 20 | Offset = {22, 33, 0, 44} |
| 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | ↓ Increasing Order |
| 44 | 33 | 22 | 0 | 0 | 0 | 0 | 0 | OFFSET |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | TMF |
| 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | TL |
| 168 | 108 | 108 | 196 | 196 | 196 | 196 | 196 | 2 nd fragment |
| | | | | | | | | 4 th fragment |

Reassemble Algorithm:

If each fragment follows a different path and arrives out of order, the final destination host can reassemble the original datagram from the fragment received by using the following strategy:

1. Identify the fragment with offset = 0 and it is the first fragment.
2. Identify the fragment with TMF = 0 and it is the last fragment.
3. Divide the data length of first fragment by 8. The second fragment has an offset value equal to that of result.
4. Divide the data length of first and second fragment by 8.

- The third fragment has an offset value equal to three.
- Repeat the process as many times as possible to construct the fragment.

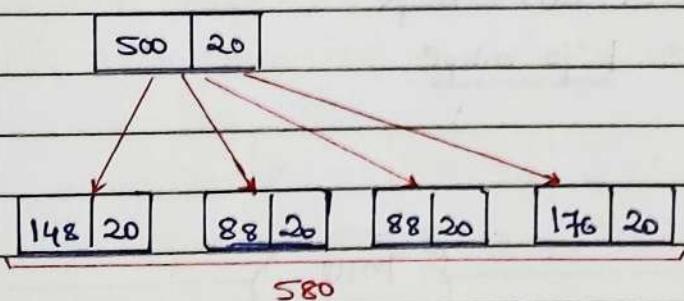
Note:

- * Fragmentation is done by intermediary devices such as Router.
- * The reassembly of fragmented datagrams is done only after reaching the destination.

Q. Why Reassembly is not done at the router?

- Ans.
- * All the fragments may not meet at a router.
 - * Fragmented packet may fragment further.
 - * Fragmented datagram may reach the destination through independent path.

By doing fragmentation at Router the NL Overhead = $580 - 20$
 $= 60 \text{ Byte}$.



$$\begin{aligned} \text{Fragmentation Overhead} &= (\text{Total no of Fragments} - 1) * \text{Total Header Size.} \\ &= (4 - 1) * 20 \\ &= \underline{\underline{60}} \end{aligned}$$

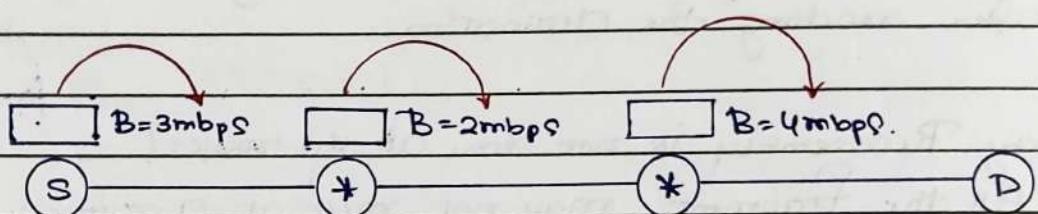
Q2 What is Network Layer Overhead?

Anc $580 - 560 = 20 \text{ Byte}$

$$\text{Efficiency} = \frac{\text{useful byte}}{\text{Total Byte}} = \frac{560}{580} = 0.9620 = \underline{\underline{86.2\%}}$$

Fragmentation Overhead.

1. Fragmentation of datagram increase the overhead.
2. This is because after fragmentation, IP header has to be attached with each fragment.
3. $\text{Total Overhead} = (\text{Total no. of fragments} - 1) * \text{Size of IP header}$



$$\text{Throughput} = \eta * B$$

$$\text{Throughput} = \eta + \text{min. bandwidth}$$

$$\begin{aligned}\text{Throughput} &= 0.86 \times 2 \text{ mbps} \\ &= \underline{\underline{1.72 \text{ mbps}}}\end{aligned}$$

ex: 1.

1500 20

MTU

$$= 525$$

492 20

504 20

505 20

$$\frac{2 \times 504 - 126}{8}$$

$$\frac{504}{8} - 63$$

$$\frac{0}{8} = 0$$

Offset

0

1

1

MF

512

524

524

TI

Problem Solving on Fragmentation:

- Q1. An IP datagram of size 1000 Bytes arrives at router. The router has to forward this packet on a link whose MTU is 100 bytes. Assume the size of the IP header is 20 bytes. The no. of fragments that the IP datagram will be divided into for transmission is. 13

Ans.

$$980 + 20.$$

$$\leftarrow 1000 \rightarrow$$

$$12 \times 80 = 960$$

$$980 - 960 = 20 \text{ Byte (Remaining)}$$

\therefore 13 parts to be divided

- Q2 If the value available in "fragment offset" field of IP header is 100, then the number of bytes ahead of this fragment is

Ans.

$$\text{Fragment offset} = 100$$

$$\begin{aligned} \text{No. of byte ahead of this fragment} &= 8^*100 \\ &= 800 \end{aligned}$$

| | | | | |
|-----------------------|-------------------|-----|--------|--|
| 100 | +1 | 800 | +1 | |
| $\frac{800 - 100}{8}$ | $\frac{0}{8} = 0$ | | Offset | |

- Q3 In IPv4 datagram, offset value is non zero and is the last one, then what is the position of datagram?

Ans. Neither first fragment nor last fragment.

HW

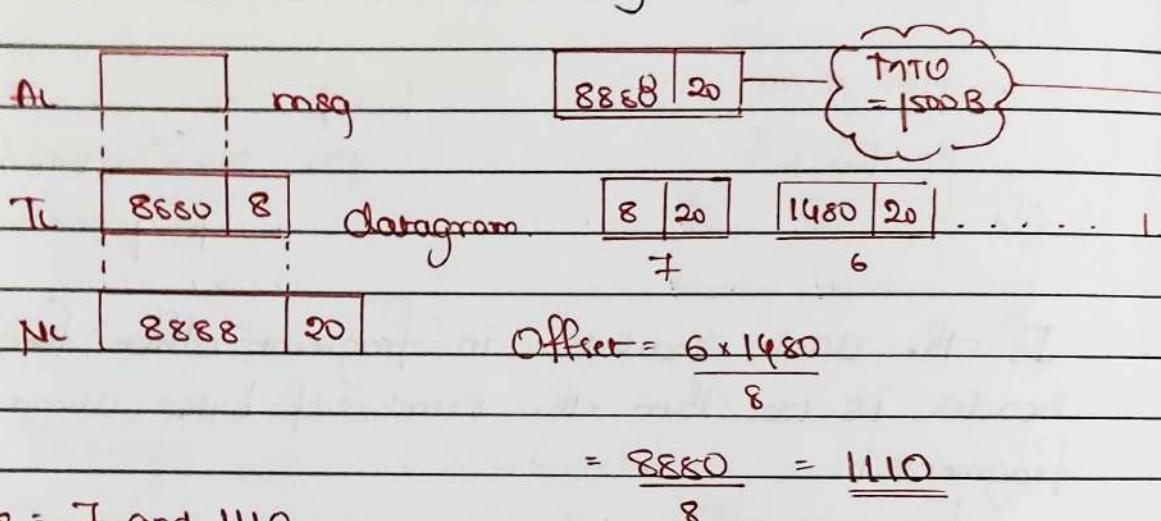
- Q4. An IP router with a MTU of 1500 bytes has received an IP packet of size 4604 bytes with an IP header of length 20 bytes. The values of the relevant fields in the header of the third IP fragment generated by the router for this packet are:

Ans.

$$\frac{2+1480}{8} = 370$$

Q5. Host A send a UDP datagram Containing 8880 bytes of user data to host B over Ethernet LAN. Ethernet frame may carry data upto 1500 bytes (i.e. MTU = 1500 bytes). Size of IP header is 20 bytes and size of TCP header is 20 bytes. There is no option field in IP header. How many total number of IP fragments will be transmitted and what will be the contents of offset field in the last fragment?

Ans.



Ans = 7 and 1110.

Q6. In an IPv4 Datagram, HLEN is 10, the value of TLEN is 10, the value of total length is 400 and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and last bytes of payload, respectively are:

Ans.

$$\text{HLEN} = 10$$

$$\text{Header Size} = 10 \times 4 = 40 \text{ bytes}$$

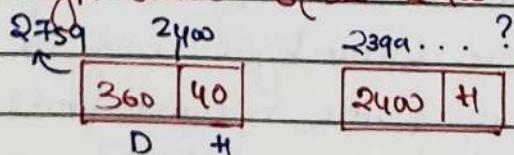
$$\text{Tl} = 400$$

$$\text{Tl} = D + H$$

$$D = \text{Tl} - H = 400 - 40 = 360 \text{ bytes}$$

Fragment offset: 300

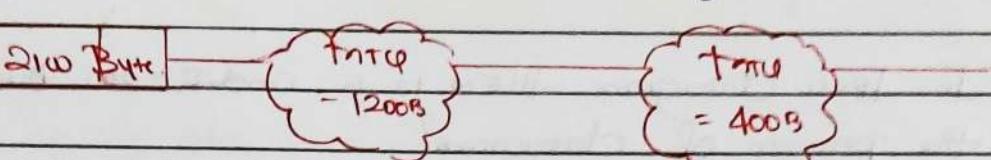
$$\text{No. of bytes type ahead} = 8 \times 300 = 2400$$



Ans: Last fragment 2400 and 2759

Q7. A message consisting of 2100 bytes is passed to IP for delivery across two networks. The first network can carry a maximum payload of 1200 bytes per frame and second network can carry a maximum payload of 400 bytes per frame, excluding network overhead. Assume that IP overhead per packet is 20 bytes. What is the total IP overhead if the second network is considered for transmission of 2100 bytes?

Ans



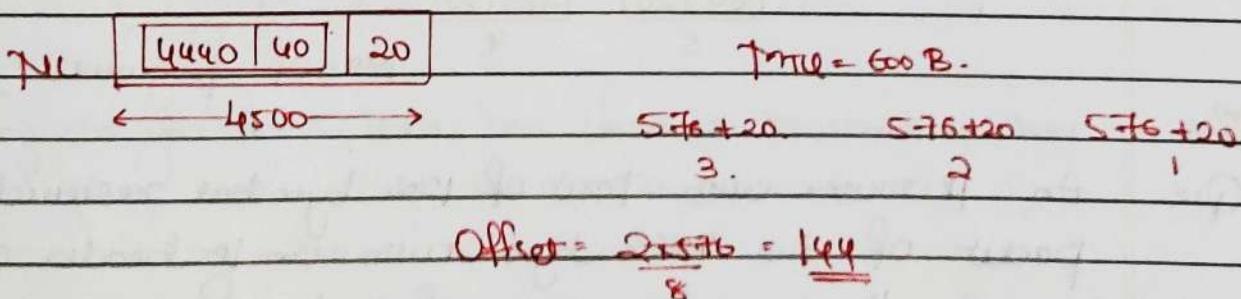
$500 + 400 + 1200 = 2100$
→ Divided into 3 fragments

$$\text{Total overhead} = 6 \times 20 = 120 \text{ B}$$

Q8. Consider an IPv4 packet with a length of 4500 bytes that includes a 20-byte IP header and 40-byte TCP header. The packet is forwarded to an IPv4 router that supports a maximum transmission unit [MTU] of 600 bytes. Assume that the length of the IP header in all outgoing fragments of this packet is 20 bytes. Assume that the fragmentation offset value stored in the first fragment is 0.

The fragmentation offset value stored in third fragment is 144.

Ans



Q9.

A packet has arrived in which the offset value is 100, the value of TLEN is 5 and the value of total length field is 100. What are the number of first byte and the last byte of the payload? (800 - 879)

Ans.

Offset value = 100

TLEN = 5

No. of bytes ahead = 8×100 Header size = $5 \times 4 = 20$ Byte

TL = 100

$$D = TL - 11 = 100 - 20 = 80$$



$$\text{Offset} = \frac{800 - 100}{8} =$$

Q10. In IPv4 datagram TLEN is 5 and TL = 200, then calculate the position of datagram?

Ans.

TLEN = 5

Header size = $5 \times 4 = 20$ Byte

TL = 200

Data = $TL - 11$

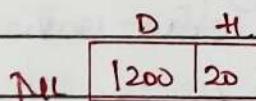
$$= 200 - 20$$

$$= 180 \rightarrow \text{not divisible by 8}$$

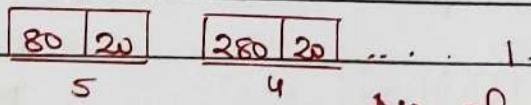
\therefore Last fragment

Q11. Consider transport layer packet (PDU) size is 1200 Byte, IPv4 header size is 20 Byte and MTU is 300 Byte then number of IP fragments is _____.

Ans.



MTU
= 300B



No. of fragments = 5

TW

Q12. An IP router with MTU of 1200 byte has received an IP packet of size 4408 byte with an IP header of 20 byte what is the total length value of the last fragment _____

Q13

If an router receives an IP packet containing 300 data bytes that has to forward the packet to the network with maximum transmission unit of 50 byte. Assume that IP

Header is 10 byte long. Find the total fragment, max fragments and offset value.

Q14 Consider Pmt size of transport layer packet is 2260 Bytes or Source host. MTU for the network is 400 Bytes and 1844 (headers). So is 20 Bytes the no. of fragments for given Pmt size 6

Ans

NL 2260 | 20

+12.

380 | 20

376 | 20

6

5

.

.

.

∴ No. of fragments = 6.

Q15 A packet has arrived with the offset value is 100 what is the number of first byte 800

Ans

Offset = 100

No. of data bytes ahead = $8 \times 100 = 800$

Q16 Consider the following fields in IP header and choose correct combination.

Ans

MF

→ zero for first fragment.

DF

→ It must be available in all fragments

Offset

→ If it is '1' then frag. is allowed

Strict Source
Routing.

→ Zero for last fragment.

Q17 Why do you think IPv4 has fragment reassembly done at the end point rather than at the top router.

Ans

Fragments may follow different routes.

Q18

In an IPv4 datagram, M bit is zero and fragment offset value is zero, then the fragment is No fragmentation.

MF = 0 → Last fragment / only fragment

Offset = 0 → 1st fragment

Q19. In an IPv4 datagram, T bit is one, then fragment is
Ans Both first and middle fragment.

~~HW~~ Q20. A packet has arrived in which the offset value is 100, the value of TTL is 5 and the value of total length is 100 what is the number of last byte

Q21. Find number of fragments while packet traverse through network units below details in incoming packet header and network characteristics. MTU size 300 Bytes, network header as 20 Bytes, DF bit is 1 and incoming datagram data size as 1000 Bytes.

Q22. Consider the following statements about the functionality of an IP based router

- I. A router does not modify the packet during forwarding
- II. It is not necessary for a router to implement any routing protocol.
- III. A router should reassemble IP fragments if the MTU of the outgoing link is larger than the sum of the incoming IP packets.

Q23. An IPv4 datagram is received by an IPv4 router, TTL field contains value 10 and total length field contains value 2060, MTU of the link is 100 bytes. Calculate the total no. of IP fragments after fragmentation.

Q24. An IPv4 datagram has arrived in which the offset value is 500, the TTL is 8, and the value of total length field is 500 and T bit is 0. What are the number of the 1st byte and the last byte and the position of the datagram.

Header, TCP

| | | | |
|---------------------|--------------------------------|--|-----------|
| | 16 bit | 16 bit. | |
| | Source Port. (16 bit) | Destination Port. (16 bit) → 4B | |
| | Sequence Number (32 bit) | → 4B | |
| | Acknowledgment number (32 bit) | → 4B | |
| 20 Bytes | | | |
| Header fixed | T.H. R.S.R. U.A.P.R.S.F | Window Size or (Advertisement window) (16 bit) | → 4B. |
| | 4 bit. 6 bit. G K H T N N | | |
| 40 B. (Variable) | Check Sum (16 bit) | Ongent Pointer (16 bit) → 4B | |
| | Options (0-40 Bytes) | | 20 Bytes. |

$$\text{Min. Header Size} = 20 \text{ B} + 0 = 20 \text{ B}$$

$$\text{Max. Header Size} = 20 \text{ B} + 40 \text{ B} = 60 \text{ B}$$

$$\text{H.L. (Header Length)} = 4 \text{ bit} \rightarrow \text{Max no. } 1111 = 15$$

Maximum header size = 60 Byte.

$$[S.F] = \frac{60}{4} = 15$$

Port no. = 16 bit.

$$\text{Range} = (0 \text{ to } 2^{16}-1) = 0 \text{ to } 65,535$$

↓ { Well known port no.
1023 Assigned & controlled by IANA }

Port No.

SMTP → 25

HTTP → 80

FTP. { 20
21 }

↓ { Reserved or Registered Port No.
49,151 Not assigned and controlled by IANA
only registered with IANA. }

DNS → 53.

↓ { Dynamic Port number.
Neither controlled nor registered
with IANA. }

65,535

Source port address: This is a 16 bit field that defines the port number of the application program in the host that is sending the segment.

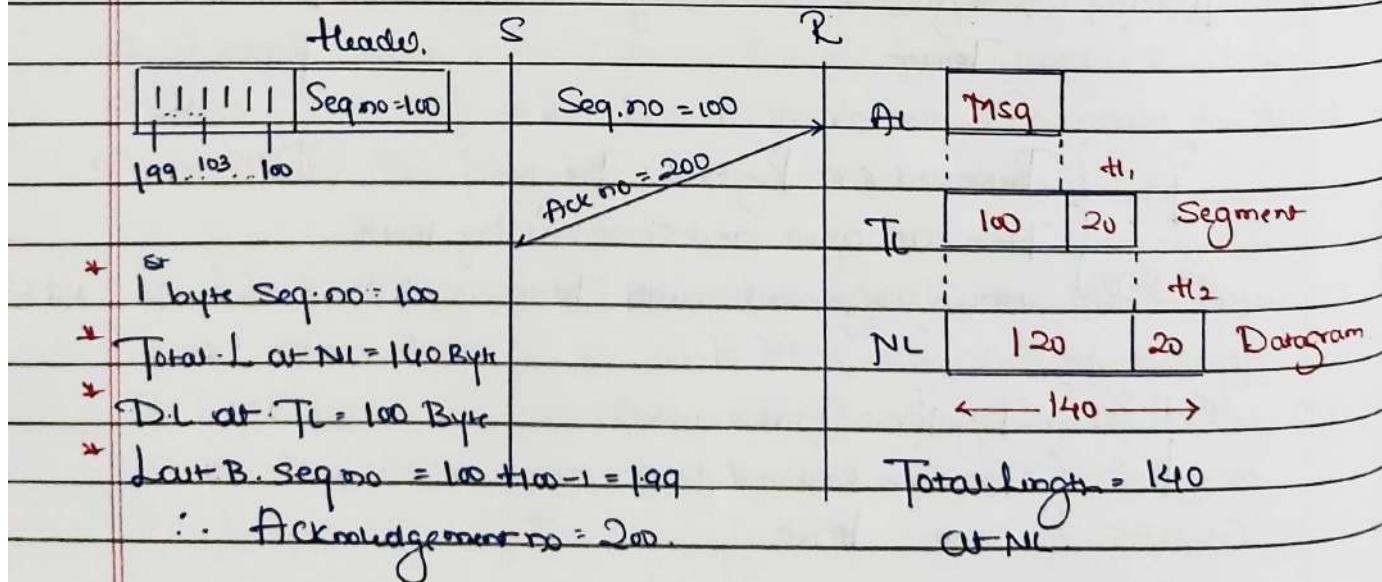
Destination port address: This is a 16 bit field that defines the port number of the application program in the host that is receiving the segment.

Sequence number: This is 32 bit field that defines the sequence number of the first data byte.

Note: * TCP is a byte Stream protocol i.e every byte is associated with one sequence number.

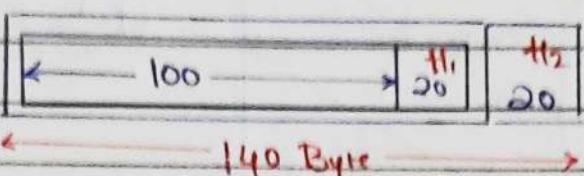
* IP is a packet stream protocol i.e every packet is associated with one sequence number.

Acknowledgement Number: This is a 32 bit field defines the sequence number of the next expected byte. If the receiver has received successfully the byte number 'x' from other party, it returns the acknowledgement number 'x+1' back to the sender.



OR

NL



→ Data Size at TL

$$\begin{aligned} \text{Total length (Ip)} &= IP(H) \\ &- TCP(H) \end{aligned}$$

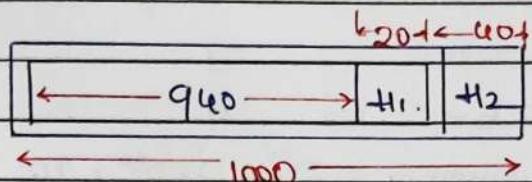
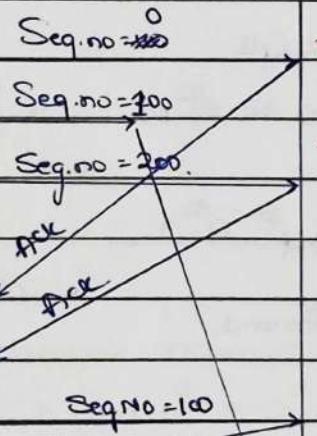
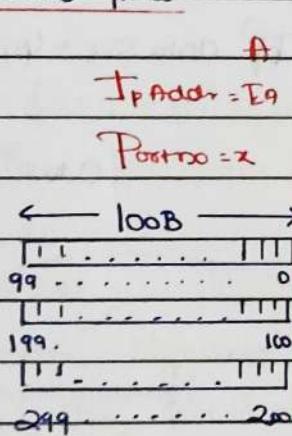
Q1. $TTL = 10$ } IP
 Total length = 1000 }
 Seq. No. ? TCP
 $HL = 5$
 $Ack\ No. = ?$

Data Size at TL = 940

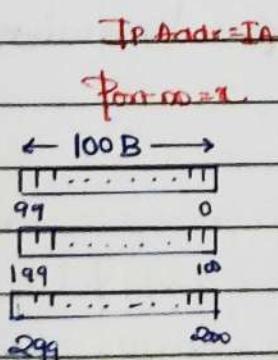
1st Byte Seq. No. = 100

$$\begin{aligned} \text{Last byte Sequence No.} &= 100 + 940 - 1 \\ &= 1039. \end{aligned}$$

Ack no. = 1040.

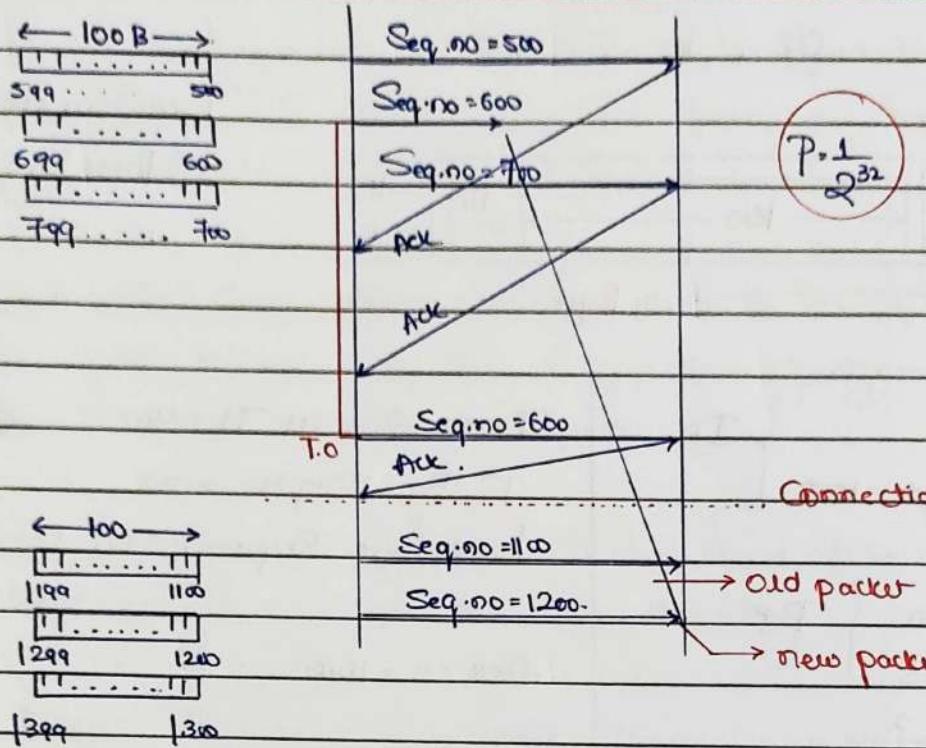
Sol:Wrap Around Time

Connection Close



Seq. no = 0
 ✓
 Seq. no = 100
 ✗

Note: TCP suggest that do not start the Sequence number with 0. Always choose any random Sequence number initially.



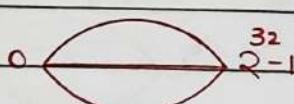
Sequence No = 32 bit

Total Sequence number = $2^{32} = 2^2 \times 2^{30} = 4G$ Sequence Number.

Data Size = 4GB

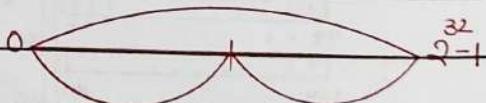
If data size > 4GB.

Seq. no = 2^{32} (0 to $2^{32}-1$)



If data size = 4GB + 4GB

0 to $2^{32}-1$ 0 to $2^{32}-1$



Random Seq. no = 1024

Wrap Around time: Time taken to wrap around.

Wrap Around.

Note: Wrap Around time depends upon bandwidth.

①

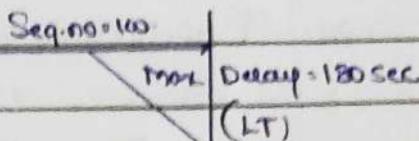
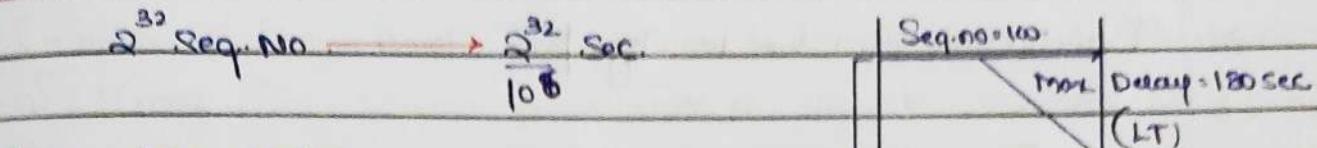
$$B = 1MBPS = 10^6 \text{ Byte/sec}$$

$$1 \text{ sec} \rightarrow 10^6 \text{ Byte}$$

$$10^6 \text{ Byte} \rightarrow 1 \text{ sec}$$

$$10^6 \text{ seq. No} \rightarrow 1 \text{ sec}$$

$$1 \text{ seq. No} \rightarrow \frac{1}{10^6} \text{ sec}$$



W.A.T. > LT No problem.

$$\text{W.A.T.} = \frac{\text{Total seq. no.}}{(\text{Bandwidth}) \text{ Byte/sec.}}$$

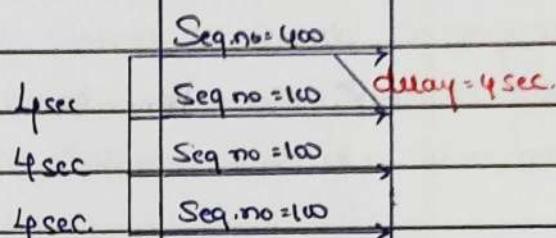
② $B = 1 \text{ Gbps} = 10^9 \text{ Byte/sec}$

10⁹ Byte → 1 Sec.

10⁹ Seq. No. → 1 Sec

1 Seq. No. → $\frac{1}{10^9}$ Sec

2³² Seq. No. → $\frac{2^{32}}{10^9}$ Sec



W.A.T. < LT

W.A.T. = 1.294 sec.

Problem.
 $(\text{Lifetime} = 180 \text{ sec.})$

$B = 1 \text{ Gbps} = 10^9 \text{ Byte/sec.}, \text{LT} = 180 \text{ sec.}$

1 Sec → 10⁹ Byte

1 Sec → 10⁹ Seq. No

180 Sec → 180×10^9 Seq. No

→ Minimum Sequence number required to avoid wrap around within the life time = $180 \times 10^9 = 2^8 \times 2^{30} = 2^{38}$.

→ Minimum number of bits required in the Sequence no. field to avoid wrap around time in the life time = $\lceil \log_2 180 \times 10^9 \rceil = 38 \text{ bit}$
 $[\log_2 \text{LT} \times B]$

Note:

1. Minimum Sequence number required to avoid wrap around time within life time = $\text{LT} \times B$.
2. Minimum number of bits required in the Sequence Number field to avoid wrap around time in the life time = $[\log_2 \text{LT} \times B]$

3. Bandwidth must be in Byte/sec.

$$\text{Extra bits} = 38 - 32 = 6 \text{ bits}$$



Option → Time Stamp = 6 bits

$$\begin{aligned}\text{Range} &= 0 \text{ to } 2^6 - 1 \\ &= 0 \text{ to } 63.\end{aligned}$$

Time Stamp = 6 bits

1st Set time Stamp value = 000000 → 0

2nd Set time Stamp value = 000001 → 1

:

64th Set time Stamp value = 111111 → 63.

$$2^6 \text{ Seq.no} = 2^6 = 64 \text{ Seq.}$$

$$2^6 \text{ Seq.NC}$$

$$2^{32} \times 64 = 2^{32+6} = 2^{38}$$

Ser.

| | | |
|--------|-------------------------|----------------|
| | S.N = 00, TimeStamp = 0 | |
| 4 sec | S.N = 00, timestamp = 1 | delay = 4 sec. |
| 4 sec. | S.N = 00, timestamp = 2 | |

Q1. Consider 200 Mbps network with a Sequence number field 28bit
The wrap around time of sequence number is.

Ans

$$B = 200 \text{ Mbps} = 200 \times 10^6 \text{ bits/sec}$$

$$B = \frac{200 \times 10^6}{8} \text{ Bytes/sec} = 25 \times 10^6 \text{ Bytes/sec}$$

Shortest:

$$25 \times 10^6 \text{ Bytes} \rightarrow 1 \text{ sec}$$

$$25 \times 10^6 \text{ Seq.No} \rightarrow 1 \text{ sec}$$

$$1 \text{ Seq.No} \rightarrow \frac{1}{25 \times 10^6} \text{ sec}$$

W.A.T = total Seq.no

[Bandwidth] Bytes/sec.

$$\text{W.A.T} = \frac{2^{28}}{25 \times 10^6} \text{ sec}$$

$$\text{W.A.T} = 10.73 \text{ sec}$$

$$\text{W.A.T} = 10.73 \text{ sec.}$$

Q2. Consider a long-lived TCP session with an end-end bandwidth of 1Gbps. The session starts with a sequence number of 1234. The minimum time (in seconds, rounded to the closest integer) before the sequence number can be used again is _____.

Ans $B = 1\text{Gbps} = 10^9 \text{ bits/sec}$

$$\text{WAT} = \frac{\text{total seq.no}}{(\text{Bandwidth}) \text{ Byte/sec}} = \frac{2^{32}}{\frac{10^9}{8}} = \frac{8 \times 2^{32}}{10^9} = 34.35 \therefore \underline{34 \text{ sec}}$$

Q3. Consider the data transfer using TCP over a 1Gbps link. Assuming that the maximum segment lifetime is set to 60 seconds. The min. number of bits required for the sequence number field of the TCP header, to prevent the sequence number space from wrapping around during the TSL is _____.

Ans $B = 10^9 \text{ bits/sec}, LT = 60 \text{ sec.}$

$$B = \frac{10^9}{8} \text{ Byte/sec.}$$

$$\begin{aligned} & \text{Min. no of bit required to avoid WAT within lifetime} \\ & = \lceil \log_2 LT \times B \rceil = \lceil \log_2 60 \times \frac{10^9}{8} \rceil - \lceil \log_2 7 \times 10^9 \rceil = [32.8] \\ & = \underline{33 \text{ bits}} \end{aligned}$$

Q5 Suppose you are asked to design a new reliable byte-stream transport protocol like TCP. This protocol named myTCP, runs over a 100Mbps network with RTT of 150ms and the max. segment lifetime of 2 minutes. Which of the following is/are valid lengths of the Sequence number field in the TCP header?

Ans $B = 100 \text{ Mbps} = 100 \times 10^6 \text{ bits/sec}, LT = 2 \text{ min} = 120 \text{ sec}$

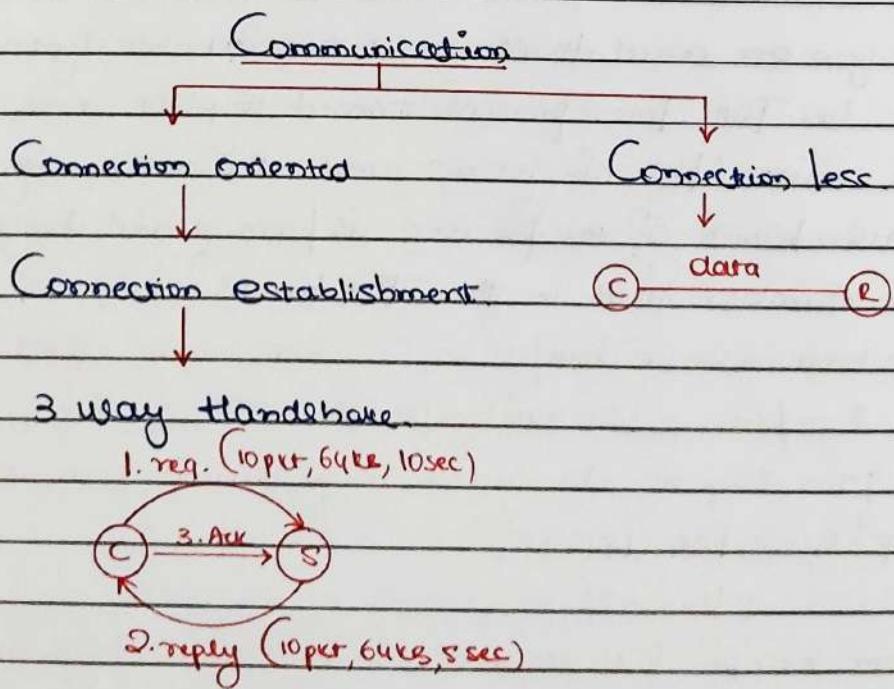
$$\frac{100 \times 10^6}{8} \text{ Byte/sec} = 12.5 \times 10^6 \text{ bytes/sec}$$

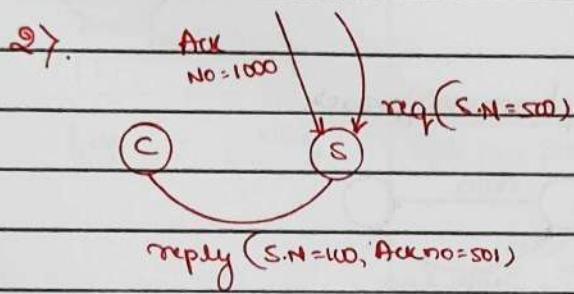
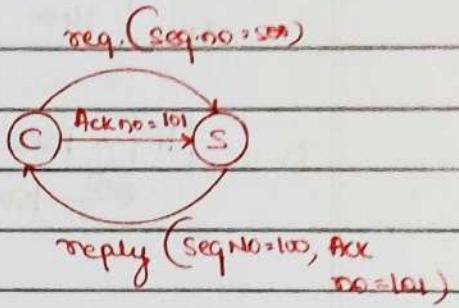
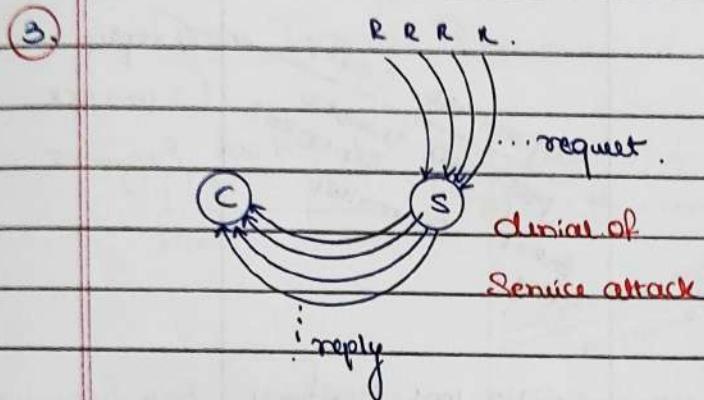
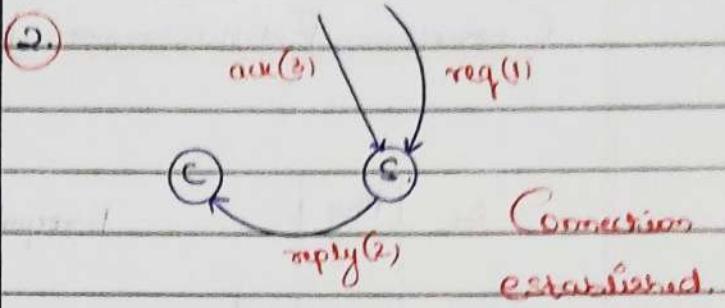
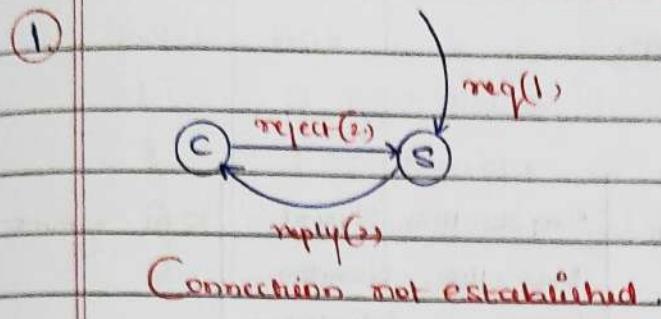
$$\begin{aligned} & \text{Min seq. no to avoid wrap around time within the lifetime} \\ & = LT \times B = 120 \times 12.5 \times 10^6 \\ & = 1500 \times 10^8 \end{aligned}$$

$$\begin{aligned} & \text{Minimum no. of bits required in the sequence length field} = \lceil \log_2 1500 \times 10^8 \rceil \\ & = [30.32] = \underline{31 \text{ bits}} \end{aligned}$$

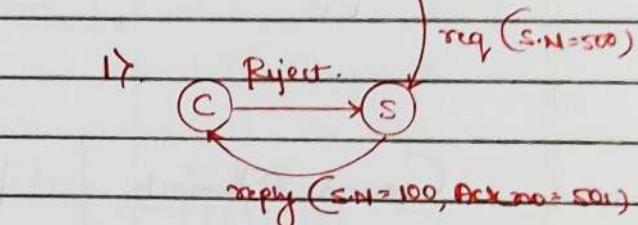
Important Points about TCP:

1. TCP is a connection oriented and reliable protocol (TCP has both flow and error control mechanism).
2. It is a virtual connection and not physical i.e. Segments of TCP may follow different paths, some of them may be lost or duplicated or arrive out of order. Segments are encapsulated in IP datagram.
3. Virtual Connection means resources like buffers are allocated in advance at the Client and Server side before starting transmission.
4. TCP connection have 3 phases:
 - (i) Connection establishment
 - (ii) Data transfer
 - (iii) Connection terminated
5. TCP connection is a Full Duplex Connection i.e. data can be sent in both the directions.
6. TCP uses Sliding window Protocol for its flow control (GBN & SR)
7. Each TCP connection have 4 windows.





Connection not established.



Note: Sequence number and Ackno
are also used for authentication
purpose

Flags

URG → Urgent Flag

ACK → Acknowledgement Flag

PSH → Push flag

RST → Reset Flag

SYN → Synchronization Flag

FIN → Finished Flag

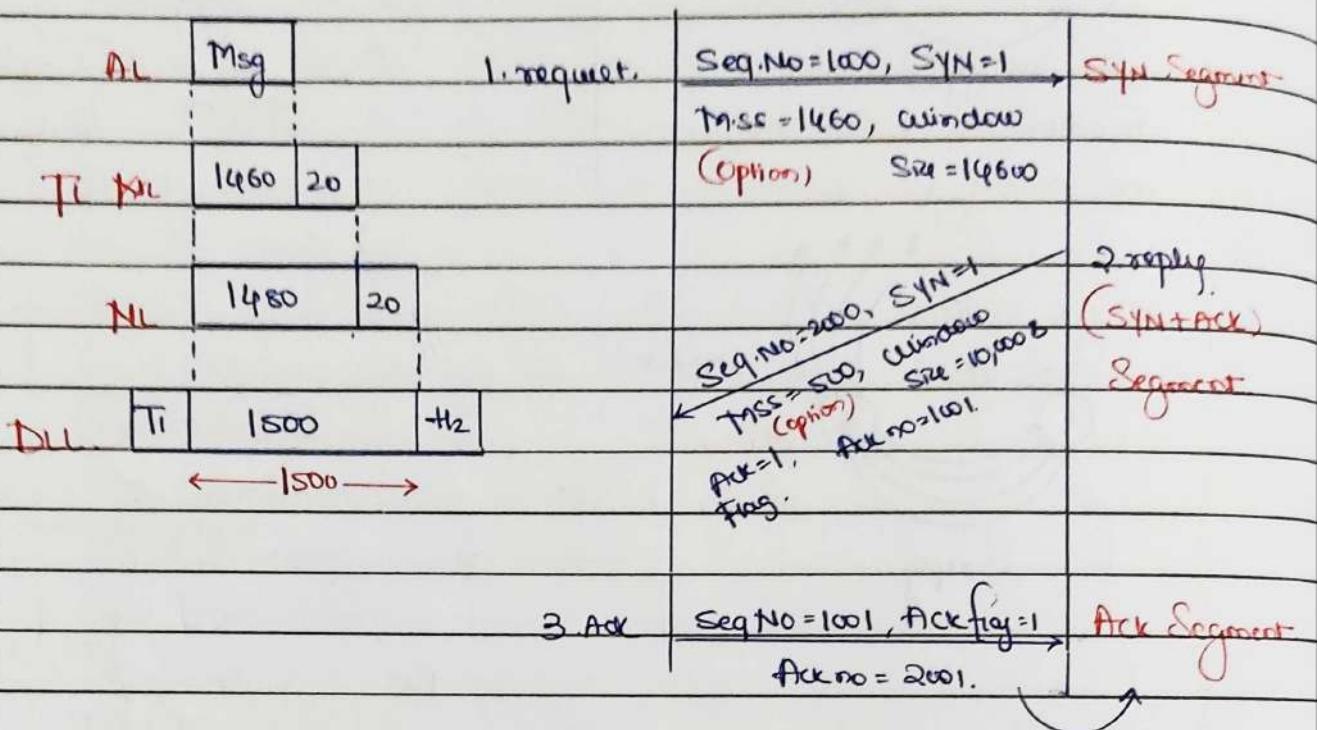
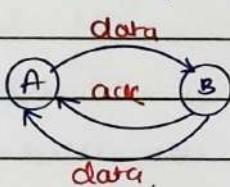
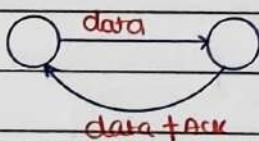
Phases of TCP Connection

1. Connection Establishment Phase

2. Data Transfer Phase

3. Connection Termination Phase

* SYN and ACK are used in
Connection Est. Phase

Connection Establishment Phase.General ApproachPiggy backed approach

SYN = 1 : Consume One Sequence number.

FIN = 1 : Consume One Sequence number.

ACK = 1 : Consume NO Sequence number.

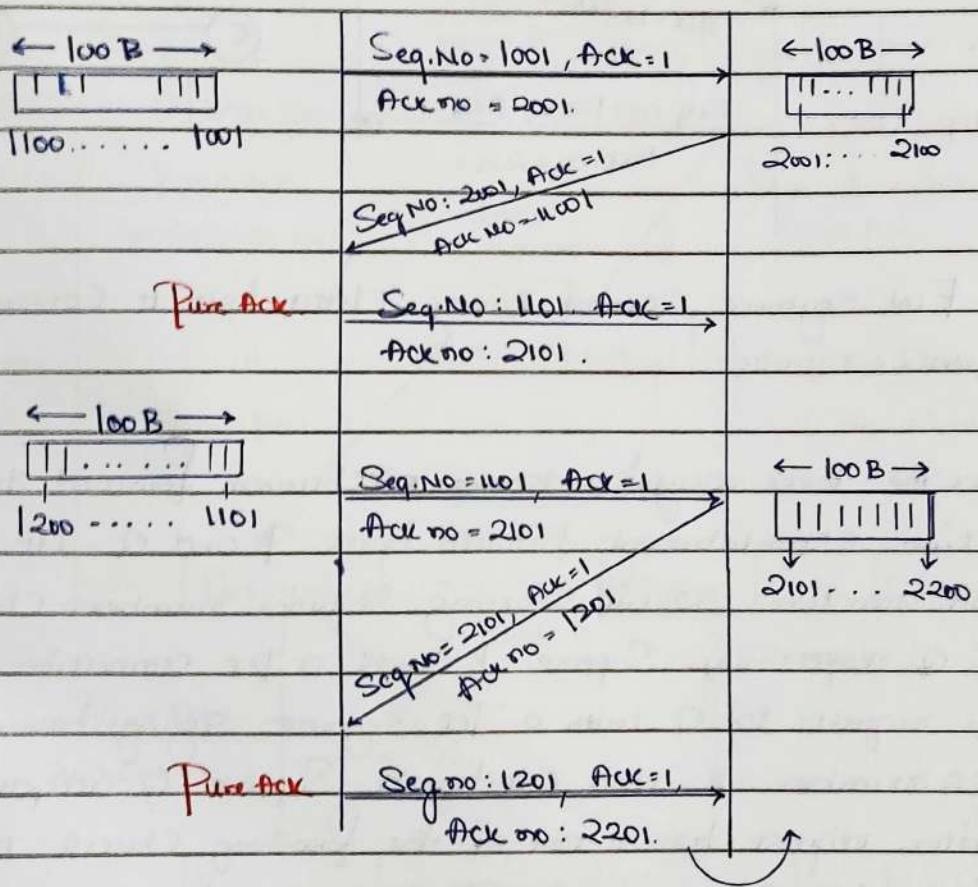
1 DataByte : Consume One Sequence number.

Note:

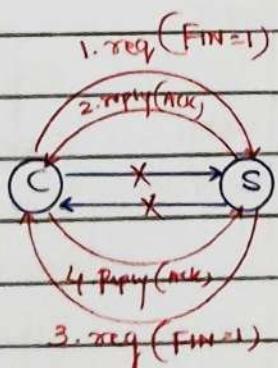
1. A SYN Segment Cannot Carry data, but it consume One Sequence number.
2. A SYN+ACK Segment Cannot Carry data, but it consume one Sequence number.
3. An ACK Segment if carry no data then it will not consume Sequence Number.

| SYN | ACK | |
|-----|-----|------------------|
| 1 | 0 | request |
| 1 | 1 | reply |
| 0 | 1 | ACK/piggybacking |
| 0 | 0 | data |

Data Transfer Phase.



Connection Termination Phase



FIN: Flag is used in connection termination phase.

Connection termination is a four-way handshake.

| | | |
|-------------|--|-------------|
| C req. | Seq.no = 1201, FIN = 1 ACK = 1, ACK NO = 1201 | S |
| | Seq.no = 1201, ACK = 1 ACK NO = 1202. | reply (ACK) |
| | Seq.no = 2201, FIN = 1 ACK = 1, ACK NO = 1202 | request. |
| req. ACK | Seq.no = 1202, ACK = 1 ACK NO = 2202. | C X S |

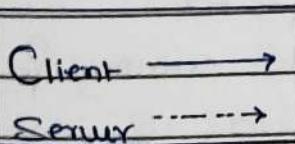
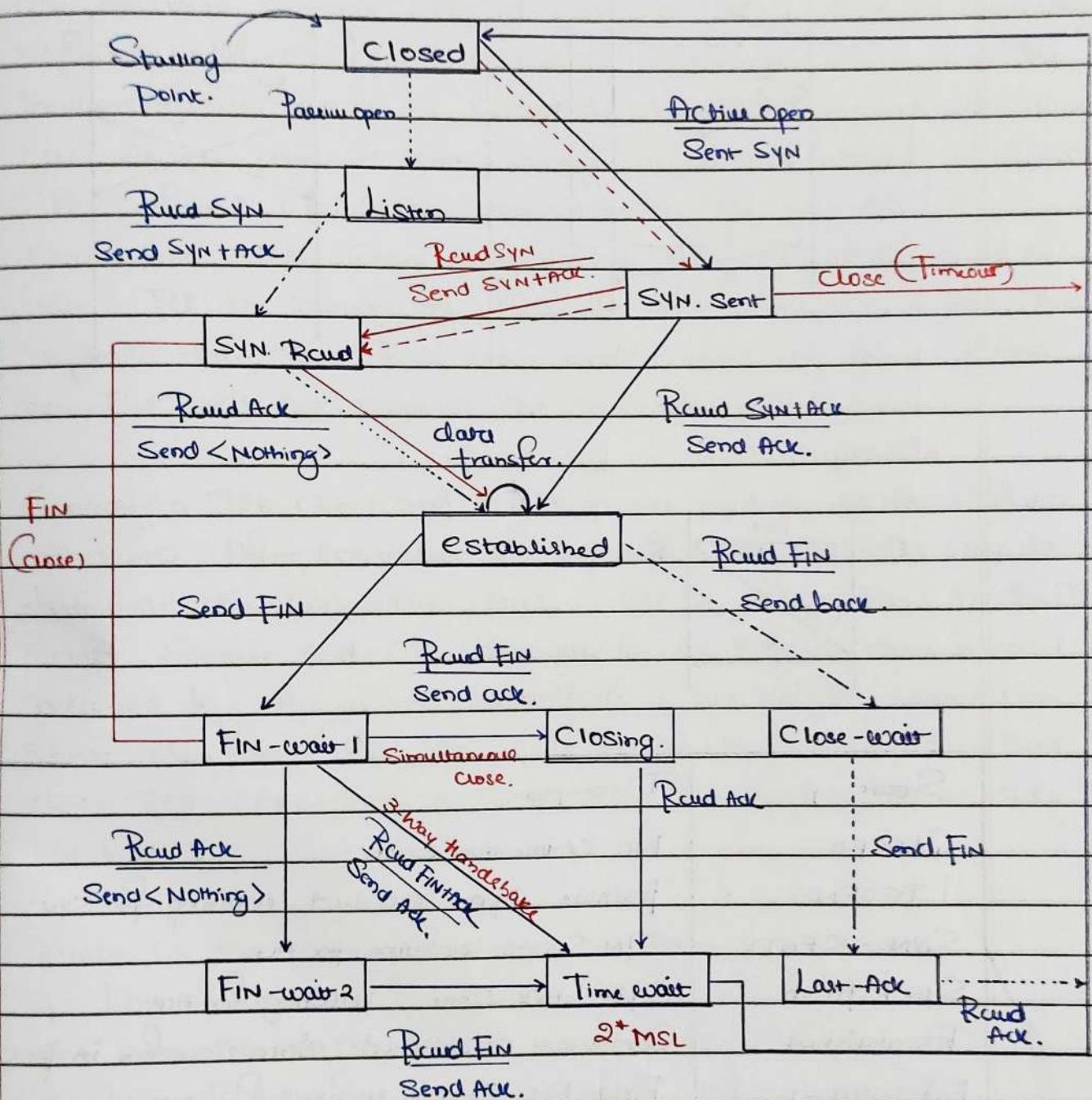
Note: FIN segment cannot carry data but it consume one sequence number.

Q1. Consider the three-way handshake mechanism followed during TCP connection establishment between hosts P and Q. Let x and y be two random 32-bit starting sequence numbers chosen by P and Q respectively. Suppose P sends a TCP connection request message request to Q with a TCP segment saying having SYN bit = 1, SEQ number = x, and ACK bit = 0. Suppose Q accepts the connection request. Which one of the following choices represents the information present in the TCP segment header that is sent by Q to P?

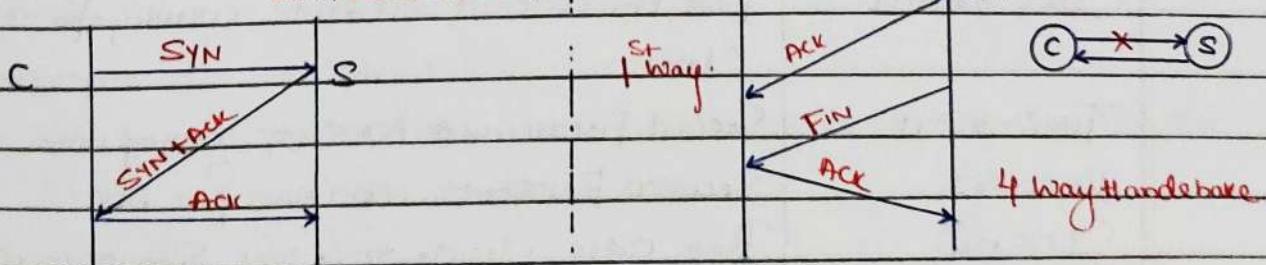
Ans.

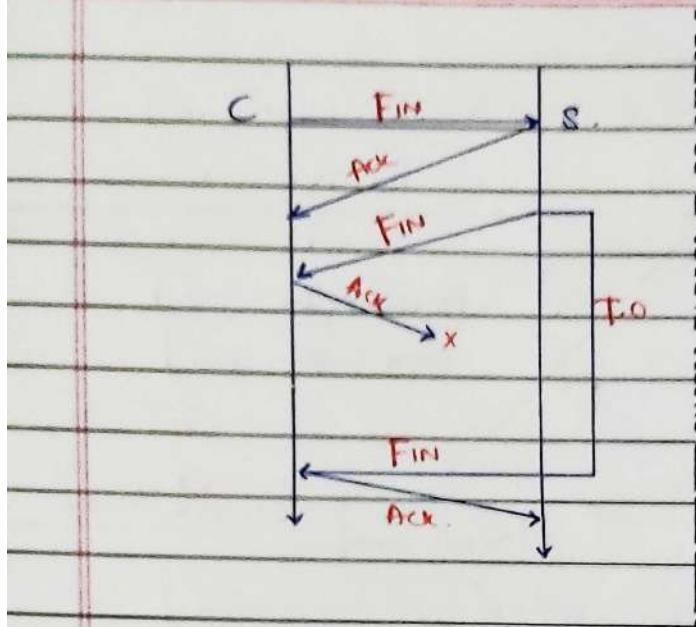
| | | | |
|--------------|---|-------------|---|
| P request | Seq.no = x, SYN = 1, ACK = 0 | Q reply. | SYN bit = 1, SEQ number = y, ACK bit = 1, ACK number = x + 1, FIN bit = 0 |
| | Seq.no = y, SYN = 1, ACK = 1 ACK NO = x + 1, FIN = 0 | | |

TCP: State Transition Diagram

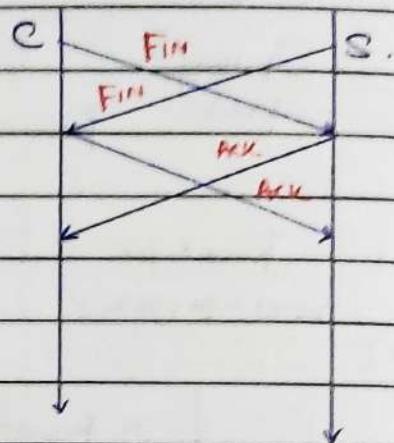


Connection termination.

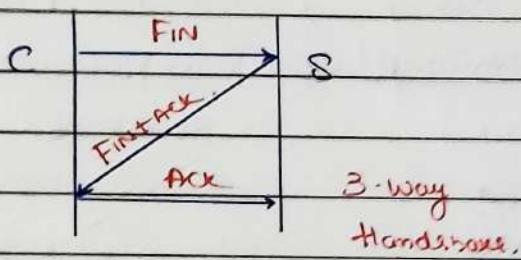




Connection termination.

2nd way

Connection termination.

3rd way

3-way Handshake.

| State | Description |
|-------------|--|
| CLOSED | No connection exists |
| LISTEN | Passive open received; waiting for SYN |
| SYN-SENT | SYN Sent; waiting for ACK |
| SYN-RCVD | SYN+ACK Sent; waiting for ACK |
| Established | Connection established; data transfer in progress |
| FIN-WAIT-1 | First FIN Sent; waiting for ACK |
| FIN-WAIT-2 | -ACK to first FIN received; waiting for second FIN |
| CLOSE-WAIT | First FIN received; ACK sent; waiting for application to close |
| TIME-WAIT | Second FIN received; ACK sent; waiting for time out |
| LAST ACK | Second FIN sent; waiting for ACK |
| CLOSING | Both sides decide to close simultaneously |

Time wait Timer

The time wait timer (2msl) is used during connection termination. The maximum segment life time (msl) is the amount of time any segment can exist in the network before being discarded. The implementation needs to choose a value for msl . Common values are 30 sec, 1 min or even 2 min. The 2msl -timer is used when TCP performs an active close and sends the final ACK. The connection must stay open for $2 \times \text{msl}$ amount of time to allow TCP to resend the final ACK in case of ACK is lost. This requires that the RTO timer at the other end times out and new FIN and ACK segment are resent.

- Q1. Consider a TCP client and a TCP Server running on two different machines. After completing data transfer, the TCP calls close to terminate the connection and a FIN segment is sent to the TCP Server. Server side TCP responds by sending an ACK which is received by the Client side TCP as per the TCP connection state diagram (RFC 973) [93]. In which state does the Client side TCP connection wait for the FIN from the server side TCP?
 Ans. **FIN-WAIT 2.**

- Q2. Which of the following statements are true?

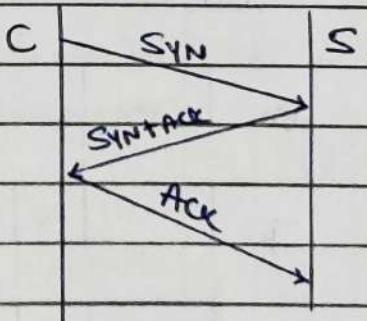
S1: Loss of SYN+ACK from Server will not establish a connection.

S2: Loss of ACK from the Client cannot establish the connection.

S3: The Server moves LISTEN \rightarrow SYN-RCVD \rightarrow SYN SENT \rightarrow Established in the State machine on no packet loss.

S4: The Server moves from LISTEN \rightarrow SYN-RCVD \rightarrow established in the State machine on no packet loss.

Ans. S1 and S4 are True



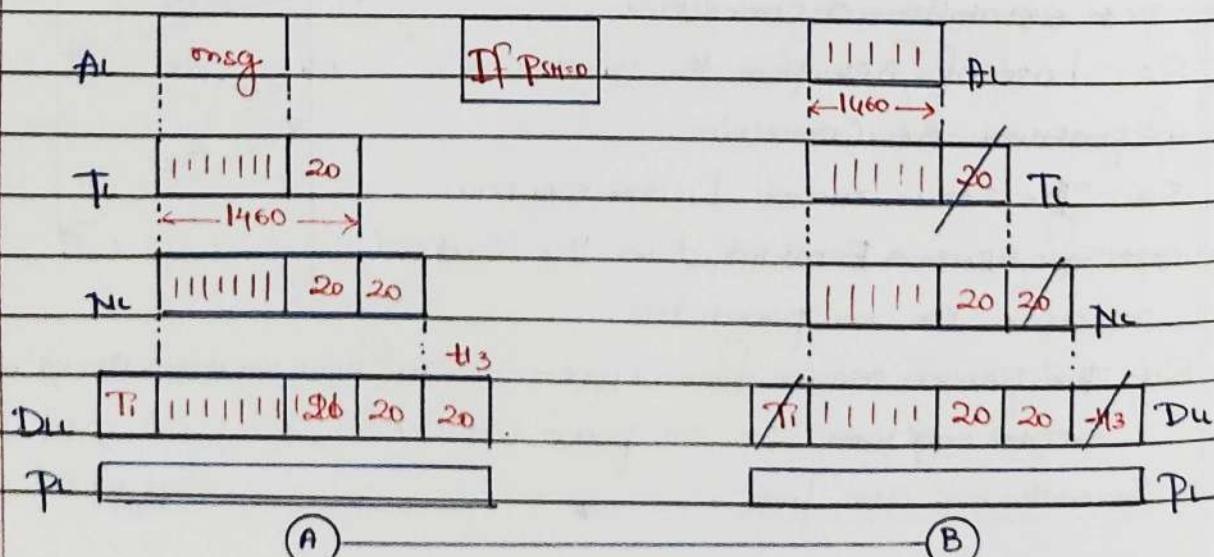
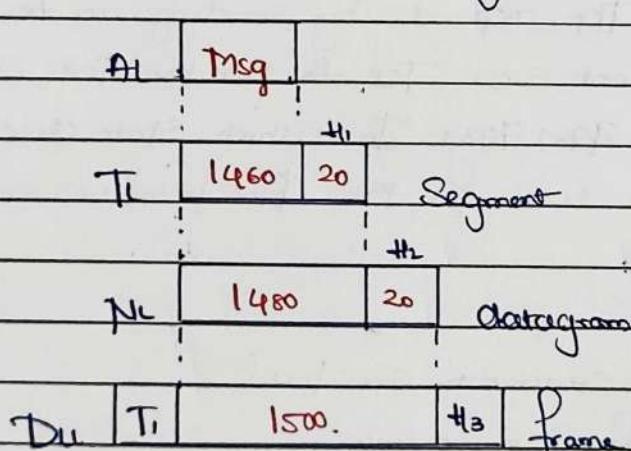
Q3. Consider a TCP server is in Close Wait State in TCP state transition diagram, which State TCP Server moves after sending FIN segment to TCP Client?

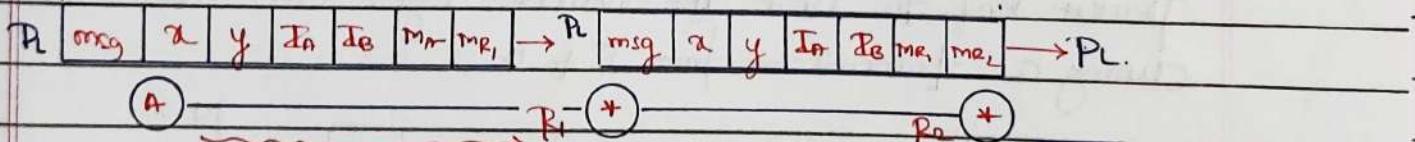
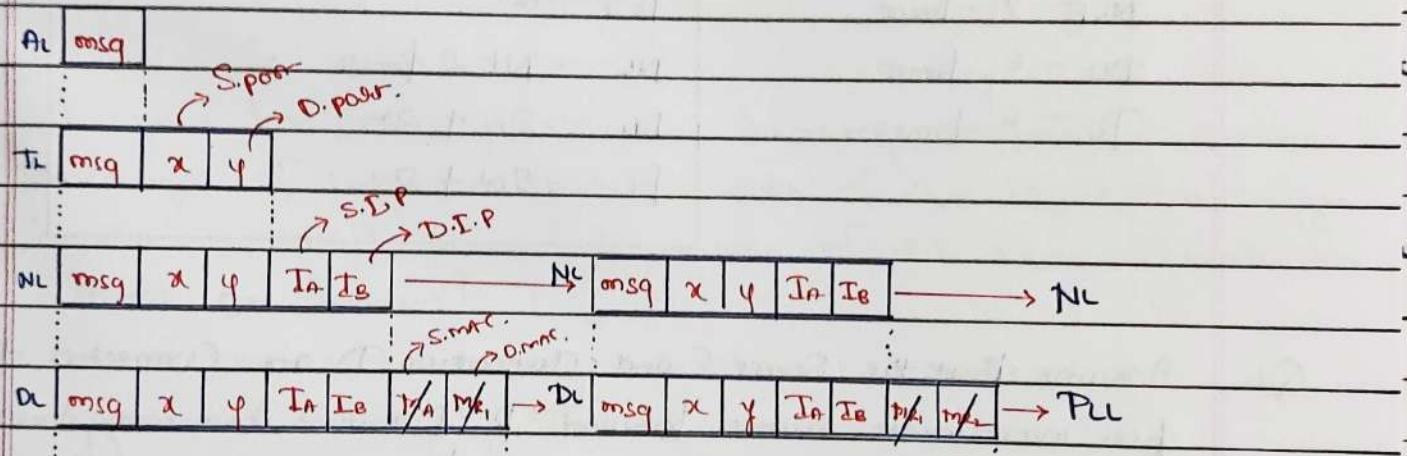
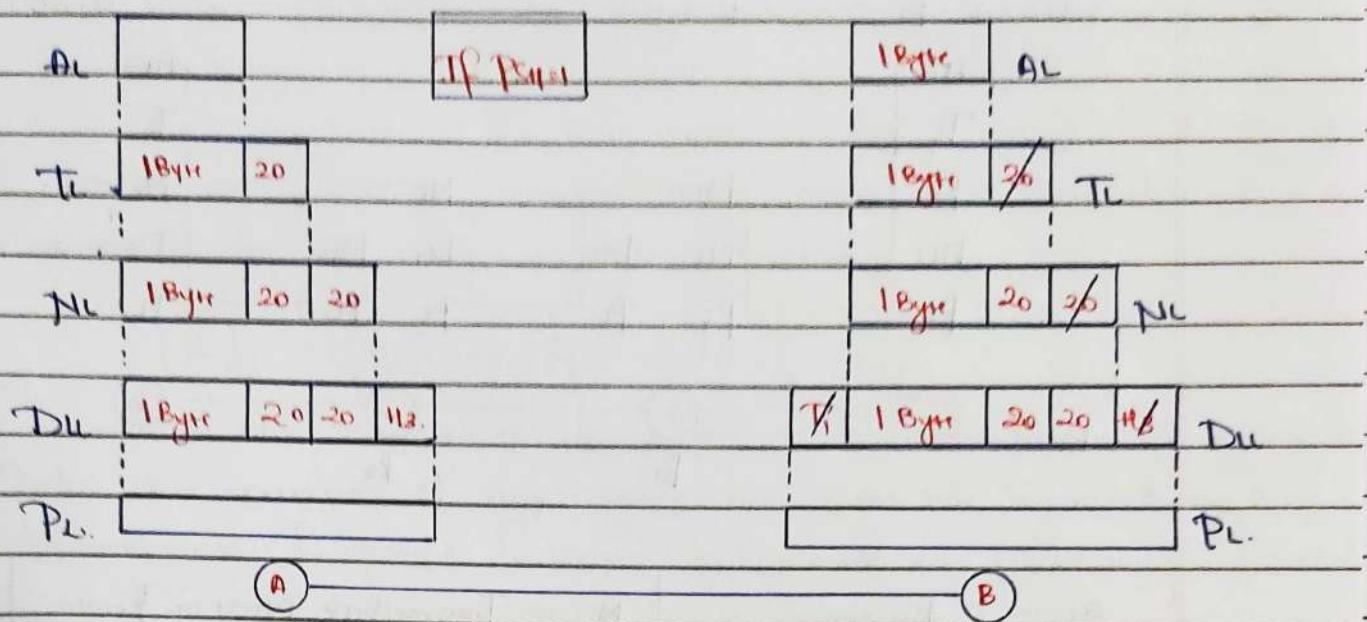
Ans. Last - Ace.

Flage.

- | | | | |
|----|-----|---|--|
| 1. | SYN | } | Connection establishment phase |
| 2. | ACK | | |
| 3. | FIN | } | Connection termination phase |
| 4. | URG | | |
| 5. | PSH | | PUSH flag: Pushes data as soon as it arrives |
| 6. | RST | | |

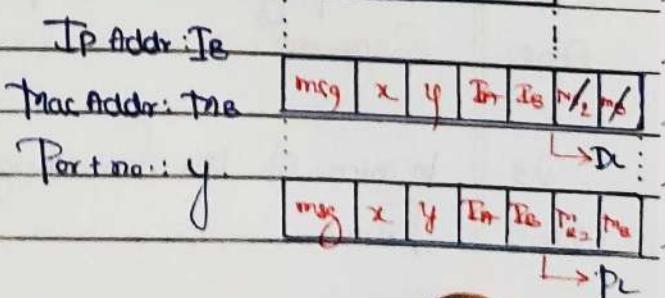
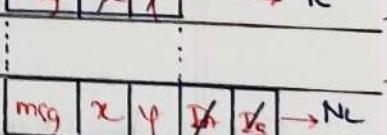
Preb Frag: Preb Frag (PSH) is used to indicate that data should not be buffered it must be pushed immediately to the lower layer or upper layer.

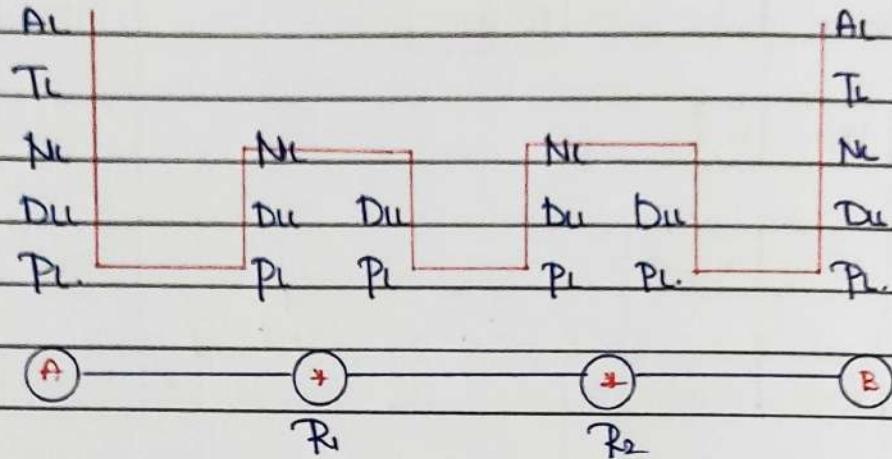




Below the diagram, the following information is provided:

- IP Addr: D₁** **ARP request** **IP Addr: T₁**
- Mac addr: T₁** **mac addr: T₁R₁** **Mac Add: M₁**
- Port no: x**
- IP Addr: D₂** **IP Addr: T₂**
- Mac addr: T₂** **Mac Add: M₂**
- Port no: y**

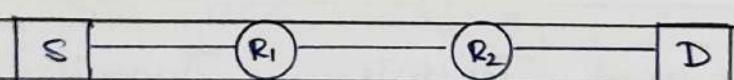




AL - 2 times
 TL - 2 times
 NL - 4 times
 DL - 6 times
 PL - 6 times

| |
|---|
| $N \rightarrow$ Intermediate Node or Router |
| $AL \rightarrow 2x$ |
| $TL \rightarrow 2x$ |
| $NL \rightarrow N + 2 \text{ times}$ |
| $DL \rightarrow 2N + 2x$ |
| $PL \rightarrow 2N + 2x$ |

Q1. Assume that the Source S and destination D are connected through two intermediate routers labelled R. Determine how many times each packet has to visit the network layer and data link layer during a transmission from S to D.



$N=2$

Ans. $N_L = N+2 \text{ times} = 2+2=4 \text{ times}$

$D_L = 2N+2 \text{ times} = 2*2+2=6 \text{ times}$

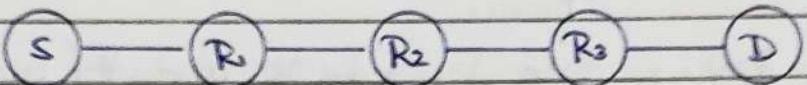
Q2. The payload in Te packet
Ans. Segment.

Q3. Which of the following Options encapsulate packet?
Ans. Frame.

Q4. Which layer is responsible for Segmentation and reassembly?

Ans. Transport Layer.

Q5. Consider the following Scenario where Source and Destination are connected via three intermediate Router.



Let P be the number of times the packet visit Network Layer and Q be the number of times packet visit Data Link Layer during a transmission of packet from source to destination. The value of P+Q?

Ans. $N = 3$. N - Intermediate Node or Router

$$N_1 + N_2 = 3 + 2 = 5 \text{ (P)}$$

$$D_L + S_{NN} = 6 + 2 = 8 \text{ (Q)} \quad \therefore P+Q = 13.$$

Q6. A system has 'n' layers protocol hierarchy. Applications generate messages of length m bytes. At each of the layers, an 'h' byte header is added. What is the fraction of the network bandwidth wasted on headers?

Ans. No of layers = n, msg size = m bytes

Header size = h bytes. Total header size = nh

Packet size = msg + header = m + nh

$$\% \text{ overhead} = \frac{nh}{m+nh}$$

URG: Urgent Flag: It is used to indicate that some bytes are urgent in the data.

Note: Sender Create a Segment and insert the urgent data at the beginning of the Segment.

Urgent Pointer: (16 bit)

- Urgent Pointer indicate end of the urgent data i.e. last urgent byte.
- If URG Flag = 0, then we have no need to read the urgent pointer.
- If URG Flag = 1, then we have to read the urgent pointer.
- It is valid only if the urgent flag is set. It is used whenever the segment contains urgent data. It defines a value that must be added to the sequence number to obtain the number of the last urgent byte in the data section of the segment.

URG Flag = 1

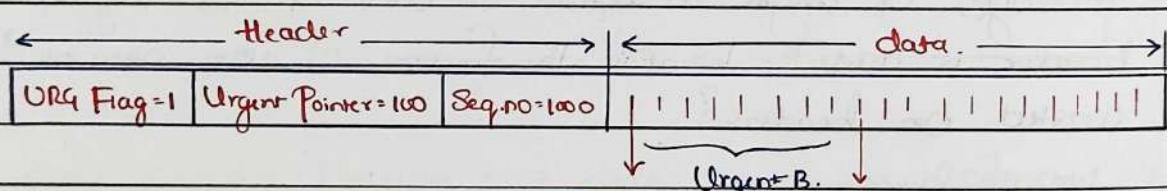
Urgent pointer = 100

Sequence no = 1000.

Last Urgent byte Seq.no. = $1000 + 100 = 1100$

Urgent bytes = $1000 - 1100$

101 Byte.



Note:

If urgent pointer = x
then no. of urgent bytes = $x+1$.

First Urgent Byte
↓
Seq.no = 1000.

last urgent Byte
↓
Seq.no = 1100.

Q. If sum of TCP segment is 1KB and header length value is 6, then Sequence no = 3500, given that URG flag = 1 and Urgent Pointer = 45, then what is the total size of the data, how many bytes are urgent, Sequence no of urgent bytes respectively.

Ans

Segment size = 1KB = 1024 Bytes

TLEN = 6

Header size = $6 \times 4 = 24$ Bytes.

Data size = $1024 - 24 = 1000$ Bytes

Seq.no = 3500

URG flag = 1

Urgent Pointer = 45

No. of Urgent byte = $45 + 1 = 46$

Last urgent byte sequence no.

$$= 3500 + 45 = 3545$$

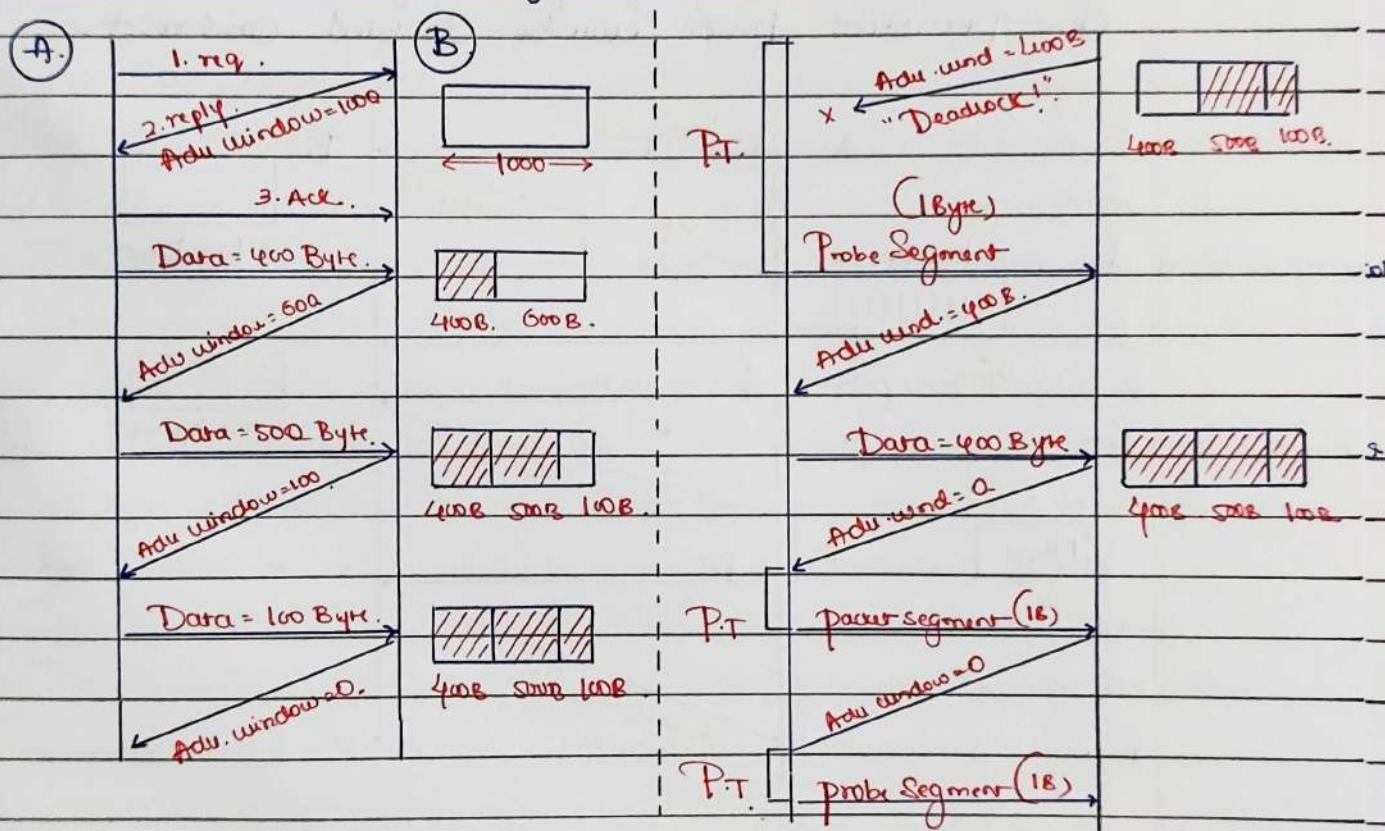
Urgent Byte = $3500 - 3545$

\downarrow
46 urgent bytes

∴ 1000 Byte, 46 Byte, Sequence no = 3500-3545.

Flow Control In TCP

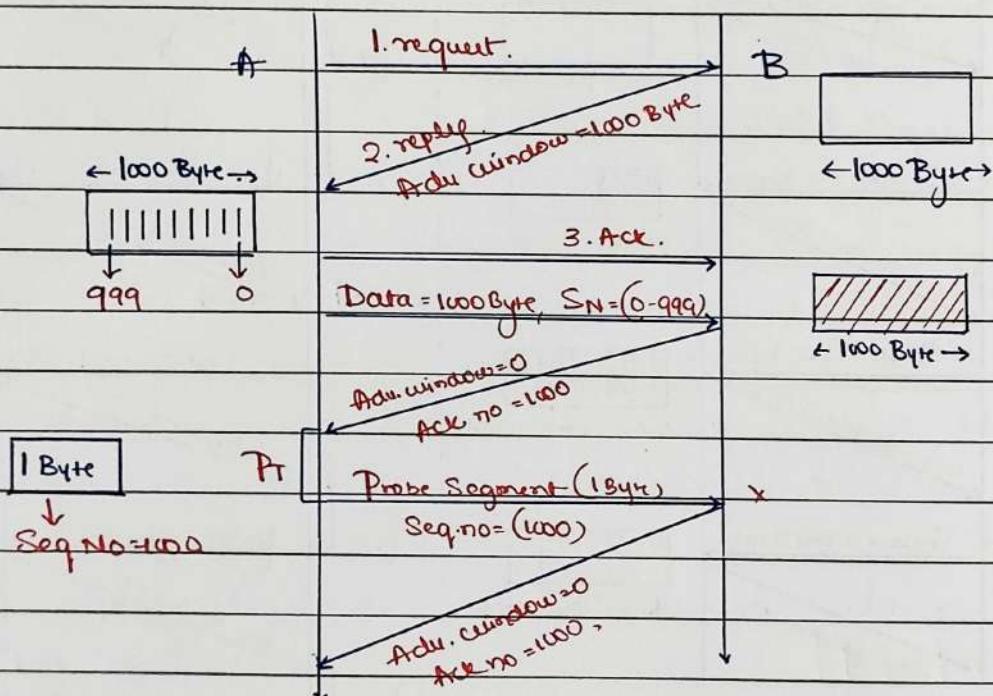
Window size or Advertising window (16 bits) [used for flow control]



Persistent Timer

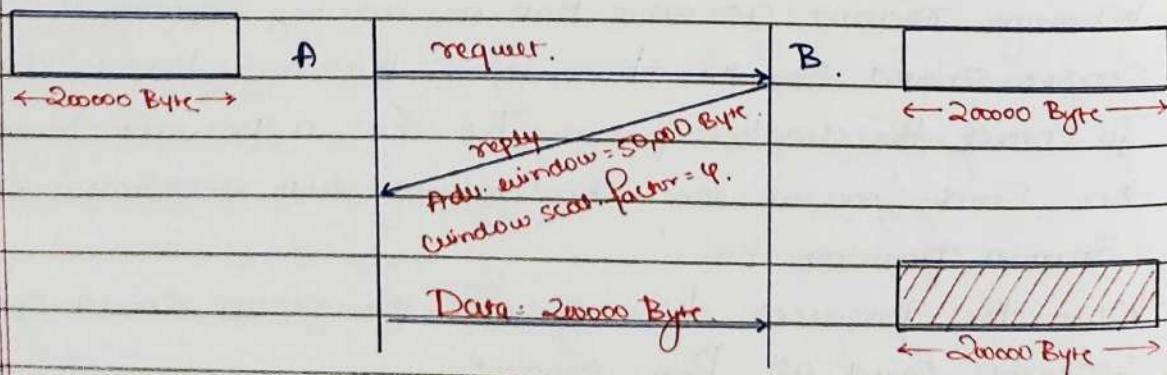
- * Whenever Receiver announces that my receiving capacity is zero then Sender should Stop the transmission this might lead to deadlock.
- * To correct the deadlock problem TCP uses a persistent timer. When then Sender receives an acknowledgement with a window size zero, it Starts a Persistent timer.
- * When the persistent timer goes off, the Sender sends a special Segment called as Probe Segment.

- * This segment contains only one byte of data. It has a sequence number, but its sequence number is never acknowledged.
- * It is even ignored in calculating the sequence number for the rest of the data.
- * Probe segment covers the retransmitting PNP that ACK was lost and should be resent.
- * The value of the Persistent timer is set to the value of retransmission timer. However if a response is not received from the receiver, another probe segment is sent and the value of persistent timer will be doubled and reset.



Window Size = 16 bit.

$$\text{Maximum no.} = 2^{16} - 1 = 65,535$$



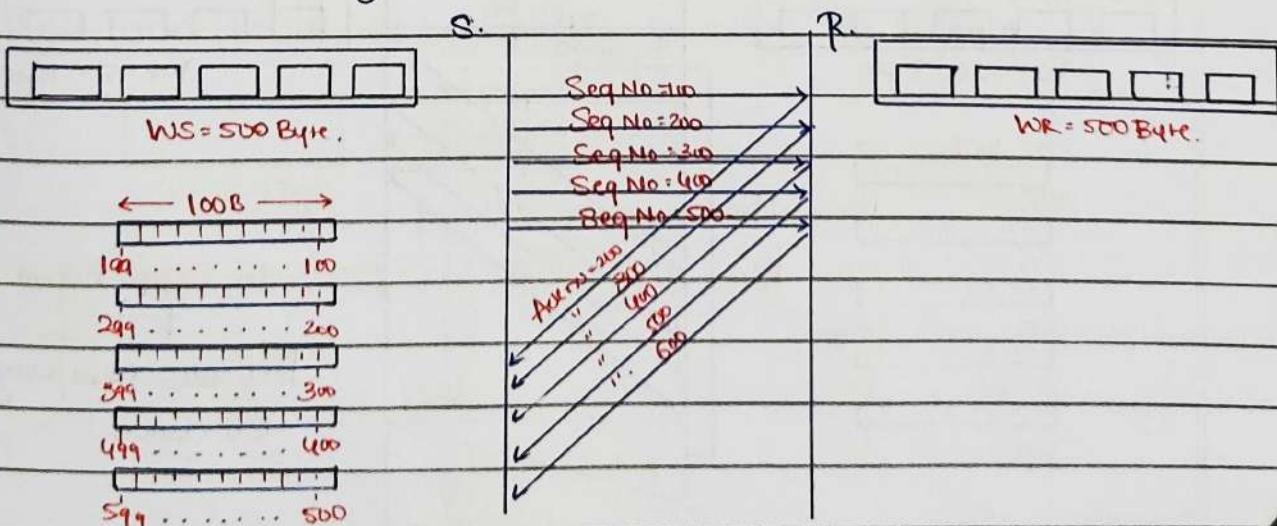
Note: According to RFC-1312 the maximum window size by using the window scale option = 2^{30} Byte = 1 GB.

$$= \underset{\text{Window Size.}}{2^{16}} \times \underset{\text{Window Scaling Factor (Options)}}{2^{14}} = 2^{30}.$$

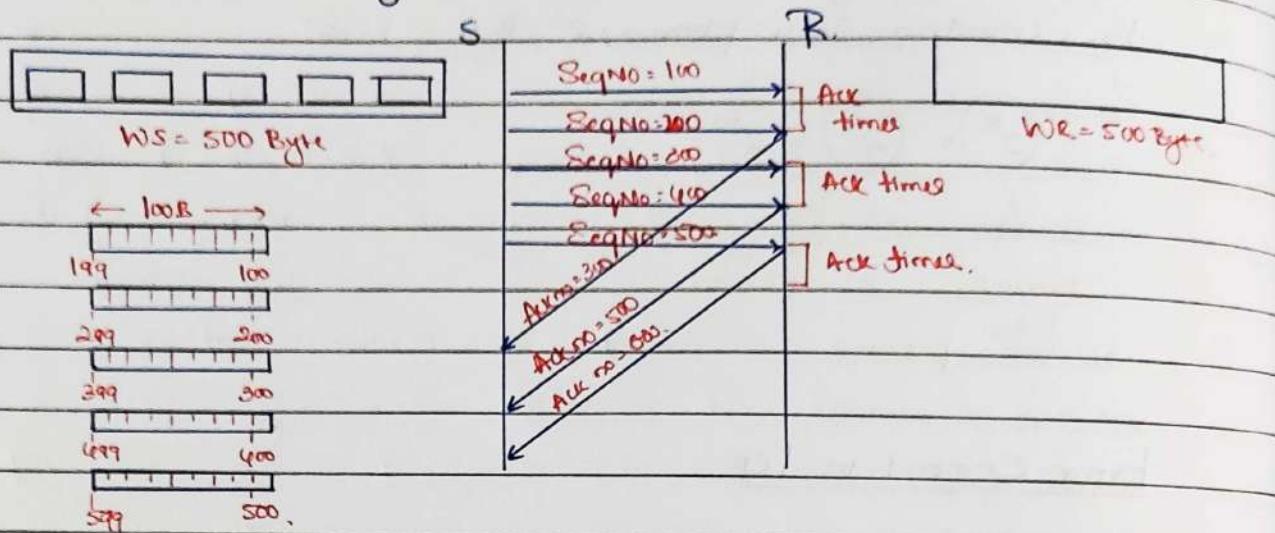
Error Control in Tcp:

- * TCP can use both Selective and Cumulative acknowledgement.
- * Receiver may choose to send independent ACK or Cumulative ACK.
- * TCP uses a combination of Selective repeat and Go-back-N protocol for error control and flow control.
- * In TCP Sender window size = receiver window size.
- * In TCP Out of order packets are accepted by the receiver. Whenever receiver receives out of order packet, it accepts that packet but send an acknowledgement for the expected packet.
- * Out of order segments are never delivered to the process.
- * TCP guarantees that data are delivered to process in order.

Selective Acknowledgement / Independent ACK



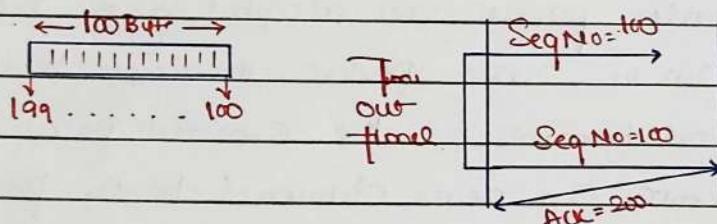
Cumulative Acknowledgement.



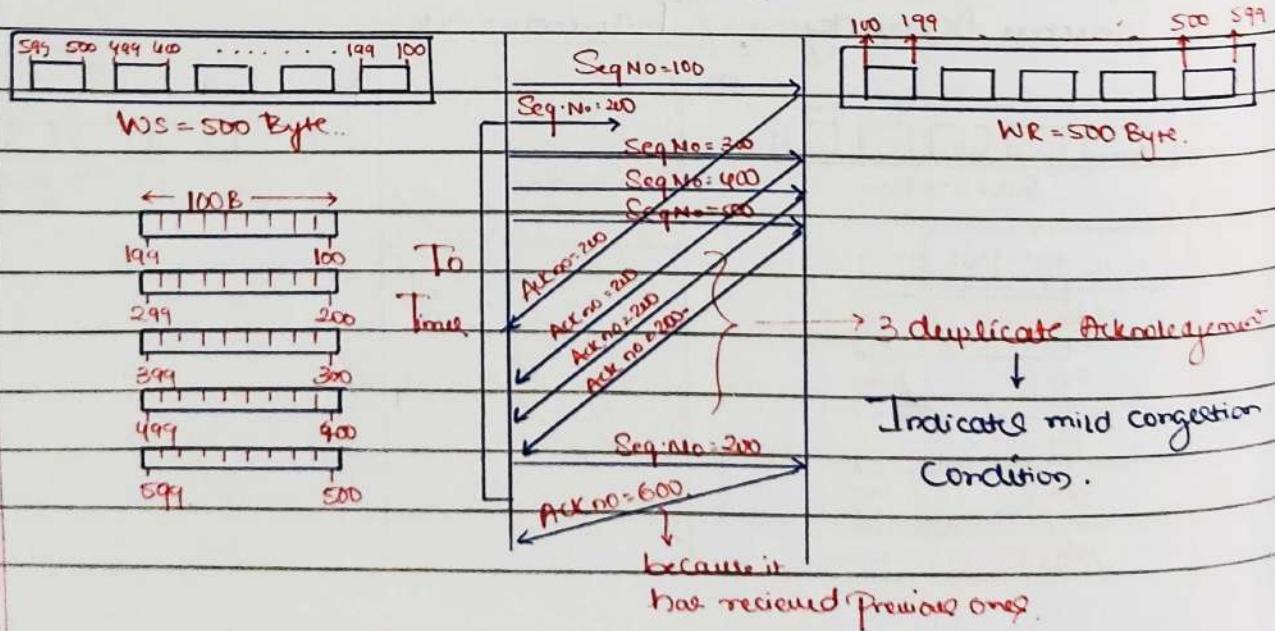
Retransmission in TCP

- (i) Retransmission after timeout timed
- (ii) Retransmission after 3-duplicate acknowledgement

Retransmission After T₀ timed

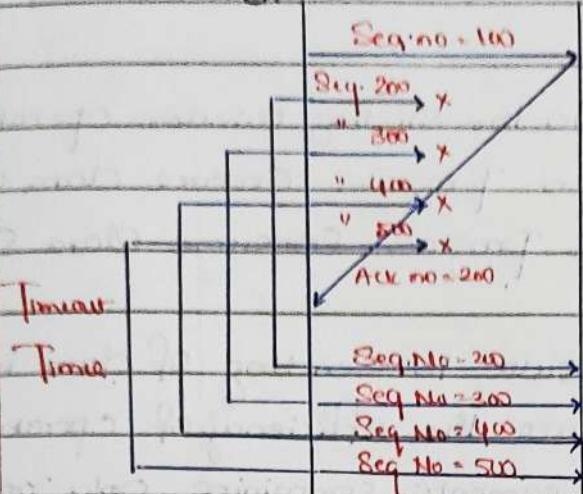


Retransmission after 3-duplicate acknowledgement [Fast Retransmission]



S.

R.

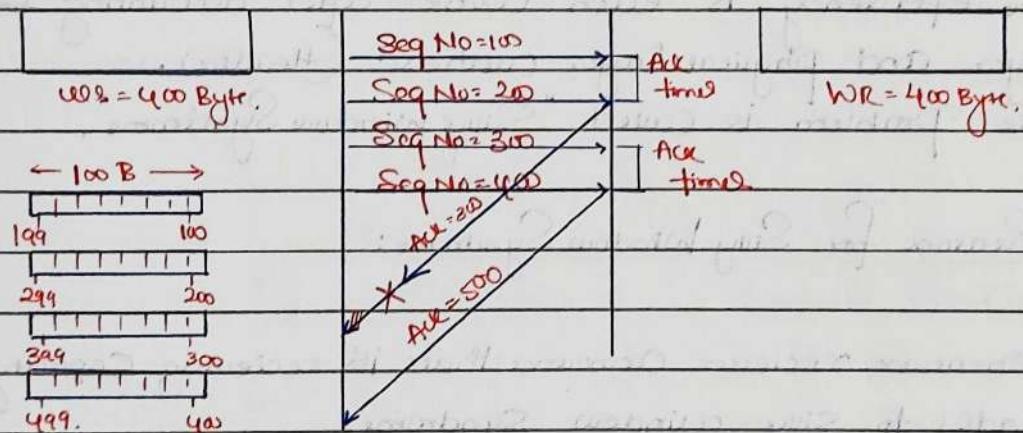
Note:

- If 3 duplicate acknowledgement not possible then we use timeout timer concept for retransmitting the lost packet.
- Timeout timer indicates Severe Congestion Condition.

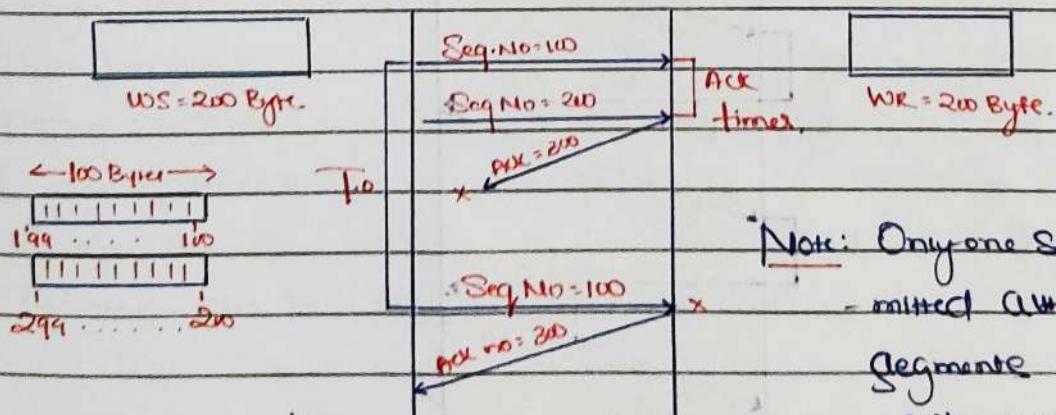
Lost acknowledgement: 1. Automatically Corrected lost ack

2. Lost ack. corrected by resending segment.

① Automatically Corrected lost ack.



② Lost acknowledgement: Corrected by resending the Segment.



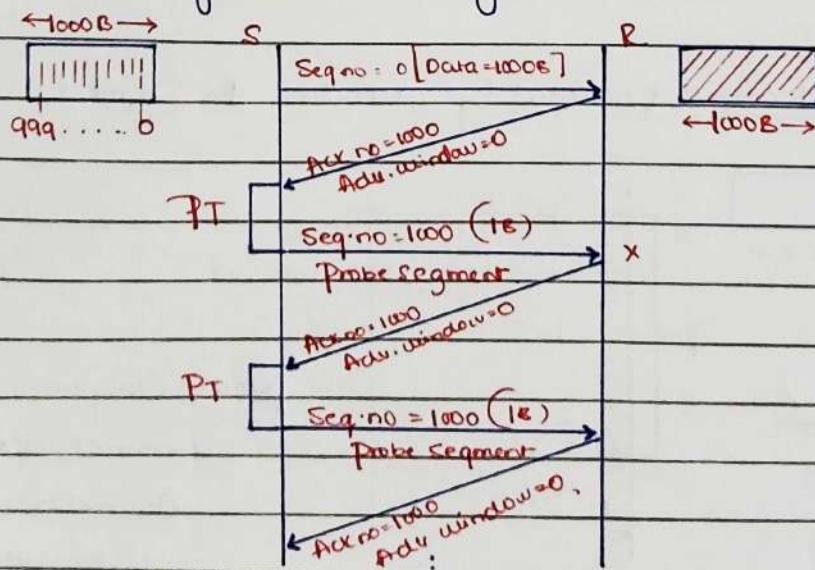
Note: Only one segment is retransmitted although two segments are not acknowledged.

Silly Window Syndrome:

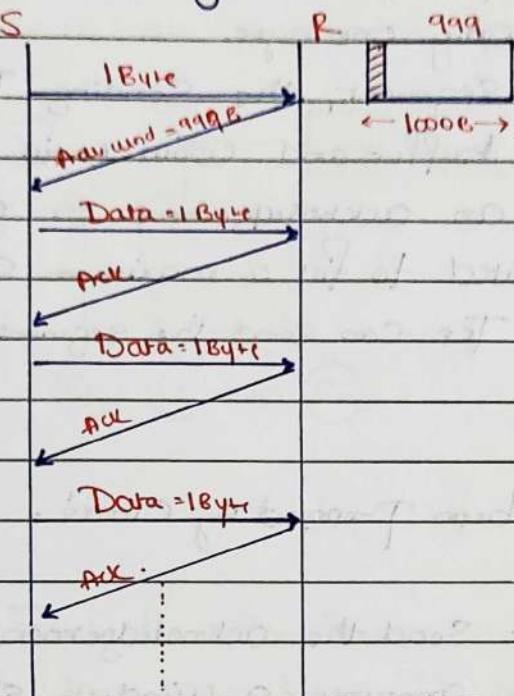
- * A Serious Problem can arise in the Sliding window Operation when either the Sending Application Program Create Data slowly or the receiving Application Program Consume Data slowly or both.
- * Any of these situations results in sending of data in very small segments, which reduce the efficiency of operation.
- * For example if TCP send Segments containing Only one byte of data, it means a 41 byte datagram (20 byte of TCP header and 20 byte of IP header) transfer only one byte of User data.
- * Here the Overhead is 41/1, which indicate that we are using the Capacity of network very inefficiently.
- * The efficiency is even worse after accounting for the Data link layer and physical layer overhead (header).
- * This Problem is called "Silly Window Syndrome".

Reasons for Silly Window Syndrome:

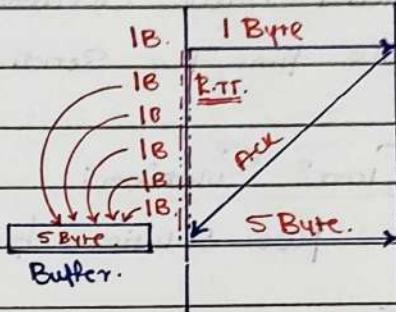
1. Whenever receiver announce that its receiving capacity is zero it leads to Silly Window Syndrome.



2 Whenever Sender produce Only One byte at a time it leads to Silly window Syndrome.

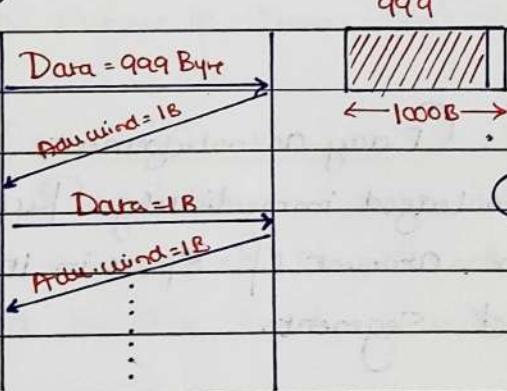


Nagle Algorithm:



If data size is $1 \text{ RTT} > \text{Tmss}$.

3 Whenever receiver consume Only one byte at a time, it leads to Silly window Syndrome.



Classic Solution:

$\frac{1}{2}$ Buffer empty.
Or
1 MSS

eg.: 1 Byte/sec

RTT = 100 sec

MSS = 200 Byte

In one RTT = 100 Byte

So we transfer 100 Byte.

→ If data size in $1 \text{ RTT} < \text{MSS}$.

1 Byte/sec

RTT = 100 sec

MSS = 50 Byte

In one RTT = 100 Byte

So we transfer 50 Byte

→ data size in one RTT $>$ MSS

Nagle's Algorithm:

1. The sending TCP send first piece of data it receive from application program even if it is only one byte.
2. After sending the first segment, the sending TCP accumulates data in the output buffer and wait until either the receiving TCP sends an acknowledgement or until enough data have accumulated to fill a maximum size segments. At this time the sending TCP can send the segment.

Clark Solution:

- Two solutions has been proposed by Clark.

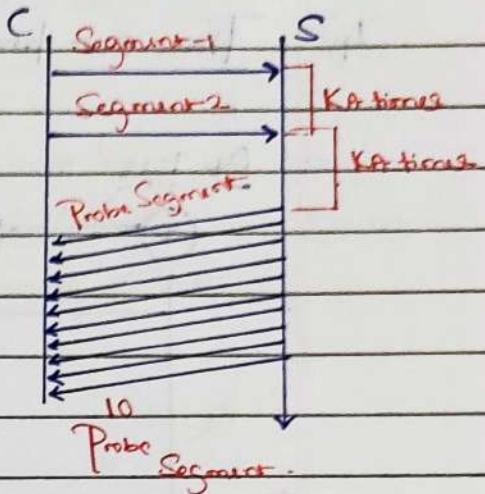
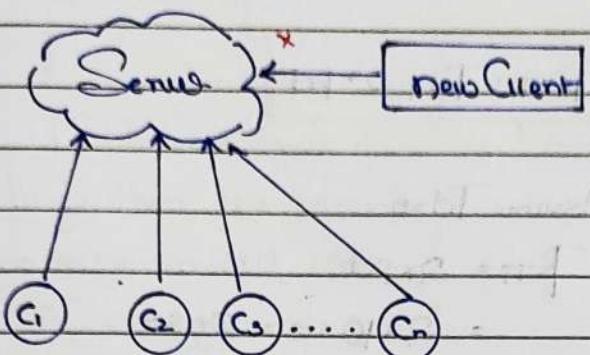
First Solution: Receiver send the acknowledgement as soon as the data arrive, but to announce a window size of zero until either there is enough space to accomodate a segment of maximum size or until atleast half of the receiver buffer is empty.

Second Solution: (Delay acknowledgement) When a segment arrives, it is not acknowledged immediately. Receiver wait until there is a certain amount of space in its buffer before acknowledging the arrived segment.

TCP Timer Management

1. keep alive timer
2. Persistent timer
3. acknowledgement timer
4. Time wait timer
5. Time out timer

1. Keep alive time: It is used to keep track of idle connections. Server will close the connection if client does not send any data for a fixed amount of time.



Note:

Each time the Server receives the packet from a Client, it reset the keep alive time. If the Server does not receive packet from the Client and keep alive time expired, it send a probe segment. If there is no response from it after 10 probe, it assume that the Client is down and terminate the connection.

2. Acknowledgement Time: Whenever receiver receives a segment, it will start a timer called 'Acknowledgement timer'. Whenever ACK times goes off, the receiver send one acknowledgement for all the segments received in this time, also known as 'Cumulative acknowledgement'.

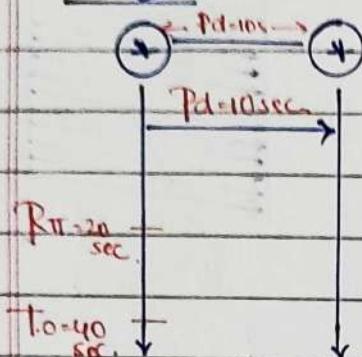
3. Time Wait Timer: The time wait time (2msl) is used during connection termination. The maximum segment life time is the amount of time any segment can exist in the network before being discarded. The implementation needs to choose a value for msL. Common values are 30sec, 1min or even 2min. The 2msl timer is used when TCP performs an active close and sends the final ACK. The connection must stay open for 2msl amount of time to allow TCP to send the final ACK in case of ACK.

is lost. This requires that the RTT timer at the other end times out and new FIN and ACK segment are resent.

4. Time out timer:

$$RTT = Td + 2 \times Pd$$

At DL



Assume $Td = 0$

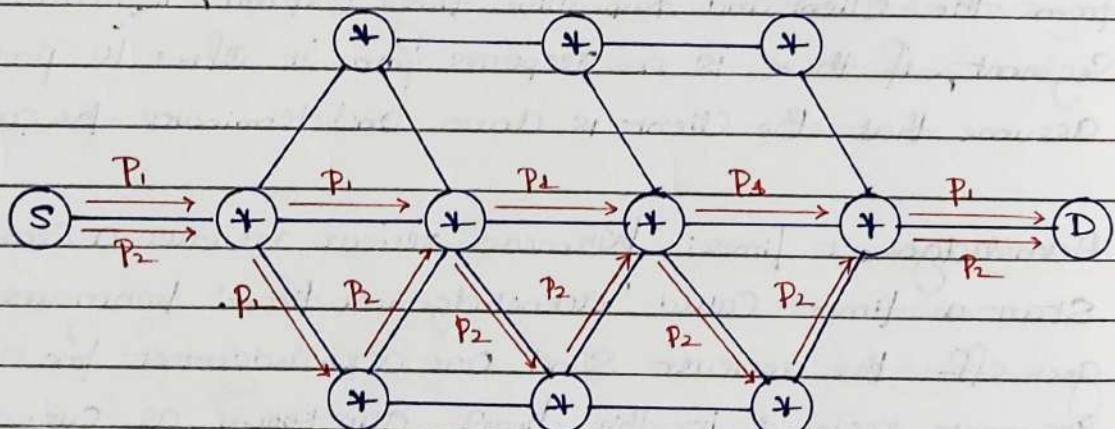
$$\rightarrow RTT = 2 \times Pd$$

$$= 2 \times 10\text{ sec} = 20\text{ sec}$$

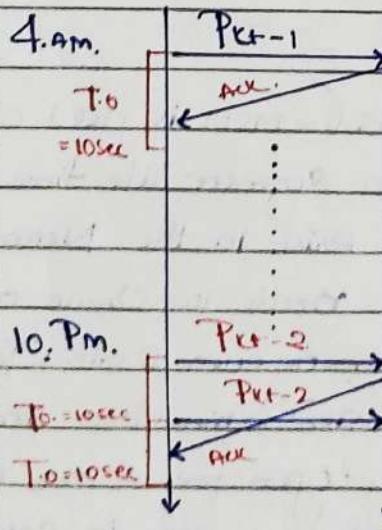
$$\rightarrow Td = 2 \times RTT$$

$$= 2 \times 20 = 40\text{ sec.}$$

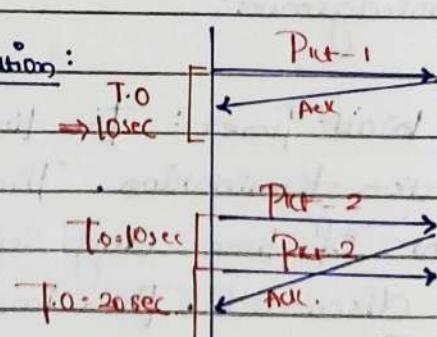
Timeout timer of Transport Layer.



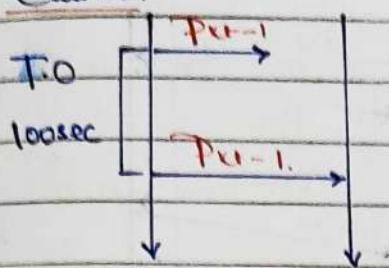
e.g.:



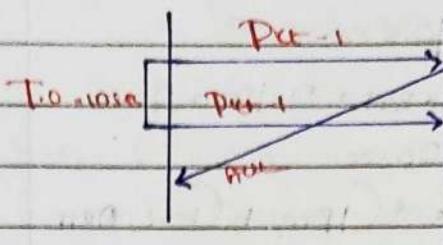
Solution:



\rightarrow Solⁿ: If traffic increases then increase the timeout times.

Case I.

Note: If timeout-time is very large then lost-packets will be retransmitted later.
eg: After 100 sec.

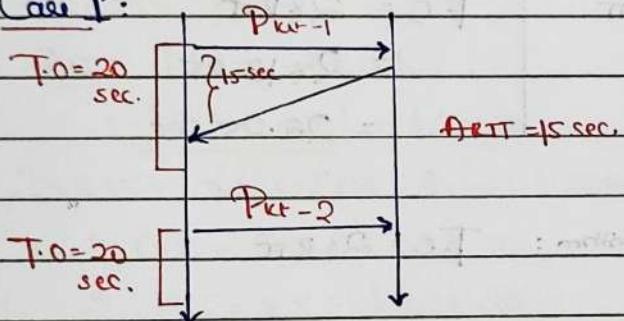
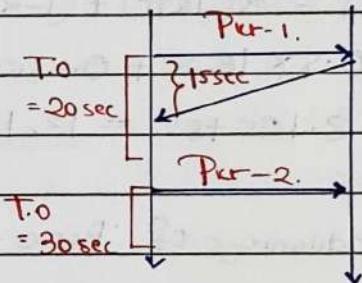
Case II.

Note: If timeout-time is very small then unnecessarily packets will be retransmitted.

$$\rightarrow 1. RTT = 10 \text{ sec} \quad (\text{Assumption})$$

$$T.O. = 2 * RTT$$

$$T.O. = 2 * 10 \text{ sec} = 20 \text{ sec}$$

Case I:Case II:

Note: The value of timeout timer should be such that
 (i) It decreases when there is a low traffic in the network
 (ii) It increases when there is a high traffic in the network.

Basic Algorithm.

$$NRTT = 2(GRTT) + (1-\alpha)ARTT$$

$$0 \leq \alpha \leq 1, \quad \alpha = \frac{1}{2} = 0.5$$

Packet-1.

$$1 RTT = 10 \text{ sec}$$

$$T.O. = 2 \cdot RTT = 2 \times 10 = 20 \text{ sec}$$

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

$$\begin{aligned} NRTT &= 2(GRTT) + (1-\alpha)ARTT \\ &= 0.5 \times 10 + 0.5 \times 15 \\ &= 12.5 \text{ sec} \end{aligned}$$

Packet-2

$$T_{RTT} = 12.5 \text{ sec}$$

$$T.O = 2 \times RTT = 2 \times 12.5 = 25 \text{ sec}$$

$$ARTT = 20 \text{ sec}$$

$$\begin{aligned} NRTT &= \alpha(T_{RTT}) + (1-\alpha)ARTT \\ &= 0.5 \times 12.5 + 0.5 \times 20 \\ &= 6.25 + 10 = 16.25 \end{aligned}$$

Packet-3

$$T_{RTT} = 16.25 \text{ sec}$$

$$T.O = 2 \times RTT = 2 \times 16.25 = 32.5 \text{ sec}$$

$$ARTT = 10 \text{ sec}$$

$$\begin{aligned} NRTT &= \alpha(T_{RTT}) + (1-\alpha)ARTT \\ &= 0.5 \times 16.25 + 0.5 \times 10 \\ &= 8.125 + 5 = 13.125 \end{aligned}$$

Packet-1

$$\begin{array}{l} T.O \\ = 20 \text{ sec} \end{array}$$

15sec
ACKPacket-2

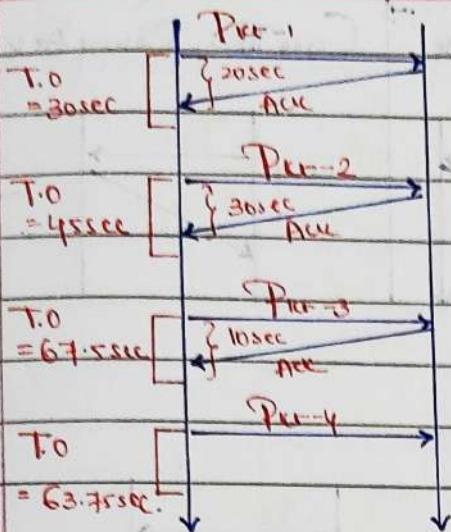
$$\begin{array}{l} T.O \\ = 25 \text{ sec} \end{array}$$

20sec
ACKPacket-3

$$\begin{array}{l} T.O \\ = 32.5 \text{ sec} \end{array}$$

10sec
ACKPacket-4

$$\begin{array}{l} T.O \\ = 26.5 \text{ sec} \end{array}$$



$$NRTT = \alpha(1RTT) + (1-\alpha)ARTT$$

$$= 0.5 \times 10 + 0.5 \times 15 + 0.5 \times 30$$

$$= 22.5 \text{ sec}$$

$$ND = 2(JD) + (1-\alpha)AD$$

$$= 0.5 \times 7.5 + 0.5 \times 15 = 11.25 \text{ sec}$$

Packet 3

JRTT =

$$JD = 11.25$$

$$T.O. = 4 \times JD + RTT$$

$$= 4 \times 11.25 + 22.5$$

$$= 45 + 22.5 = 67.5$$

$$ARTT = 10 \text{ sec.}$$

$$JD = |1RTT - ARTT|$$

$$= |22.5 - 10| = 12.5 \text{ sec.}$$

$$NRTT = \alpha(1-1RTT) + (1-\alpha)ARTT$$

$$= 0.5 \times 22.5 + 0.5 \times 10$$

$$= 11.25 + 5 = 16.25 \text{ sec}$$

$$ND = \alpha(JD) + \alpha(1-\alpha)AD$$

$$= 0.5 \times 11.25 + 0.5 \times 12.5$$

$$= 5.625 + 6.25 = 11.875$$

Packet 4

$$1RTT = 16.25$$

$$JD = 11.875$$

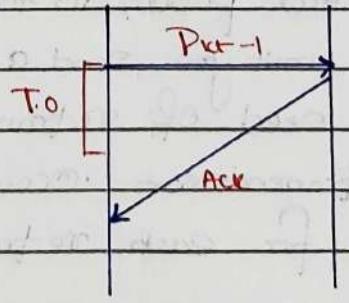
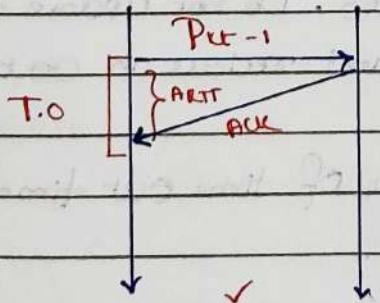
$$T.O. = 4 \times JD + RTT$$

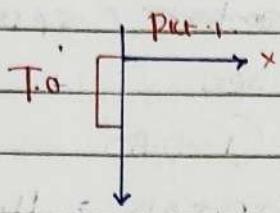
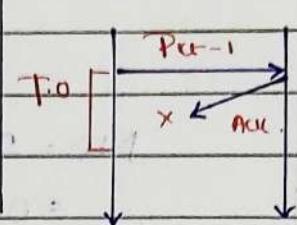
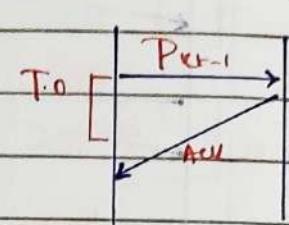
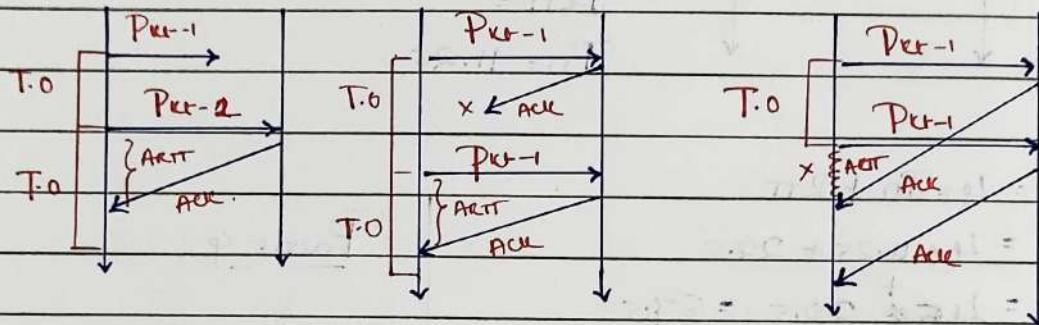
$$= 4 \times 11.875 + 16.25$$

$$= 47.5 + 16.25$$

$$T.O. = 63.75$$

Problems in Basic and Jacobson's Algorithm.



Case I : Lost data packet.Case II : Lost ACK.Case III : Delay ACK.Solutions:Note:

If there is a time out timer then there is a possibility to receive two acknowledgement.

(i) from original packet

(ii) from retransmitted packet.

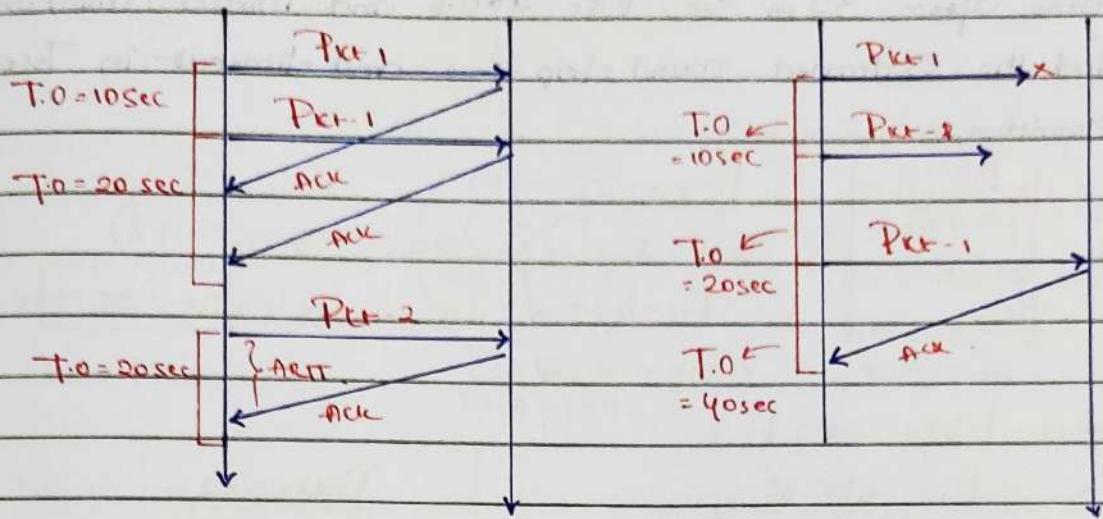
Then there is an ambiguity that which acknowledgement must be considered for next calculations and which must be the time out timer for retransmitted packet. Therefore Karn's has solved this problem by proposing the following strategy:

Karn's Modification:

Do not consider the round-trip time of a retransmitted packet in the calculation. Do not update the value of RTT until you send a segment and receive an acknowledgement without need of retransmission.

If retransmission occurs value of time out timer is doubled for each retransmission.

Case III Solution (According to Karn's Algorithm).

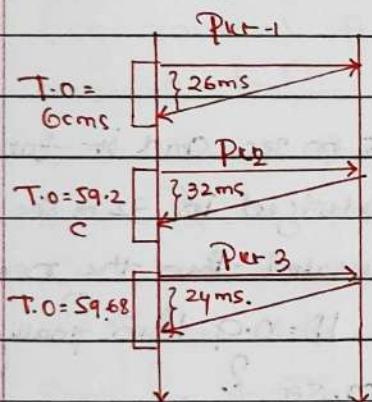


Q1. If the TCP round-trip time, RTT, is currently 30 msec and the following acknowledgement come in after 26, 32 and 24 msec, respectively, the new RTT estimate will be ____ msec.

Note: Use $\alpha = 0.9$.

Ans:

Basic Algorithm:



Packet -1

$$\begin{aligned} RTT &= 30 \text{ msec} \\ T.O. &= 2 \times RTT = 6 \text{ msec} \\ ARTT &= 26 \text{ msec} \\ NRTT &= 2(RTT) + (1-\alpha)ARTT \\ &= 0.9 \times 30 + 0.1 \times 26 \\ &= 29.6 \text{ msec} \end{aligned}$$

Packet 2

$$\begin{aligned} IRTT &= 29.6 \text{ msec} \\ T.O. &= 2 \times IRTT = 59.2 \text{ msec} \\ ARTT &= 32 \text{ msec} \\ NRTT &= \alpha(IRT) + (1-\alpha)ARTT \\ &= 0.9 \times 29.6 + 0.1 \times 32 \\ &= 26.64 + 3.2 \\ &= 29.84 \text{ msec} \end{aligned}$$

Packet 3

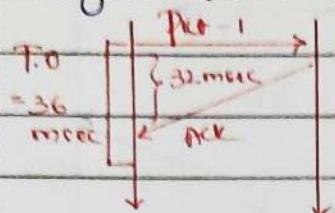
$$\begin{aligned} IRTT &= 29.84 \text{ msec} \\ T.O. &= 2 \times IRTT = 59.68 \text{ msec} \\ ARTT &= 24 \text{ msec} \\ NRTT &= \alpha(IRT) + (1-\alpha)ARTT \\ &= 0.9 \times 29.84 + 0.1 \times 24 \\ &= 26.856 + 2.4 \\ &= 29.256 \text{ msec} \end{aligned}$$

Packet 4

$$IRT = 29.256$$

Q2. In TCP, the current RTT is 20 msec and acknowledgement come after 32 msec. Use $\alpha=0.5$ and initial duration as 4. Find the estimated round-trip time and timeout in Jacobson's algorithm.

Ans.



Packet 1

$$RTT = 20 \text{ msec}, \alpha = 0.5, T_0 = 4$$

$$T.O. = 4 \times T_0 + RTT = 4 \times 4 + 20 = 36 \text{ msec}$$

$$ARTT = 32 \text{ msec.}$$

$$AD = |RTT - ARTT|$$

$$= |20 - 32| = 12$$

$$NRRT = \alpha(RTT) + (1-\alpha)ARTT$$

$$= 0.5 \times 20 + 0.5 \times 32$$

$$= 10 + 16 = 26 \text{ msec}$$

$$ND = 2(T_0) + (1-\alpha)AD$$

$$= 0.5 \times 4 + 0.5 \times 12$$

$$= 2 + 6 = 8.$$

$$\Rightarrow 26 \text{ msec, } 58 \text{ msec.}$$

Packet 2

$$RTT = 26 \text{ msec}$$

$$T_0 = 8$$

$$T.O. = 4 \times T_0 + RTT$$

$$= 4 \times 8 + 26$$

$$= 32 + 26 = 58 \text{ msec}$$

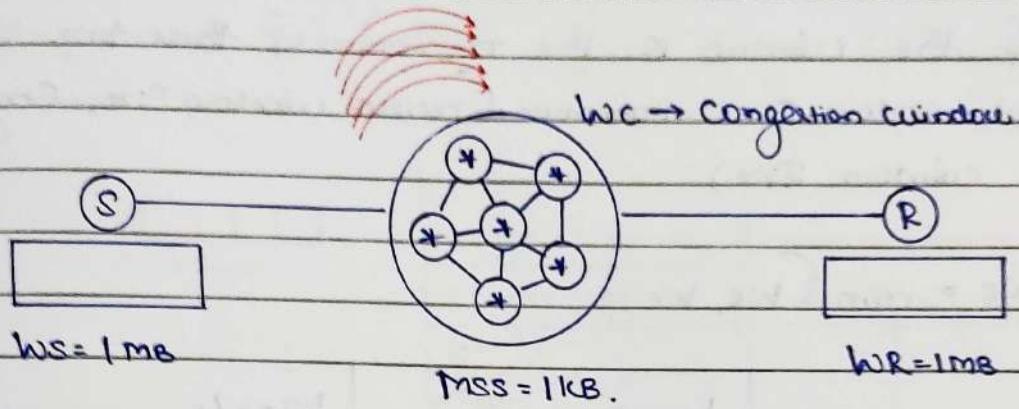
HW

Q3. The T.C.P round trip time is currently 35 msec and it takes a segment at this moment to be acknowledged in 32 msec after which the new RTT value is to be calculated then the new acknowledgement comes in after 40 msec, $T_0 = 0.9$ then finally what will be new estimated RTT in msec?

TCP Congestion Control

1980's

Jacobson.



$$\text{No. of Segments} = 1024$$

$$\text{No. of Segments} = \frac{1 \text{ ms}}{1 \text{ KB}}$$

$$WS = \min\{\text{Network Capacity}, \text{Receive Capacity}\}$$

$$= \frac{2^{20}}{2^{10}} = 2^0 \cdot = 1024.$$

$$WS = \min(WS_C, WS_R)$$

An internet is a combination of networks and connecting devices (e.g. routers). A packet from a sender may pass through several routers before reaching its final destination. A router has a buffer that stores the incoming packets, process them, and forwards them. If a router receives packets faster than it can process, congestion might occur and some packets could be dropped. When a packet does not reach the destination, no acknowledgement is sent for it. The sender has no choice but to retransmit the lost packet. This may create more congestion and more dropping of packets, which means more retransmissions and more congestion. A point may be reached in which the whole system collapses and no more data can be sent. TCP therefore needs to find some way to avoid this situation.

Congestion Window:

In TCP, the sender's window size is determined not only by the receiver but also by congestion in the network.

The Sender has two pieces of information: the receiver-advertised window size and the Congestion window size. The actual size of the window is the minimum of these two.

→ Actual window size = minimum (receiver window size, Congestion window size).

$$WS = \min(WR, WC)$$

| | | |
|----------------------|---------------------|---------------------|
| $WC = 1$ | $WC = 2$ | $WC = 4$ |
| $WS = \min(WC, WR)$ | $WS = \min(WC, WR)$ | $WS = \min(WC, WR)$ |
| $WS = \min(1, 1024)$ | $= \min(2, 1024)$ | $= \min(4, 1024)$ |
| $WS = 1$ | $= 2$ | $= 4$ |

→ $WR = 1024$ segments, $T_H = \frac{1}{2} WR = 512$ segments

→ $WC = 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 513, 514, 515, \dots, 1024, 1024, \dots$

Congestion Control Algorithm

It has 3 phases:

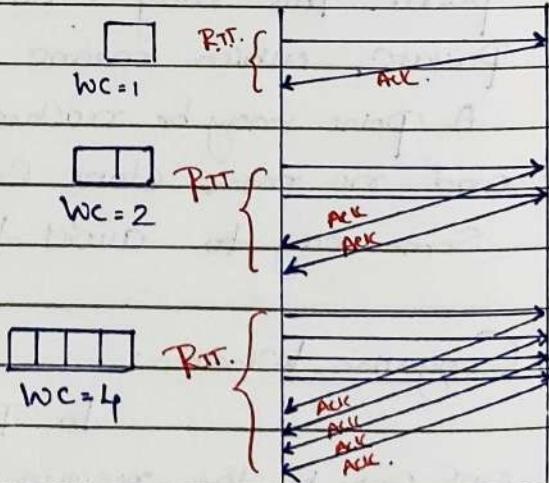
1. Slow Start Phase (exponential increase)
2. Congestion avoidance (additive increase)
3. Congestion detection (multiplicative decrease)

Slow Start Phase:

- * In the Slow Start phase, the size of the congestion window increases exponentially until it reaches a threshold.

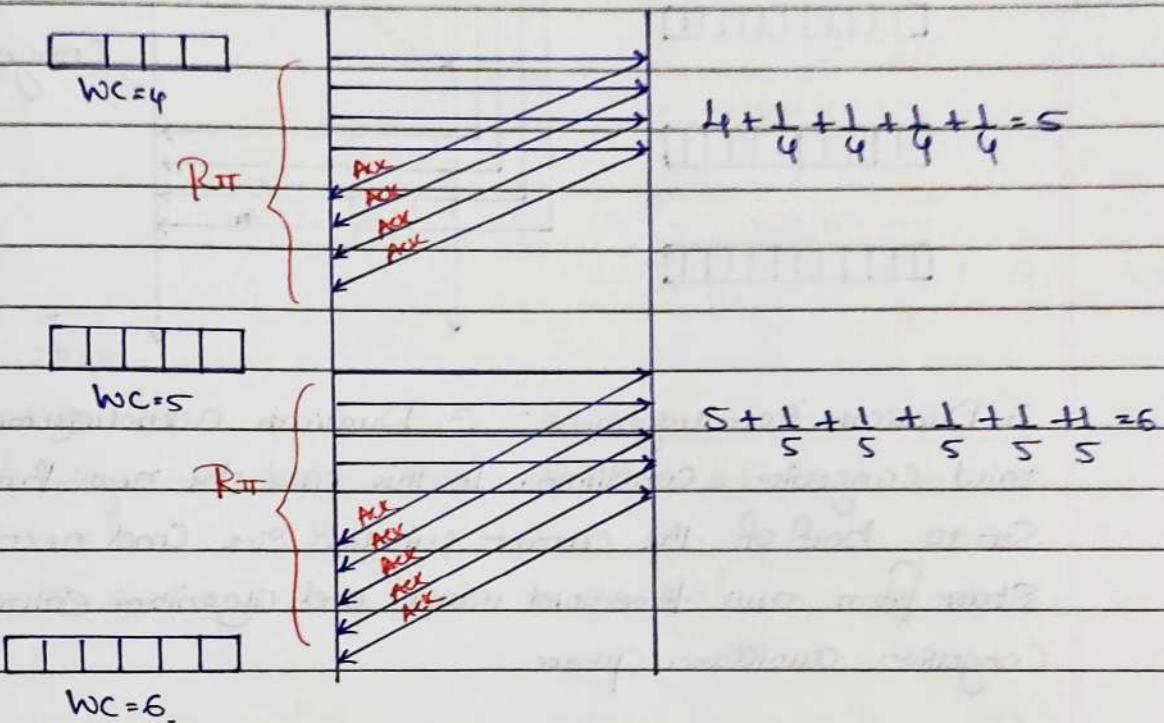
- * After one RTT, WC will double in Slow Start phase.

- * If an ACK arrives $WC \leftarrow WC + 1$.



Congestion avoidance

- * To avoid congestion before it happens we must slow down or exponential growth. In Congestion avoidance we use additive increase instead of exponential increase.



- * After one R_{tt} the Congestion window can be increased by one only
- * If one ACK arrives $WC = WC + 1$

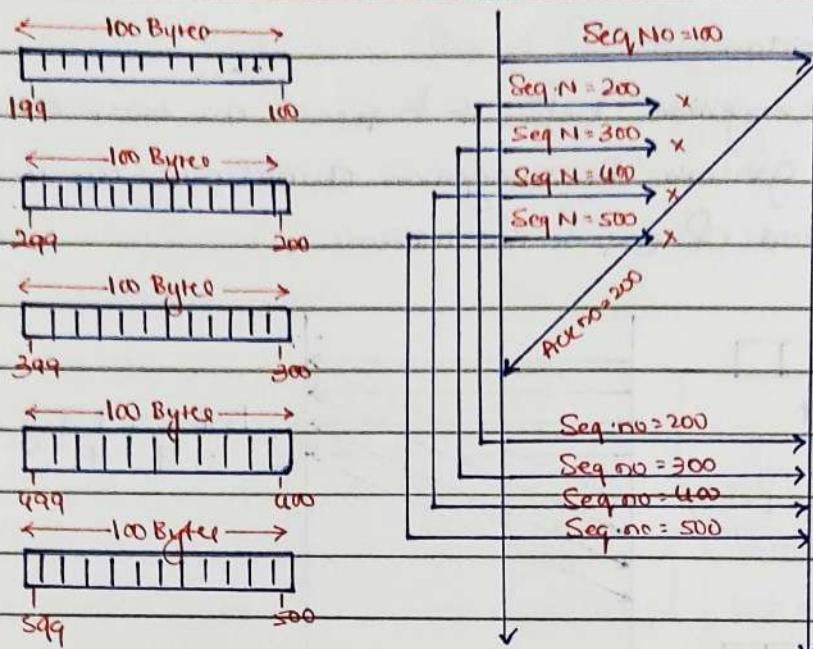
Congestion Detection:

Congestion can be detected in two ways :

1. Time out timer
2. 3 Duplicate acknowledgement

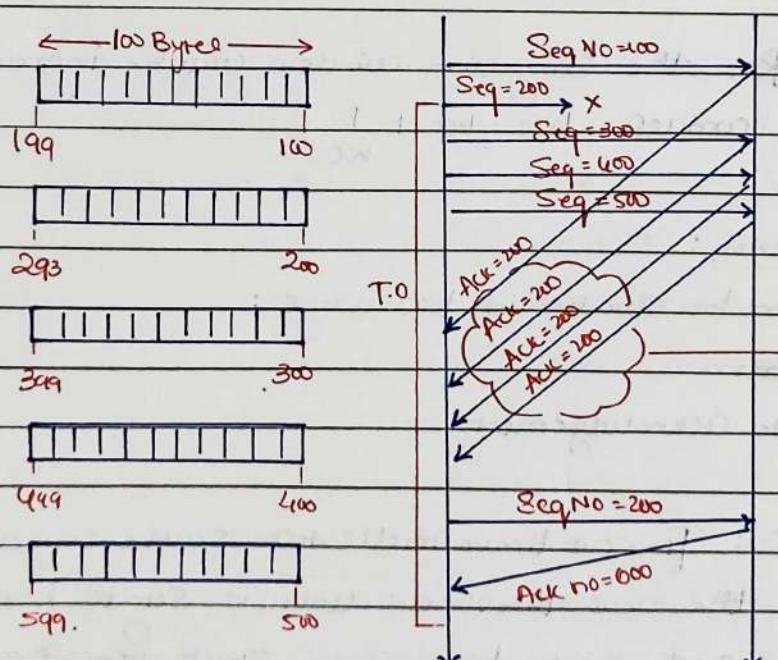
Time-out timer : Time out timer indicates severe congestion condition.

In this case the new threshold value is set to half of current window size and next transmission starts from one segment and algorithm enters in a slow start phase.



* Timeout timer indicate Severe Congestion Condition.

3 Duplicate Acknowledgement: 3 Duplicate Acknowledgement indicate mild Congestion condition. In this case the new threshold value is set to half of the current window size and next transmission starts from new threshold value and algorithm enters into a Congestion avoidance Phase.



→ 3 duplicate ACK indicating mild Congestion Condition.

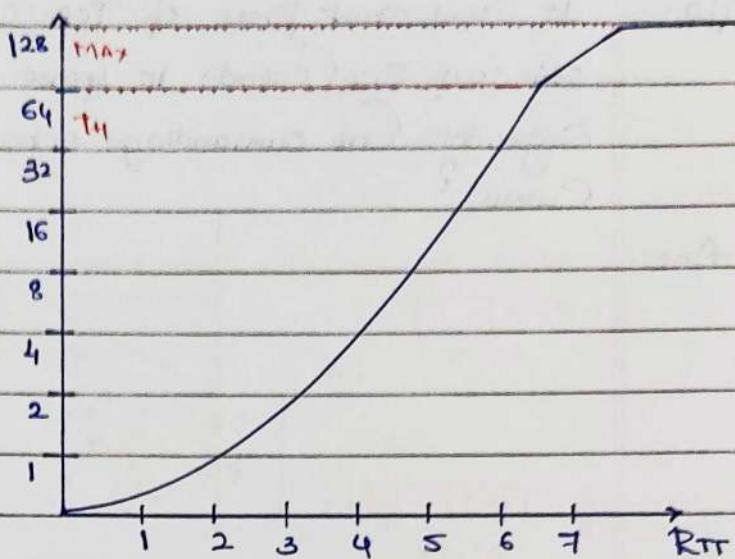
Q1.

$$W.R = 128 \text{ KB}$$

$$\text{MSS} = 1 \text{ KB} \quad \text{No. of Segments} = \frac{128 \text{ KB}}{1 \text{ KB}} = 128$$

$$T_H = \frac{1}{2} \times 128 = 64 \text{ segments.}$$

$$W_C = 1, 2, 4, 8, 16, 32, 64 \\ 65, 66, \dots 128, 128 \dots$$



$$Q2. WR = 128 \text{ KB}$$

$$MSS = 1 \text{ KB}$$

$$\text{No. of segments} = \frac{128 \text{ KB}}{1 \text{ KB}} = 128, T_H = \frac{1}{2} WR = 64 \text{ segments.}$$

$NTH = 19$

$\rightarrow 1, 2, 4, 8, 16, 32, 64, 65, 66, 67, 68 \uparrow NTH = 34$
 3 dup. ack. $T.O.$

$\rightarrow 4, 8, 16, 19, 20 \uparrow NTH = 10$
 3 dup. ack. $T.O.$

eg: $19 \uparrow NTH = 9.5$
 3 dupl. ack $9, 10, 11, 12$
 (start with 9)

Q1. Consider the following statements regarding the slow start phase of the TCP Congestion Control algorithm. Note that Cwnd stands for the TCP Congestion window and MSS denotes the maximum segment size.

- (i) The cwnd increases by 2mss on every successful acknowledgement.
- (ii) The cwnd approximately doubles on every successful acknowledgement.
- (iii) The cwnd increases by 1mss every round trip time.
- (iv) The cwnd approximately doubles every round trip time.

Which of the following is correct?

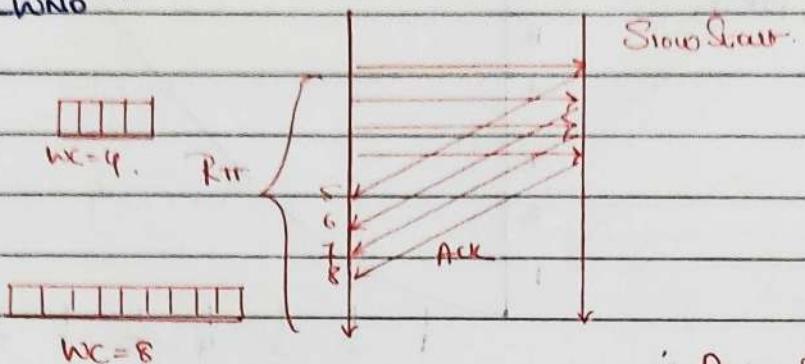
Anc

Only iv is true

Q2.

In Slow start phase of TCP Congestion Control, current congestion window size (CWND) is 4 mss and sender gets 4 successful ACKs of segments (no outstanding ACK) then what should be the value of CWND?

Ans.



$$\therefore \text{Ans} = 8 \text{ mss}$$

Q3.

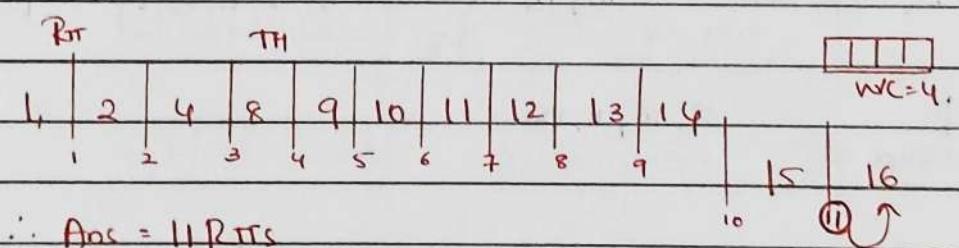
If receiver window size is 1600 Byte and maximum segment size is 1000 Byte then after how many RTT Sender will send full window?

Ans

$$WR = 1600 \text{ Byte}$$

$$MSS = 1000 \text{ Byte} \quad \text{No. of Segments} = \frac{1600 \text{ B}}{1000 \text{ B}} = 16$$

$$TH = \frac{1}{2} WR = 8 \text{ segments}$$



$$\therefore \text{Ans} = 11 \text{ RTTs}$$

Q4.

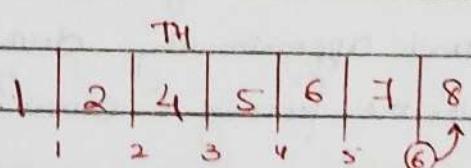
If receiver window size is 8000 Byte and maximum segment size is 1000 Byte then after how many RTT Sender will send full window?

Ans.

$$WR = 8000 \text{ Byte}$$

$$MSS = 1000 \text{ Byte} \quad \text{No. of segments} = \frac{8000 \text{ B}}{1000 \text{ B}} = 8$$

$$TH = \frac{1}{2} WR = 4 \text{ segments}$$

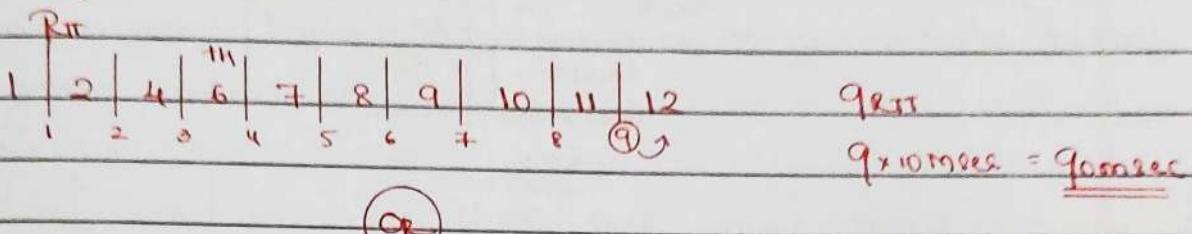


$$\therefore \text{Ans} = 6 \text{ RTTs}$$

Qs. Consider the effect of using Slow Start on a line using a 10-msec round-trip-time. The receive window is 24KB and the maximum segment size is 2KB. How long does it take before the first five windows can be sent?

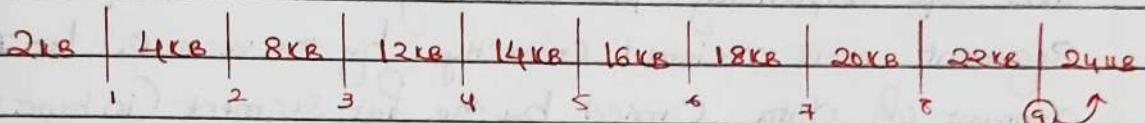
Ans. $RTT = 10\text{msec}$, $WR = 24\text{KB}$, $MSS = 2\text{KB}$, No. of segments = $\frac{24\text{KB}}{2\text{KB}} = 12$

$$TH = \frac{1}{2} WR = 6$$



$WR = 24\text{KB}$

$$TH = \frac{1}{2} WR = 12\text{KB}$$



after 90 msec = $9 \times 10\text{msec} = 90\text{msec}$

Q6. On a TCP Connection Current Congestion Window Size is Congestion Window = 4KB. The window size advertised by the receiver is Advertise window = 6KB. The last byte sent by the sender is LastByteSent = 10240 and last byte acknowledged by receiver is Last byte acknowledged = 8192. The current window size at sender is?

Ans

$$Wc = 4\text{KB}, Ws = 6\text{KB}$$

$$WMS = \min(Wc, Ws) = 4\text{KB}$$

$$= 4 \times 1024\text{B} = 4096\text{Byte}$$

$$\therefore Ans = \underline{4096\text{ Byte}}$$

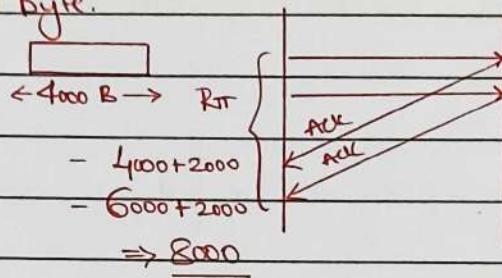
$$\left. \begin{array}{l} \text{Last byte Sent} = 10240 \\ \text{Last byte ACK} = 8192 \\ 10240 - 8192 \\ \hline 2048 \text{ Byte} \end{array} \right\} \text{Just to confirm.}$$

Q7. Suppose that the maximum transmit window size for a TCP connection is 12000 bytes. Each packet consist of 2000 bytes. At some point of time, the connection is in Slow-start phase with a current

transmit window of 4000 bytes. Subsequently the transmitter receives the acknowledgements. Assume that no packets are lost and there are no time-outs. What is the maximum possible value of the current transmit window?

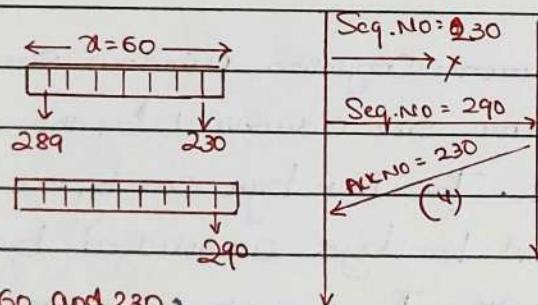
Ans.

Pkt Size = 2000 Byte.



Q8. Consider a TCP connection in a state where there are no outstanding ACKs. The sender sends two segments back-to-back. The sequence numbers of the first and last second segments are 230 and 290 respectively. The first segment was lost, but the second segment was received correctly by the receiver. Let x be the amount of data carried by the first segment (in bytes), and y be the ACK number sent by the receiver. The values of x and y .

Ans.



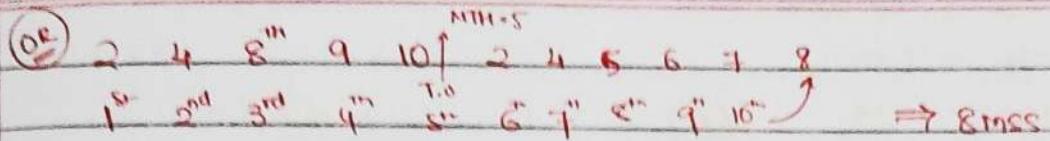
Q9. Consider an instance of TCP's additive increase multiplicative decrease (AIMD) algorithm where the window size at the start of the slow start phase is 2mss and threshold at the start of the first transmission is 8mss. Assume that a timeout occurs during the 5th transmission. Find the congestion window size at the end of the tenth transmission.

T0, NTH=5

Ans.

2 4 8th 9 10th ↑ 1, 2, 4, 5 6 7

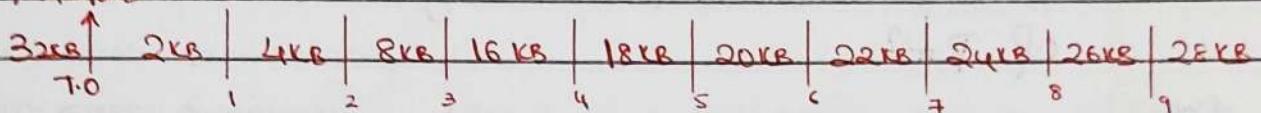
1st 2nd 3rd 4th 5th 6th 7th 8th 9th 10th ↑ $\Rightarrow 7\text{mss}$ ✓



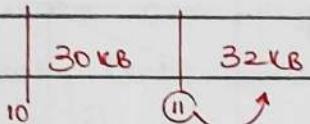
Q10. Let the size of Congestion window of a TCP connection be 32KB when a timeout occurs. The round-trip time of the connection is 100 msec and maximum segment size used is 2KB. The time taken (in msec) by the TCP connection to get back to 32KB Congestion window is _____

Ans:

$$NTH = 16KB$$



$$RTT = 100 \text{ msec}$$



$$\text{Signal Size} = 2KB$$

$$11 RTT$$

$$11 + 100 \text{ msec} = 1100 \text{ msec}$$

Q11. Consider a TCP connection between a Client and Server using the following specifications, the round-trip time is 6msec, the size of the receive advertised window is 50KB, slow-start threshold at the Client is 32KB, and maximum segment size is 2KB. The connection is established at time $t=0$. Assume that there are no timeouts and errors during transmission. Then the size of the congestion window (in KB) at time $t+60$ ms after an acknowledgement are proceeded is _____

is

$$\text{At } t=0 \rightarrow 2KB$$

$$RTT = 6msec$$

$$\text{At } t+6 \rightarrow 4KB$$

$$WR = 50KB$$

$$\text{At } t+12 \rightarrow 8KB$$

$$\text{Slow Start threshold} = 32KB$$

$$\text{At } t+18 \rightarrow 16KB$$

$$\text{Segment Size} = 2KB$$

$$\text{At } t+24 \rightarrow 32KB(\text{TH})$$

$$t=0$$

$$\text{At } t+30 \rightarrow 34KB$$

} Slow Start

Phase

$$\text{At } t+36 \rightarrow 36KB$$

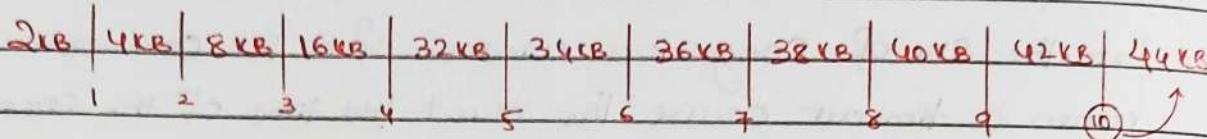
$$\text{At } t+42 \rightarrow 38KB$$

$$\text{At } t+48 \rightarrow 40KB$$

At $t+54 \rightarrow 12\text{KB}$

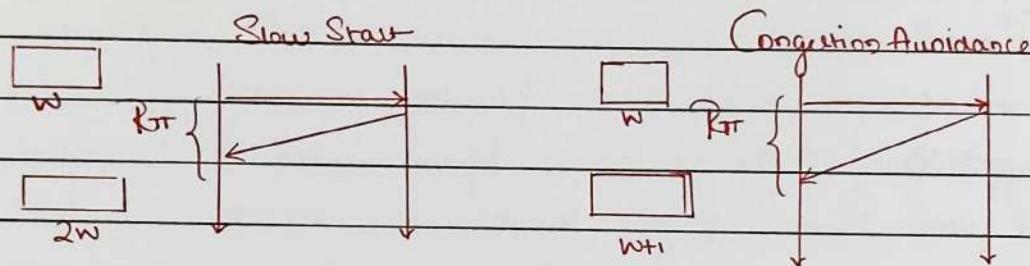
At $t+60 \rightarrow 44\text{KB}$

OR



Q12. Let the window size be a 'w' at the beginning of RTT. Assuming there are no losses in the RTT. What are the respective window sizes for 'slow start' and congestion avoidance after completion of RTT?

Ans

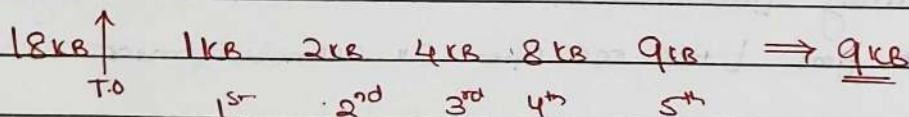


Ans : $2w, w+1$

Q13 Suppose that the TCP congestion window is set to 18KB bytes and a timeout occurs. How big the window be in the first transmission if the next four transmission burst are all successful? Assume that the maximum segment size is 1KB.

Ans

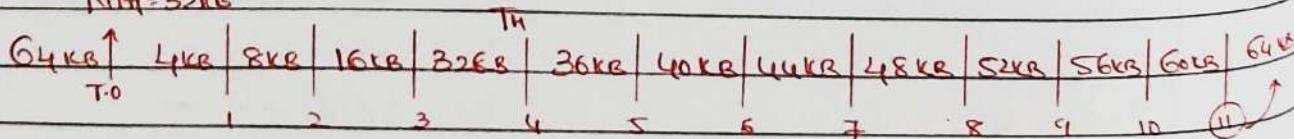
$$NTH = 9\text{KB}$$



Q14. Let the size of congestion window of TCP connection be 64KB when a timeout occurs. The round trip time of a connection is 80 msec and max. Segment Size used is 1KB. The time taken by the TCP Connection to get back to 64KB congestion window is

Ans

$$NTH = 32\text{KB}$$



1) RTT, 11780 msec

\Rightarrow 880 msec

11w)

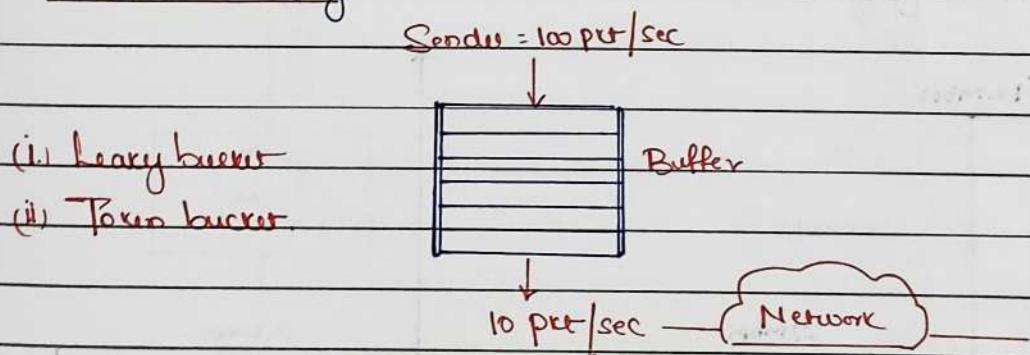
- Q15. While establishing TCP connection both sides and we are established as 48,000 bytes. Maximum Segment Size (mss) is 3,000 bytes. At one point if Sender receives 4 acknowledgements, the window size in the next transmission is _____ bytes.

- Q16. In TCP Congestion Control, the Congestion Window

- A. increases exponentially
- B. increase exponentially upto threshold value after that increase linearly
- C. increases exponentially upto threshold value after that increase linearly upto Sender window size
- D. None of the above

- Q17. In TCP Congestion Control-Two algorithms Current Congestion window size is 16 mss. Timeout occurs at Sender end, then what is the Congestion window size at Sender end during fifth transmission?

Traffic Shaping

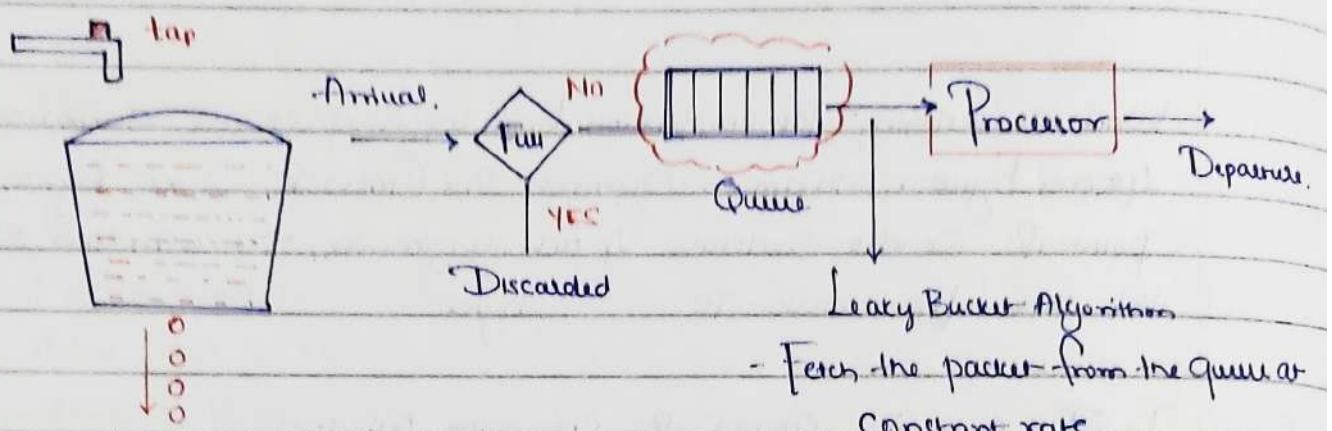


* Another method of congestion control is a "shape" the traffic before it enters into the Network.

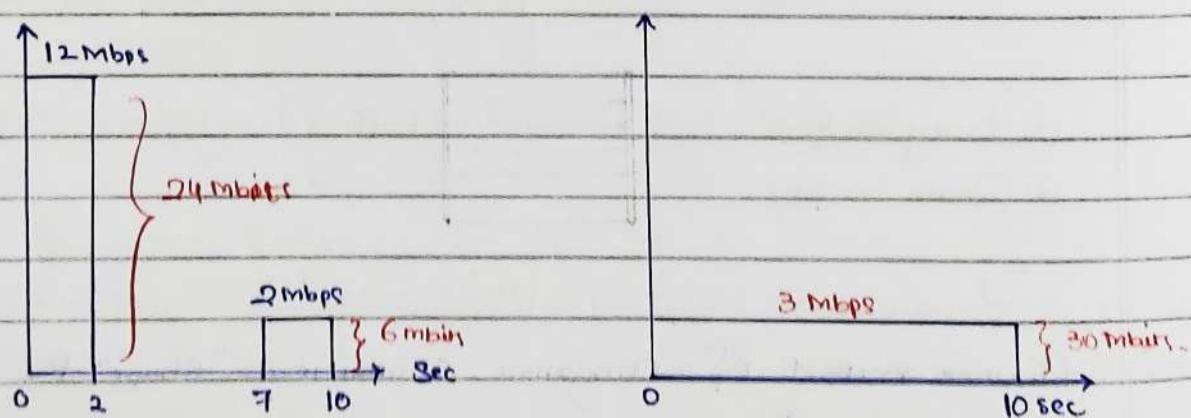
* Traffic Shaping Controls the "rate" at which packets are sent.

* During connection establishment, the Sender and Receiver negotiate a traffic pattern.

Leaky Bucket



- ① If a bucket has a small hole at the bottom, the water leave from the bucket at a constant rate as long as there is water in the bucket.
- ② The rate at which the water leave does not depends on the rate at which the water is input unless the bucket is empty.
- ③ If the bucket is full, water overflows. The input rate can vary, but the output rate remains constant.
- ④ Similarly in networking, a technique called leaky bucket can smooth out bursty traffic.
- ⑤ Leaky bucket algorithm shapes the bursty traffic into fixed rate traffic by averaging the rate.



Bursty Data

$$10 \text{ sec} \rightarrow 24 \text{ Mbit} + 6 \text{ Mbit}$$

$$\rightarrow 30 \text{ Mbit/s}$$

$10 \text{ sec} \rightarrow 30 \text{ Mbit}$
Fixed data rate.

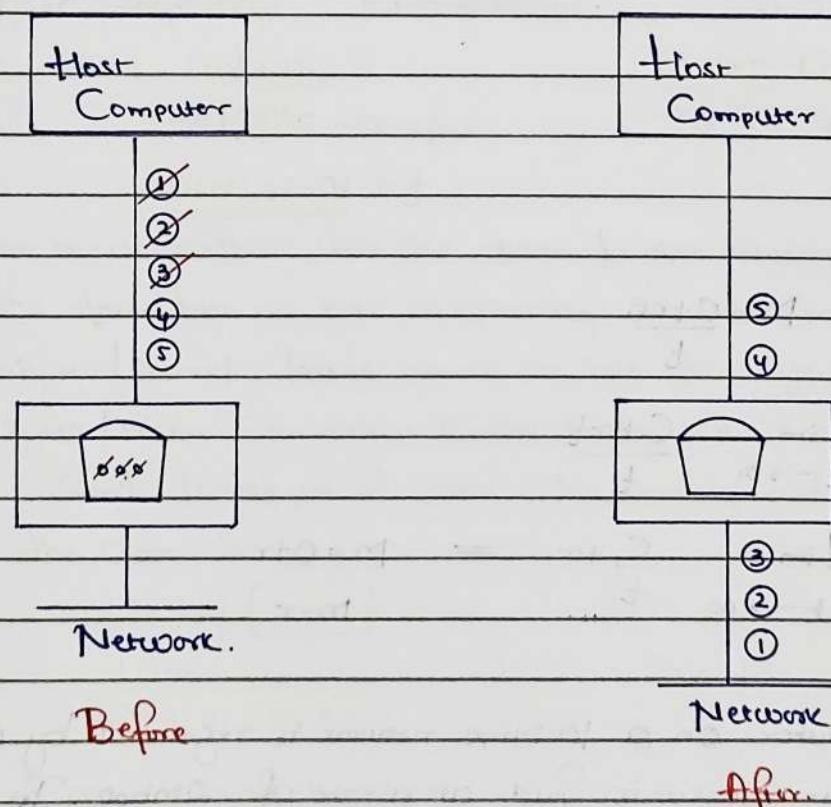
Disadvantage of Leaky Bucket:

The leaky bucket is very restrictive. It does not credit for an ideal host. For eg: if a host is not sending for a while, its bucket becomes empty. Now if the host has bursty data, the leaky bucket allows only an average rate. The time when the host was ideal is not taken into account.

Token Bucket

Token bucket algorithm allows ideal hosts to accumulate credit for the future in the form of token.

- * At regular intervals tokens are thrown into the bucket.
- * Bucket has a maximum capacity.
- * If there is a ready packet, a token is removed from bucket and packet is sent.
- * If there is no token in the bucket then packet cannot be sent.

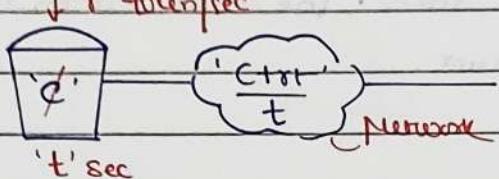


Let the capacity of token bucket is 'C' token and token enter the bucket at the rate of ' r ' token per second.

Maximum no. of packets that can be entered into the network during any time interval of length 't' is

$$\text{Maximum No. of packets} = C + rt$$

$$\text{Maximum avg rate for token bucket} = \frac{C+rt}{t}$$



$$t \text{ sec} \rightarrow C + rt$$

$$1 \text{ sec} \rightarrow \frac{C + rt}{t}$$

Q1. Consider a token bucket of capacity 250 KB and the tokens arrive at a rate of 2MB/sec. If the maximum output rate is 25 MB/sec. What is the burst time?

Ans: $C = 250 \text{ KB}$, $r = 2 \text{ MB/sec}$, $M = 25 \text{ MB/sec}$

$$M = \frac{C + rt}{t}$$

$$Mt = C + rt$$

$$t = \frac{C}{m-r}$$

$$t = \frac{250 \text{ KB}}{25 \text{ MB/sec} - 2 \text{ MB/sec}}$$

$$Mt - rt = C$$

$$= \frac{250 \text{ KB}}{23 \text{ MB/sec}}$$

$$(m-r)t = C$$

$$= 250 \text{ KB}$$

$$t = \underline{\underline{10.86 \text{ msec}}}$$

Note: $M = \frac{C+rt}{t}$

$$= \lim_{t \rightarrow \infty} \frac{C + rt}{t}$$

$$= \lim_{t \rightarrow \infty} \frac{C + rt}{t} = M = r$$

$$M = r$$

Q2. A computer on a 10 Mbps network is regulated by a token bucket. The token bucket is filled at a rate of 2Mbps. It is initially filled to capacity with 16 Megabits. What is the maximum duration for which the computer can transmit at the full 10Mbps?

Ans: $r = 2 \text{ Mbps}$, $C = 16 \text{ Mbytes}$, $M = 10 \text{ Mbps}$

$$t = \frac{C}{m-r} = \frac{16 \text{ mbits}}{10 \text{ mbps} - 2 \text{ mbps}} = \frac{16 \text{ mbits}}{8 \text{ mbps}} = \frac{16 \text{ mbits}}{8 \text{ mbits/sec}} = 2 \text{ sec}$$

Q3. A computer on a 6-mbps network is regulated by a token bucket. The token bucket is filled at a rate of 1mbps. It is initially filled to capacity with 8 megabits. How long can the computer transmit at full 6mbps?

Ans: $M=6 \text{ mbps}, r=1 \text{ mbps}, C=8 \text{ mbits}$

$$t = \frac{C}{m-r} = \frac{8 \text{ mbits}}{6 \text{ mbps} - 1 \text{ mbps}} = \frac{8 \text{ mbits}}{5 \text{ mbits/sec}} \Rightarrow 1.6 \text{ sec}$$

Q4. Imagine that the maximum packet size is 100 bytes, the token bucket rate is 10 million bytes/sec, the token bucket size is 1million bytes, and the maximum transmission rate is 50 million bytes/sec. How long can a burst at maximum speed last?

Ans: $r=10 \text{ MB/sec}, C=1 \text{ MB}, M=50 \text{ MB/sec}$

$$t = \frac{C}{m-r} = \frac{1 \text{ MB}}{50 \text{ MB/sec} - 10 \text{ MB/sec}} = \frac{1 \text{ MB}}{40 \text{ MB/sec}} \Rightarrow 0.025 \text{ sec}$$

$$\Rightarrow 25 \text{ msec}$$

Q5. For a host machine that uses the token bucket algorithm for congestion control, the token bucket has a capacity of 1MB and max output rate is 20 MB/sec/second. Tokens arrive at rate to sustain output at a rate of 10 MB/sec/second. The token bucket is currently full and the machine needs to send 12 MBbytes of data. The minimum time required to transmit the data is 1.1 seconds.

Ans. $C=1 \text{ MB}, M=20 \text{ MB/sec}, r=10 \text{ mb/sec}$

$$t = \frac{C}{m-r} = \frac{1 \text{ MB}}{20 \text{ MB/sec} - 10 \text{ MB/sec}} = \frac{1 \text{ MB}}{10 \text{ MB/sec}} = 0.1 \text{ sec} \quad (\text{time taken to empty the bucket})$$

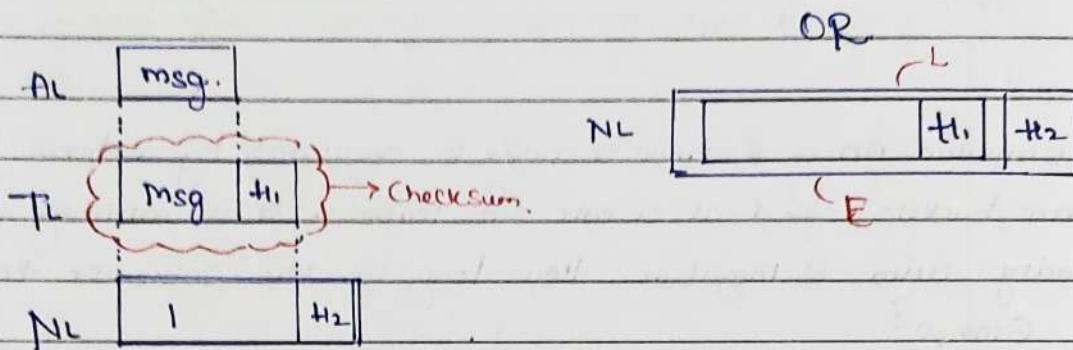
In 0.1 sec we can transfer data = $0.1 * 20 \text{ MB} = 2 \text{ MB}$

Total data = 12 MB, Remaining data = $12 \text{ MB} - 2 \text{ MB} = 10 \text{ MB}$

\therefore for transmitting 10 MB data we need only 1 sec (bcz $r=10 \text{ mb/sec}$)

$$\text{Total time} = 0.1 \text{ sec} + 1 \text{ sec} \Rightarrow 1.1 \text{ sec}$$

Tcp Checksum



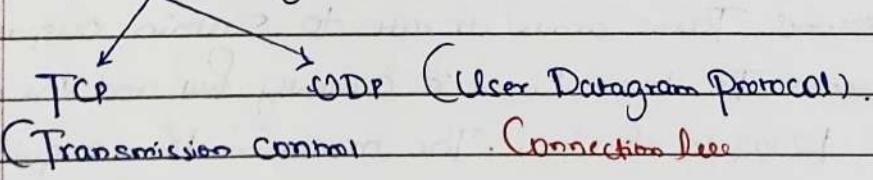
$$\text{TCP Checksum} = \text{TCP data} + \text{TCP header} + \text{IP Pseudoheader}$$

IP Pseudoheader.

| | | | |
|------------------------------------|-----------------|-------------------------------|------------------------------------|
| S.I.P (32bit) | | | $\rightarrow 4B$ |
| D.I.P (32bit) | | | $\rightarrow 4B$ |
| Reserved 00000000 (8bit) | Protocol (8bit) | Tcp Segment Length (16bit) | $\rightarrow 4B$ <hr/> 12 Byte. |

Transport Layer Protocol.

Transport Layer can be Connection oriented or Connection less.



Connection Oriented

TCP

1. Tcp is reliable process to process delivery of entire message
2. Tcp is connection oriented
3. Tcp connection are full duplex and point to point.
4. Tcp connection has 3 phases:

- (i) Connection establishment
 - (ii) Data transfer
 - (iii) Connection termination
5. Each TCP connection is associated with four windows.
6. TCP uses "three way handshake" to establish TCP connection.
7. TCP is not suitable for broadcasting and multicasting.
8. TCP header size is 20 byte but if options are added it will become 60 byte.
9. TCP provides end-to-end error control and flow control.
10. Data will be received at the destination in order.

Out of Order Segment:

- * TCP implements today do not discard out of order segments. They store them temporarily and flag them as out of order until the missing segment arrives.
- * However that out of order segment need delivered to process.

Note: Data may arrive out of order and be temporarily stored by receiving TCP, but TCP guarantees that no out-of-order data delivered to the process.

UDP

1. UDP is message oriented connection less datagram protocol.
2. It is unreliable transport protocol.
3. It does not provide flow control and error control and congestion control.
4. It does not add anything to service except process to process delivery of data.
5. Header is simple & fixed in size i.e. 8 bytes.

UDP-Header

| Source Port. (16 bit) | Destination Port. (16 bit) | 32 bit = 4B |
|--------------------------|-------------------------------|-----------------------|
| Length (16 bit) | Checksum (16 bit) | 32 bit = 4B 8 Byte |

Source port address: This is a 16 bit field that defines the port no. of the application program in the host that is sending the segment.

Destination Port Address: This is a 16 bit field that defines the port number of the application program in the host that is receiving the segment.

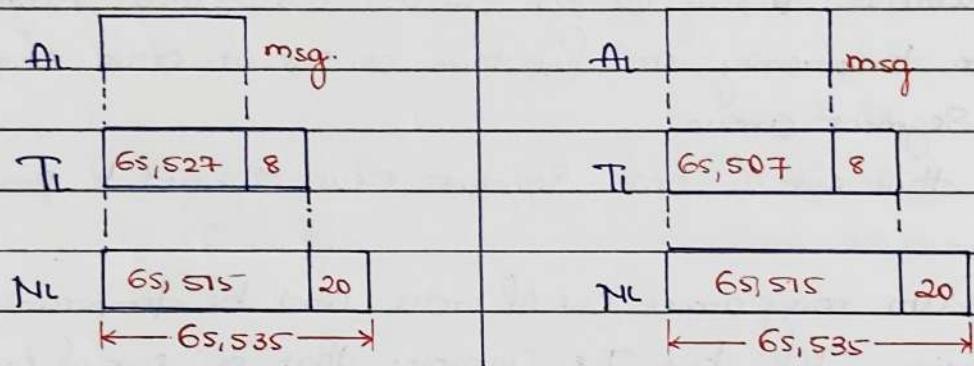
Total Length = 16 bit.

$$\text{Maximum number} = 2^{16} - 1 = 65,535$$

$$T_L = \text{Data} + \text{Header}$$

$$65,535 = \text{Data} + \text{Header}$$

$$\text{Max UDP Data} = 65,535 - 8 \rightarrow 65,527$$

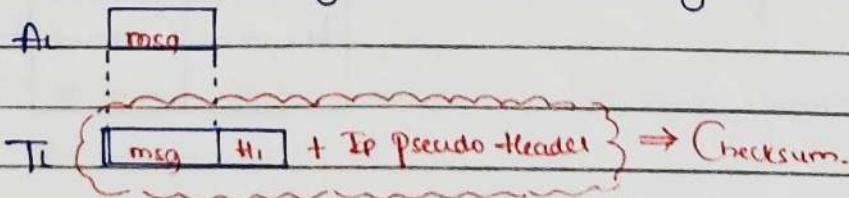


Note:

- Practically data size at Transport Layer for UDP is maximum 65,507 Bytes.
- Only those process sending short message less than 65,507 bytes ($65,535 - 20$ (IP header) - 8 (UDP header)) can use UDP.

Checksum [UDP Checksum = UDP data + UDP header + IP pseudo-header]

UDP Checksum includes three sections: a Pseudo header, UDP header, and data coming from application layer.



T/F Pseudo-header.

| | |
|---------------------------|------|
| S.I.P (32bit) | → 4B |
| D.I.P (32bit) | → 4B |
| Reserved (8bit) | → 4B |
| Protocol (8bit) | → 1B |
| (PP Total Length (16bit)) | 12B |

Q. The following is the content of a UDP header in hexadecimal format.

S.port | D.port | Tl | Checksum
 C B E 4 0 0 0 D 0 0 1 C 0 0 1 C

a. What is the Source Port number?

$$\begin{aligned} \text{S.port} &= (\text{CBE4})_{16} \\ &= 12 \times 16^3 + 11 \times 16^2 + 8 \times 16^1 + 4 \times 16^0 = 52,100. \end{aligned}$$

b. What is the Destination Port number?

$$\text{D. port} = (\text{D00D})_{16} = 13 \times 16^0 = 13.$$

c. What is the total length of the user datagram?

$$\text{Tl} = (\text{001C})_{16} = 1 \times 16^1 + 9 \times 16^0 = 28.$$

d. What is the length of the data?

$$\text{Total length} = \text{data + header}, \quad 28 = \text{Data} + 8, \quad \therefore \text{Data} = 20 \text{ byte}$$

e. Is the packet directed from a client to server or vice versa?

$$\text{D. port no} = 13 \text{ (well known port no)} \rightarrow \left\{ \begin{array}{l} 0 - 1023 \\ \downarrow \\ \text{Server} \end{array} \right.$$

∴ Packet is moving from Client to Server.

* When Destination Port number is well known Port number then data is moving from Client to Server.

* When source Port number is well known Port number then data is moving from Server to Client.

Note:

Unlike TCP, the Checksum Calculation is not mandatory in UDP. No Error Control or Flow Control is provided by UDP. Hence UDP depends on IP and ICMP for error reporting.

Optional inclusion of checksum:

The Sender of UDP packet can choose not to calculate the Checksum. In this case the Checksum field is filled with all 0's before being sent.

Q. What value is sent for the Checksum in each one of the following hypothetical situations?

1. The sender decides not to include the checksum.
2. The sender decides to include the checksum, but the value of the sum is all 1's.
3. The sender decides to include the checksum, but value of sum is all 0's.

Solutions:

- ① The value sent for checksum field is all 0's to show that the checksum is not calculated.
- ② When the sender complements the sum, the result is all 0's, the sender complements the result again before sending. The value sent for the checksum is all 1's. The second complement operation is needed to avoid confusion with the case in part 1.
- ③ This situation never happens because it implies that the value of every term included in the calculation of the sum is all 0's, which is impossible; some fields in the Pseudohandler have non zero values.

Why UDP?

1. The application that required one request one reply. TCP is not suitable hence we use UDP.
2. Application that required constant dataflow TCP is not suitable hence we use UDP.
3. Applications that required multimedia data transfer, applications that require fastness than reliability TCP is not suitable, hence we use UDP.
4. UDP used for management process such as SNMP (Simple n/w management protocol)
5. UDP is used for some route updating protocols such as RIP.
6. For broadcasting and multicasting TCP is not suitable, hence we use UDP.
7. UDP is normally used for interactive real-time applications.
8. It is suitable for process with internal flow-and error control mechanisms. For eg: the Trivial File Transfer Protocol (TFTP) process includes flow and error control. It can easily use UDP.

| TCP | UDP |
|--------------------------------------|---|
| * Dynamic header (20-60 Byte) | Fixed header (8 Byte) |
| * End-to-end flow control | No flow control |
| * Error control (Checksum mandatory) | No error control (Checksum optional) |
| * Connection Oriented | Connection less |
| * Reliability in delivery of msg. | Not reliable |
| * Sequence number | No Sequence number |
| * Acknowledgement no. | No acknowledgement number |
| * Overhead is high | Overhead is low |
| * Keeps track of order (Sequence) | No. order |
| * Protocols: HTTP, FTP, SMTP, POP | Protocol: DNS, SNMP, TFTP, NFS, RIP, BOOTP, DHCP, All real-time and multimedia protocols. |

Note:

- * Client Server Application Such as DNS need the Service of UDP because a Client need to send a short request to server and to receive a quick response from it. The request and response can each fit in one user Datagram. Since only one message is exchanged in each direction.
- * a) Client Server Application Such as SMTP, which is used in electronic mail, Cannot use the Service of UDP because a user might send a long e-mail which could include multimedia (images, videos etc). If the Application uses UDP and the message does not fit in one user Datagram, the message must be split into the Application into different user Datagrams. Here the connectionless service may create problems. The user datagrams may arrive and be delivered to the receiver Application out of order. The receiver application may not be able to reorder the pieces.

MEDIUM ACCESS CONTROL

Multiple Access Protocols.

Random Access Protocol

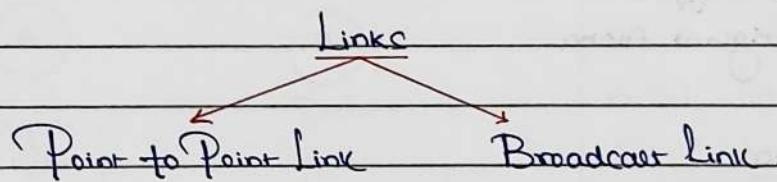
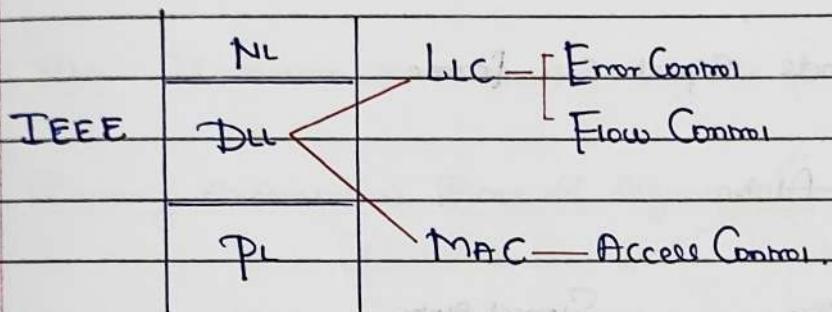
- ALOHA
- CSMA
- CSMA/CD
- CSMA/CA

Control Access Protocol

- Reservation
- Polling
- Token passing.

Centralized Access Protocol

- FDMA
- TDMA
- CDMA



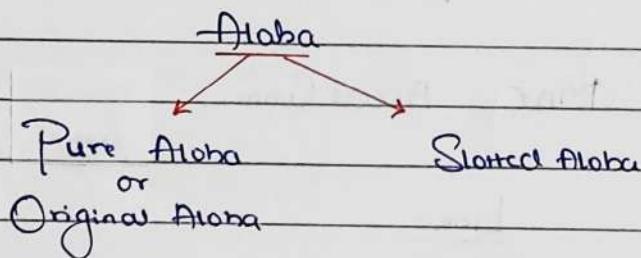
Random Access Protocol

1. In random access, no station is superior to another. Station and time is assigned control over. Another i.e. no station permits or stops another station to send data.
2. Any station can send the data whenever it wants.
3. If more than one station tries to send then there is an access conflict (Collision and the frame will be either destroyed or modified).

4. To avoid collision stations must send data by executing a procedure or a condition defined by the protocol.
5. There is no fixed order in which stations send data so these are called Random access protocols.
6. Each station competes for the channel hence they are also known as contention methods.

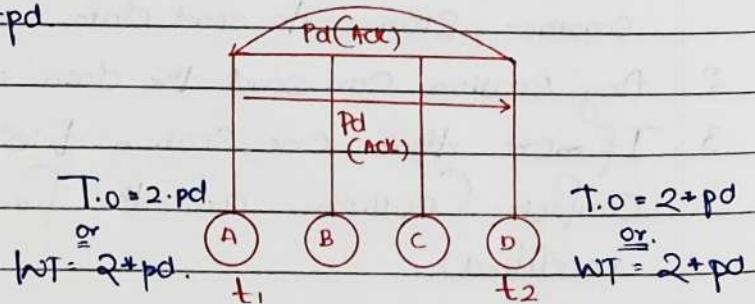
Introduction to Aloha

- * Aloha was developed at University of Hawaii in 1970s.
- * It was designed for wireless LAN but it can be used in any shared medium.
- * Each station sends equal size frame.



Pure Aloha

- * It allows stations to transmit the data at any time whenever they want.
- * Hence collision chances are very high.
- * After transmitting the data packet stations must wait for the ACK.
- * If acknowledgement does not arrive after a time out period, the station assumes that frame (or the acknowledgement) has been destroyed.
- * The timeout period is equal to the maximum possible round trip propagation delay i.e. $2 \cdot pd$.



- * After the timeout, Station will again send data but if it is immediate, tries to send data packet then collision will occur because timeout is also same for all the stations. Hence no station can effectively send data.

- * So stations must not send frame immediately after timeout.
- * It must wait for random amount of time called back off time.

$$\text{Back off time} = k \times \text{slot time}$$

$(0 \rightarrow 2^n - 1)$

$k \rightarrow$ Any random number in btw $0 - 2^n - 1$.

$n \rightarrow$ Collision number.

Note: Collision number is with respect to data pkt

$$\rightarrow \text{Slot time} = (\text{RTT} / (2 \times \text{Pd}) \text{ or } T_d \text{ or } P_d)$$

Note: Maximum number of attempts for the station is 15.

Binary exponential Back off Algorithm (2 stations)

| | | A | B |
|---------------------------------------|---------------------------------------|--|-----------------------------|
| t_1 | t_1 | Collision | |
| Data pkt - 1. | | | |
| $n=1$ | | | |
| $k \rightarrow 0 \text{ to } 2^0 - 1$ | $k \rightarrow 0 \text{ to } 2^0 - 1$ | $P(A) = \frac{1}{2} = 50\%$ | |
| $k \rightarrow 0 \text{ to } 2^0 - 1$ | $k \rightarrow 0 \text{ to } 2^0 - 1$ | | $P(B) = \frac{1}{2} = 50\%$ |
| $k \rightarrow 0, 1$ | $k \rightarrow 0, 1$ | | |
| | | $P(\text{Collision}) = \frac{2}{4} = 50\%$ | |

\rightarrow If we choose $(0, 1)$

Backoff time for A = $k + \text{slot time}$

$$= 0 \times \text{slot time} = 0$$

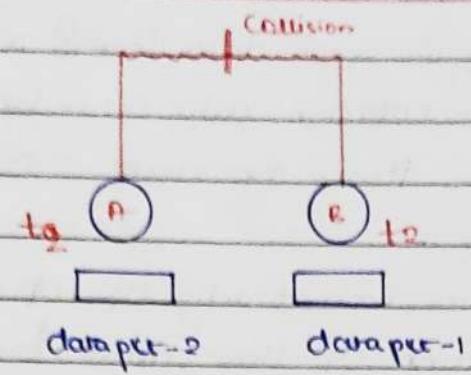
or
WT for A

Backoff time for B = $k + \text{slot time}$

$$= 1 \times \text{slot time}$$

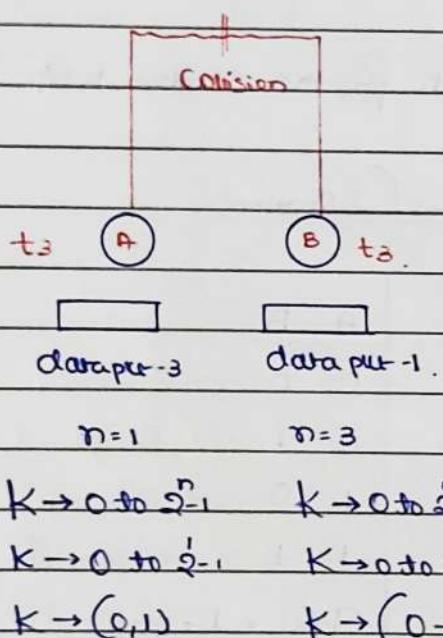
Waiting time for B





$$\begin{aligned}
 n &= 1 & n &= 2 \\
 K &\rightarrow 0 \oplus 2^{-1} & K &\rightarrow 0 \oplus 2^{-1} \\
 K &\rightarrow 0 \oplus 2^{-1} & K &\rightarrow 0 \oplus 2^{-1} \\
 K &\rightarrow (0,1) & K &\rightarrow 0 \oplus 3 \\
 && K &\rightarrow (0,1,2,3)
 \end{aligned}$$

| A | B |
|---|---|
| 0 | 0 → Collision $P(A) = \frac{5}{8} = 62.5\%$ |
| 0 | 1 → A won |
| 0 | 2 → A won |
| 0 | 3 → A won $P(B) = \frac{1}{8} = 0.125 = 12.5\%$ |
| 1 | 0 → B won |
| 1 | 1 → Collision |
| 1 | 2 → A won $P(\text{Collision}) = \frac{2}{8}$ |
| 1 | 3 → A won $= \frac{1}{4} = 25\%$ |



$$\begin{aligned}
 n &= 1 & n &= 3 \\
 K &\rightarrow 0 \oplus 2^{-1} & K &\rightarrow 0 \oplus 2^{-1} \\
 K &\rightarrow 0 \oplus 2^{-1} & K &\rightarrow 0 \oplus 2^{-1} \\
 K &\rightarrow (0,1) & K &\rightarrow (0-7)
 \end{aligned}$$

| A | B | A | B |
|---|---------------|---|---------------|
| 0 | 0 - Collision | 1 | 0 - B won |
| 0 | 1 - A won | 1 | 1 - Collision |
| 0 | 2 - A won | 1 | 2 - A won |
| 0 | 3 - A won | 1 | 3 - A won |
| 0 | 4 - A won | 1 | 4 - A won |
| 0 | 5 - A won | 1 | 5 - A won |
| 0 | 6 - A won | 1 | 6 - A won |
| 0 | 7 - A won | 1 | 7 - A won |

$$P(A) = \frac{13}{16} = 0.8125 = 81.25\%.$$

$$P(B) = \frac{1}{16} = 0.0625 = 6.25\%.$$

$$P(\text{Collision}) = \frac{3}{16} = 0.1875 = 12.5\%.$$

→ Initially the probability of collision = 100%.

After 1st collision " " " " = 50%.

After 2nd collision " " " " = 25%.

After 3rd collision " " " " = 12.5%.

- Probability of collision is decreasing exponentially so Back off algorithm is also known as "exponential back off algorithm".

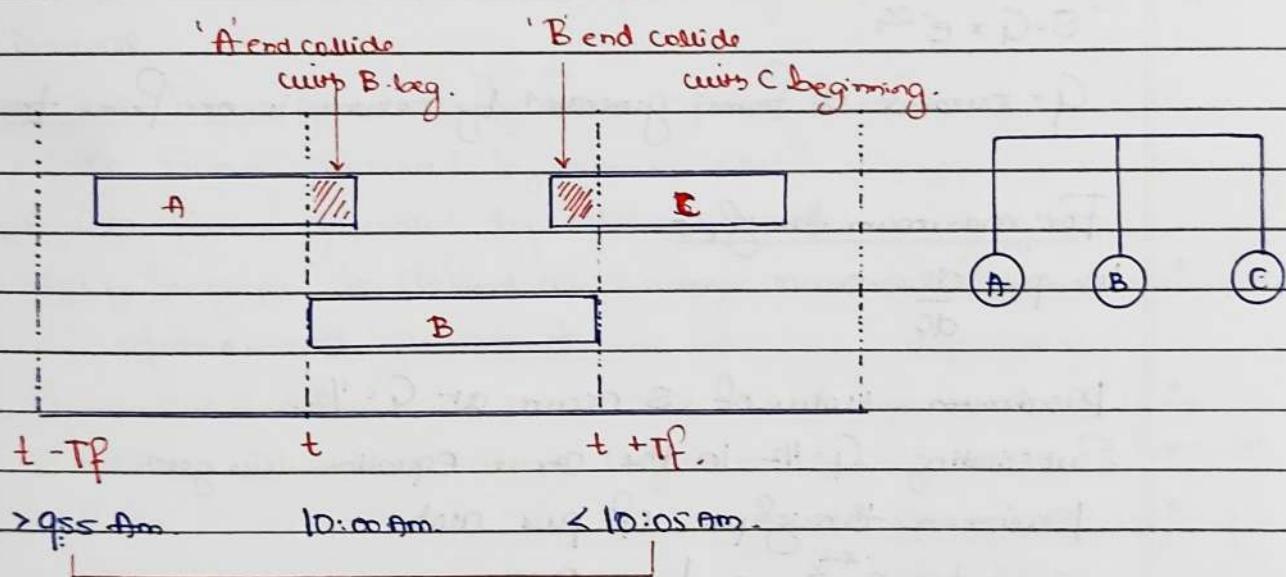
Disadvantage of Back off Algorithm:

- This algorithm suffers from Capture effect. If any station wins in the 1st collision then it has a more probability for winning in the next collision.

eg: initially $P(A) = 25\%$
 $P(B) = 62.5\%$.
 $P(C) = 81.25\%$.

Vulnerable time for pure Aloha

Vulnerable time is the range of time where collision take place.



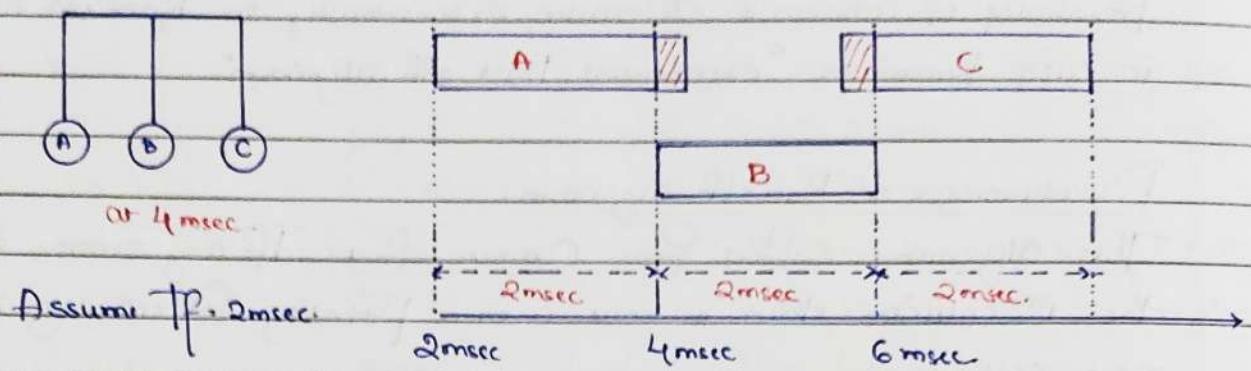
Vulnerable time = 10 min

Vulnerable time for pure Aloha = $2^t \cdot Tf$

Transmission time for single frame (T_f) = FrameSize - $\frac{L}{Baudwidth}$

Assume Transmission time for single frame $T_f = 5 \text{ min}$.) about diagram.

2.



A starts at 2.01 msec

 $A \rightarrow 2.01 \text{ msec} \text{ to } 4.01 \text{ msec}$

C starts at 5.98 msec.

2 msec — 6 msec

Vulnerable time = 1 msec

Vulnerable time for pure aloha = $2 \times T_f$

Throughput of pure aloha

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

G = number of frames generated by network in one frame transmission.

For maximum throughput.

* We put $\frac{dS}{dG} = 0$

* Maximum value of S occurs at $G = 1/2$.

* Substituting $G = 1/2$ in the above equation we get:

* Maximum throughput of pure aloha

$$= \frac{1}{2} \times e^{-\frac{2 \times 1/2}{2}} = \frac{1}{2e} = 0.184$$

∴ Maximum throughput of pure aloha = 18.4%

Note:

1. If 1000 frames are generated by frame in one frame transmission time then maximum 184 frames can be delivered successfully.

2. $S_{max} \rightarrow G = \frac{1}{2}$

One half frame should be generated in one frame transmission time

to achieve maximum throughput.

OR

One frame should be generated in two frame transmission time to achieve maximum throughput \rightarrow Vulnerable time = $2 \times T_F$

- ③ If one frame is generated by the network in two frame transmission time then in this situation we will achieve maximum throughput.
- ④ Vulnerable time $2T_F$ is basically representing if one frame is generated by the network in two frame transmission time then there will be no collision. So if there is no collision So we will achieve maximum throughput.

eg. If pure aloha network transmits 200 bit frames on shared channel of 200 kbps. What is the throughput if the system (all stations together) produce.

(i) 1000 frames generated by frame n/w in 1 sec?

(ii) 500 frames generated by n/w in 1 sec?

(iii) 250 frames generated by n/w in 1 sec?

Note: Throughput is defined as average number of frames successfully transmitted per second.

Ans.

Frame Size = 200 bits

Transmission time = Frame

Bandwidth

Bandwidth = 200 kbps = 200×10^3 bits/sec

$$= \frac{200 \text{ bits}}{200 \times 10^3 \text{ bits/sec}} = \frac{1}{10^3} \text{ sec} = 1 \text{ msec}$$

Solution (i):

$$1 \text{ sec.} \longrightarrow 1000$$

$$1 \text{ msec.} \longrightarrow 1000 \times 10^3 \text{ Frame}$$

$$q = 1$$

(No. of frames generated in one frame transmission time)

$$\text{Throughput} = S = q \times e^{-2q}$$

$$= 1 \times e^{-2 \times 1} = \frac{1}{e^2} = 0.135, \therefore \text{Throughput} = 13.5\%$$

$$\text{Avg. no. of frames generated successfully transmitted per sec} = 1000 \times 0.135 \\ = \underline{\underline{135}}$$

Solⁿ (iii)

$$1 \text{ sec} \longrightarrow 500 \text{ frame}$$

$$1 \text{ msec} \longrightarrow 500 \times 10^3 \text{ frame}$$

$$= 5 \times 10^6$$

$$= 5/10 \text{ frame} \Rightarrow$$

$$q = \frac{1}{2}$$

$$\text{Throughput } g = G + e^{-2g}$$

$$= 1 + e^{-2+1/2}$$

$$= \frac{1}{2} = 0.184$$

$$= \underline{\underline{18.4 \text{ b}}}$$

Avg no of frames successfully transmitted

$$\text{per sec.} = 500 \times 0.184 \Rightarrow 92.$$

Solⁿ (iii)

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

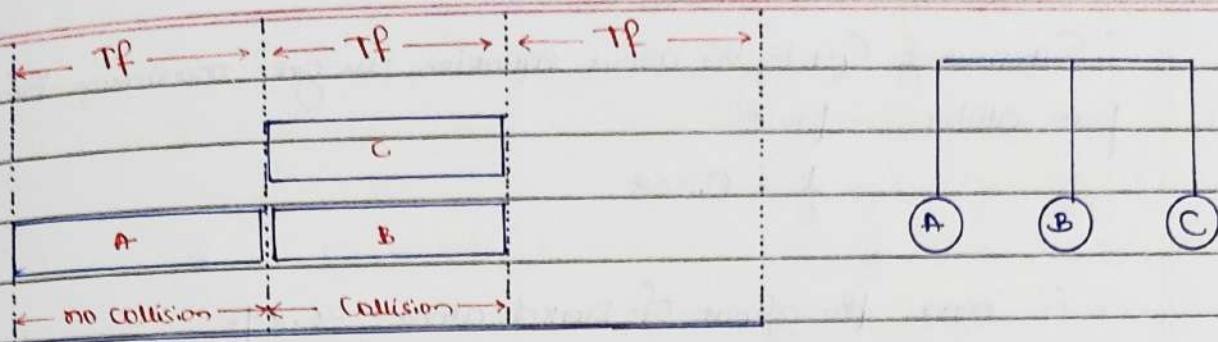
$$\text{Throughput} = 0.152 \rightarrow 15.2\%$$

$$\text{Average no. of frames successfully transmitted/sec} = 0.152 \times 250 \\ = \underline{\underline{38}}$$

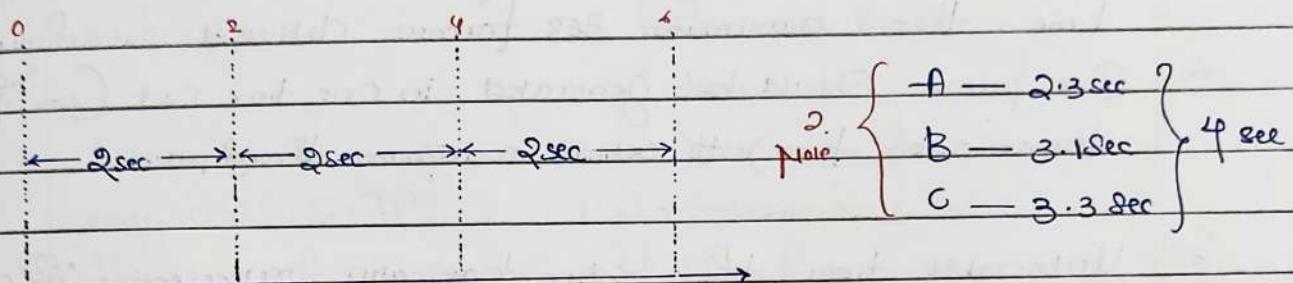
Slotted Aloha.

- * Slotted Aloha divides the time of shared channel into discrete intervals called as time slot (time slot = transmission time for one frame).
- * Any station can transmit its data in any time slot.
- * The only condition is that station must start its transmission from beginning of time slot.
- * If the beginning of the slot is missed, then station has to wait until beginning of next slot.
- * A collision may occur if two or more stations try to transmit data at the beginning of the same time slot.

Variable time for slotted aloha \rightarrow Variable time is the range of time where collision take place (TP).



Vulnerable time for Slotted Aloha = T_f .



Assumed $T_f = 2 \text{ sec}$

Station A Starts at 2.3 sec \rightarrow 4 sec
Station B Starts at 3.1 sec \rightarrow 6 sec

Note:

- For example $T_f = 2 \text{ sec}$ and Station has data to send at 2.3 sec, then it will send at 4 sec and Station has data to send at 5 sec then it will send at 6 sec.
- In slotted data Collision can take place for eg: if three Station have data to send at 2.3, 3.1, 3.3 sec then all of them will send at 4 sec.

Throughput of Slotted Aloha:

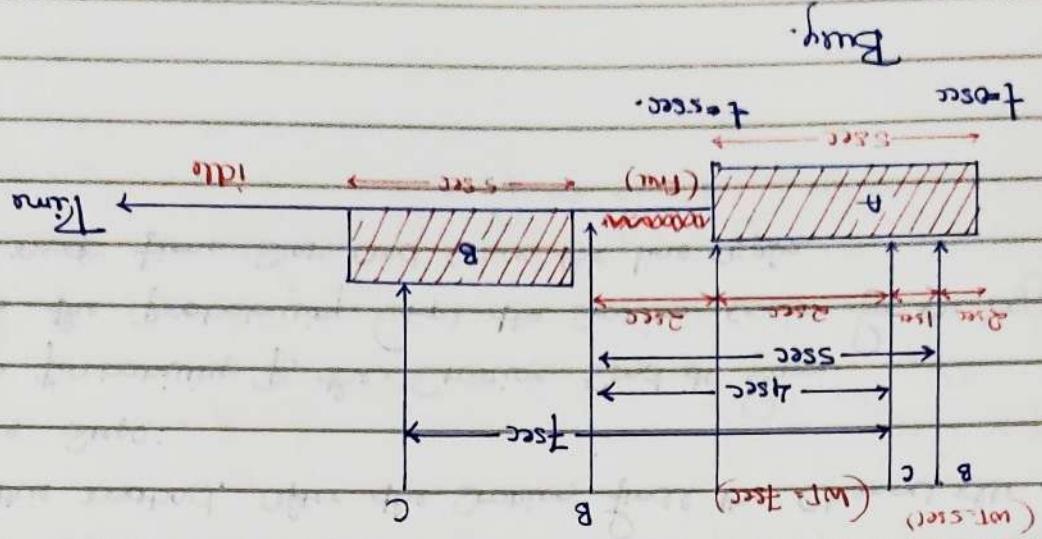
$$S = G \times e^{-G}$$

G = no. of frames generated by n/w in one frame transmission time.

For maximum throughput:

* We put $\frac{dS}{dG} = 0$

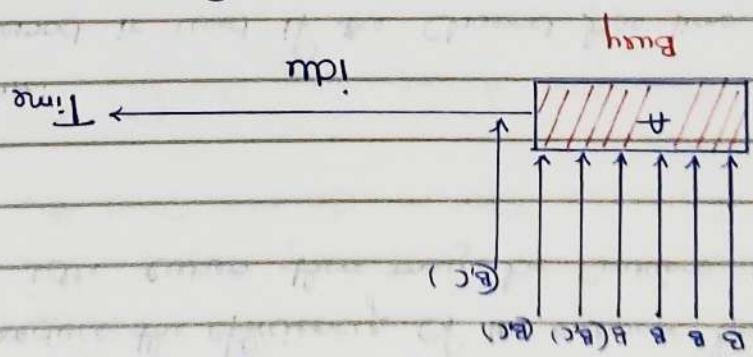
* Maximum value of S occurs at $G=1$



In non-persistent Sma- once the station is ready with the data it will sense the channel, if the channel is busy then it will wait for random duration of time and again sense the channel.

No-n-Persistent CSMA:

Probability of collision is big for example, if two stations receive
ready in the middle of the field transmission, both will receive
partially until the transmission ends, and then both will begin
transmissions exactly simultaneously then collision will occur.



The rate of 1-per cent error is about 20 percent.

Fermentation CSMA

Persistent Methods in CSMF:

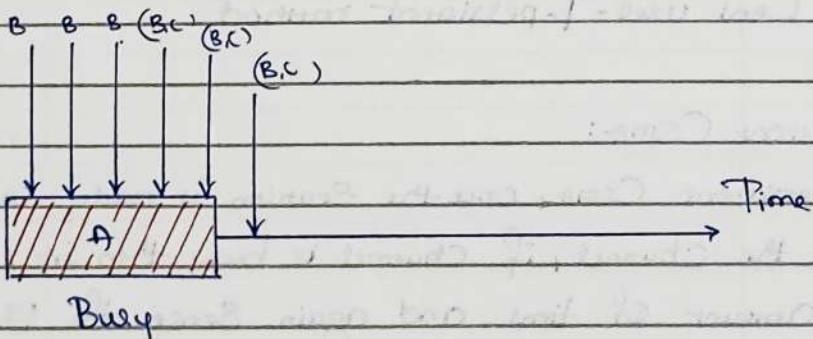
* Once the Channel is free: thus it immediately transmits the frame.

Note :

- In non-persistent CSMA finding the channel idle at the same time by different stations is less. So collision is less compared to 1-persistent.
- This method reduces the efficiency of the network because the medium remains idle even when there may be stations with frame to send.

P-persistent CSMA:

- * P-persistent method is used if the channel has time slot with a slot duration, equal or greater than the maximum propagation time.
- * It uses advantages of both 1-persistent and non-persistent.
- * It reduces the chance of collision and improves efficiency.



- * In this method, after the station finds the channel idle it follows these steps:

1. With probability P , the station sends its frame.
2. With the probability $(1-p)$ the station waits for the beginning of the next time slot and checks the line again.

CSMA/CD (Carrier Sense Multiple Access / Collision Detection)

- * CSMA does not specify what station will do after collision.
- * In CSMA if two stations sense the channel to be idle and begin transmitting simultaneously, then both stations data will collide and still stations will keep on sending the data.
- * Better way to save the time and bandwidth is to detect the collision and immediately stop this strategy is used in CSMA/CD.
- * In CSMA/CD stations do not send the entire frame and then look for collision.
- * In CSMA/CD transmitting the frame and detecting the collisions are continual process.
- * Sender needs two different port i.e. one for sending the data and another for detecting the collision.
- * If collision is detected then sender immediately stops transmitting the data.

| |
|-----|
| S.P |
| L.P |

→ Sending port : for sending the data

→ Listening port : for detecting the collision.

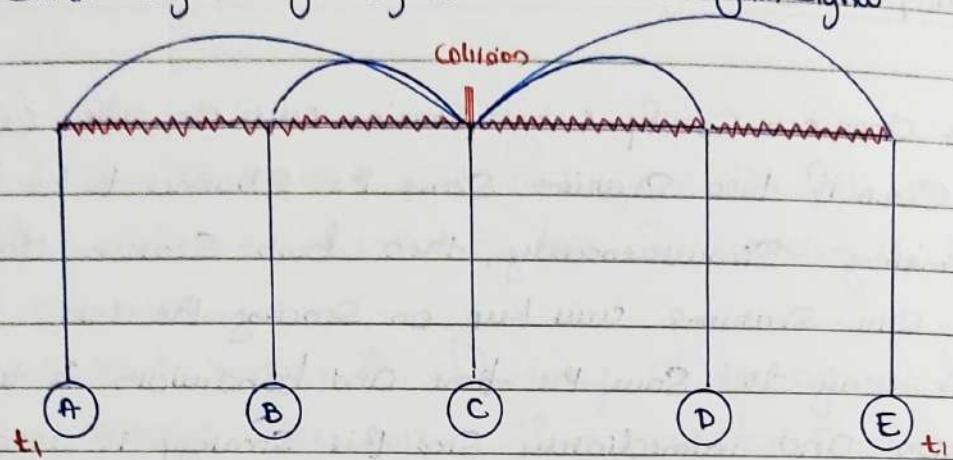
No acknowledgement:

There is no need of acknowledgement, if collision is not detected then frame is definitely received by receiver.

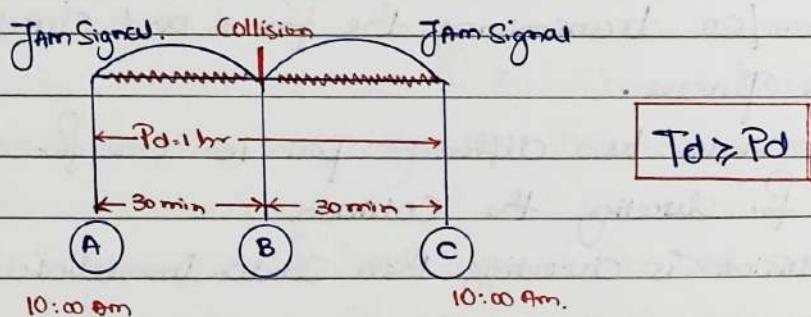
No Copy:

Once frame is transmitted sender does not maintain a copy of that frame because station is simultaneously sending the frame and detecting the collision, if collision is not detected that means receiver has successfully received the frame.

Collision Signal or Jam Signal.



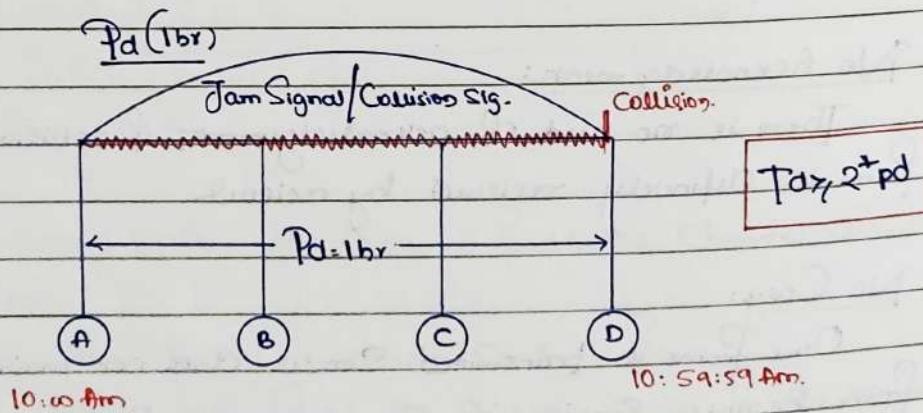
Minimum Frame to detect the collision:



At 10:00 AM \rightarrow Both 'A' and 'C' Start transmitting the data.

At 10:30 AM \rightarrow Collision

At 11:00 AM \rightarrow Both A and C receive Collision Signal.

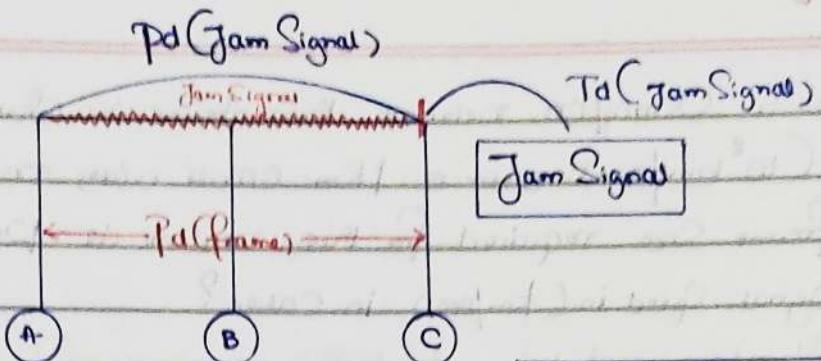


10:00 AM \rightarrow 'A' Start transmitting the data.

10:59:59 AM \rightarrow 'D' Start transmitting the data

11:00 AM \rightarrow Collision

12:00 PM \rightarrow 'A' receive Collision Signal.



$$T_d(\text{Jam Signal}) = \frac{\text{Jam Signal Size}}{\text{Bandwidth}}$$

$$T_d(\text{Frame}) \geq P_d(\text{frame}) + T_d(\text{Jam Signal}) + P_d(\text{Jam Signal})$$

$$T_d(\text{Frame}) \geq 2 * P_d + T_d(\text{Jam Signal})$$

↓
Minimum Frame Size to detect the collision

$$\frac{\text{Frame Size (L)}}{\text{Bandwidth (B)}} \geq 2 * P_d + T_d(\text{Jam Signal})$$

$$\text{Frame Size} \geq (2 * P_d + T_d(\text{Jam Signal})) * \text{Bandwidth}$$

$$L \geq (2 * P_d + T_d(\text{Jam Signal})) * B \quad (\text{exact formula})$$

minimum frame size to detect the collision in CSMA/CD.

Q1. Building a CSMA/CD network running at 1Gbps over a 1km cable with no repeaters. The signal speed in the cable is 200,000 km/sec. The minimum frame size is _____ bits.

$$B = 1\text{Gbps} = 10^9 \text{ bits/sec}, d = 1\text{km}$$

$$V = 200000 \text{ km/sec}$$

$$T_d \geq 2 * P_d + T_d(\text{Jam Signal})$$

$$\frac{L}{B} \geq 2 * P_d$$

$$L \geq 2 * P_d * B$$

$$L \geq 2 * \frac{d}{V} * B$$

$$L \geq \frac{2 * 1\text{km}}{200000 \text{ km/sec}} * 10^9 \text{ bits/sec}$$

$$L \geq 10^6 \text{ bits}$$

$$L \geq 10000 \text{ bits}$$

Q2. Consider a CSMA/CD network that transmits data at a rate of 100 Mbps (10^8 bits/sec) over a 1 Km cable using no repeaters. If the min frame size required for this network is 1250 bytes, what is the signal speed in (km/sec) in cable?

Ans

$$B = 10^8 \text{ bits/sec}, d = 1 \text{ Km}, L = 1250 \text{ Byte} = 8 \times 1250 = 10,000 \text{ bits}$$

$$T_d \geq 2 \times Pd + Td \quad (\text{for Signal})$$

$$Td \geq 2 \times pd$$

$$\frac{L}{8} \geq 2 \times pd \Rightarrow \frac{10,000 \text{ bits}}{10^8 \text{ bits/sec}} \geq \frac{2 \times 1 \text{ Km}}{v}$$

$$= \frac{1}{10^4} \geq \frac{2}{v}$$

$$v = 2 \times 10^4 \text{ Km/sec}$$

$$v = \underline{\underline{20,000 \text{ Km/sec}}}$$

Q3. A network has a data transmission bandwidth of 20×10^6 bits per sec. It uses CSMA/CD in the MAC layer. The maximum signal propagation time from one node to another node is 40 microseconds. The minimum size of a frame in the network is _____ bytes.

Ans

$$B = 20 \times 10^6 \text{ bits/sec}$$

$$Pd = 40 \mu\text{sec} = 40 \times 10^{-6} \text{ sec}$$

$$1 = ?$$

$$Td \geq 2 \times Pd + Td \quad (\text{for Signal})$$

$$\frac{L}{8} \geq 2 \times pd$$

$$L \geq 2 \times Pd + B$$

$$L \geq 2 \times 40 \times 10^{-6} \text{ sec} + 20 \times 10^6 \text{ bits/sec}$$

$$L \geq 1600 \text{ bits}$$

$$L \geq \frac{1600}{8} \text{ Byte} \Rightarrow L \geq \underline{\underline{200 \text{ Byte}}}$$

Introduction To Ethernet

IEEE 802 Project: IEEE started Project 802 so that different LAN can be interconnected.

IEEE 802.1 → Bridge LAN

IEEE 802.2 → LLC

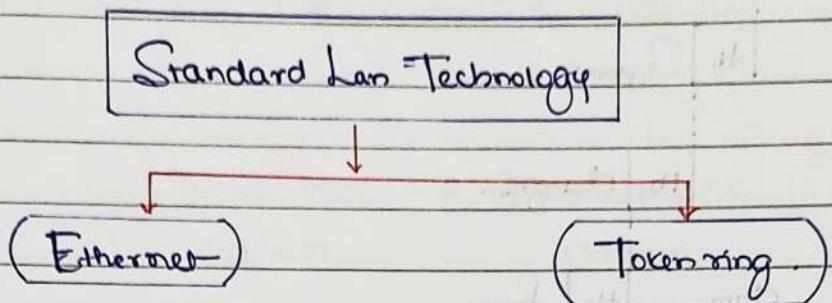
IEEE 802.3 → Ethernet (CSMA/CD)

IEEE 802.4 → Token Bus.

IEEE 802.5 → Tokenring

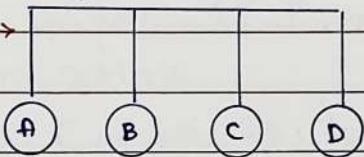
IEEE 8.02.11 → Wireless LAN (CSMA/CD)

IEEE 802.16 → Wireless WAN



Ethernet Characteristics

1. It offers connection less communication.
2. No flow control and packet level error control.
3. No acknowledgement.
4. It uses bus topology.



5. Ethernet uses CSMA/CD as access control method to deal with the collision.
6. In Ethernet signal is broadcasted by sender hence every station on LAN receive it.
7. Ethernet uses Manchester encoding technique for converting data bits into signal.

$$(\text{Baud rate} = 2 \times \text{bit rate})$$

$$\text{Bit rate} = \frac{1}{2} \text{ baud rate}$$

Ethernet Evolution

Standard

Ethernet

10 mbps

Fast Ethernet

100 mbps

Gigabit

Ethernet

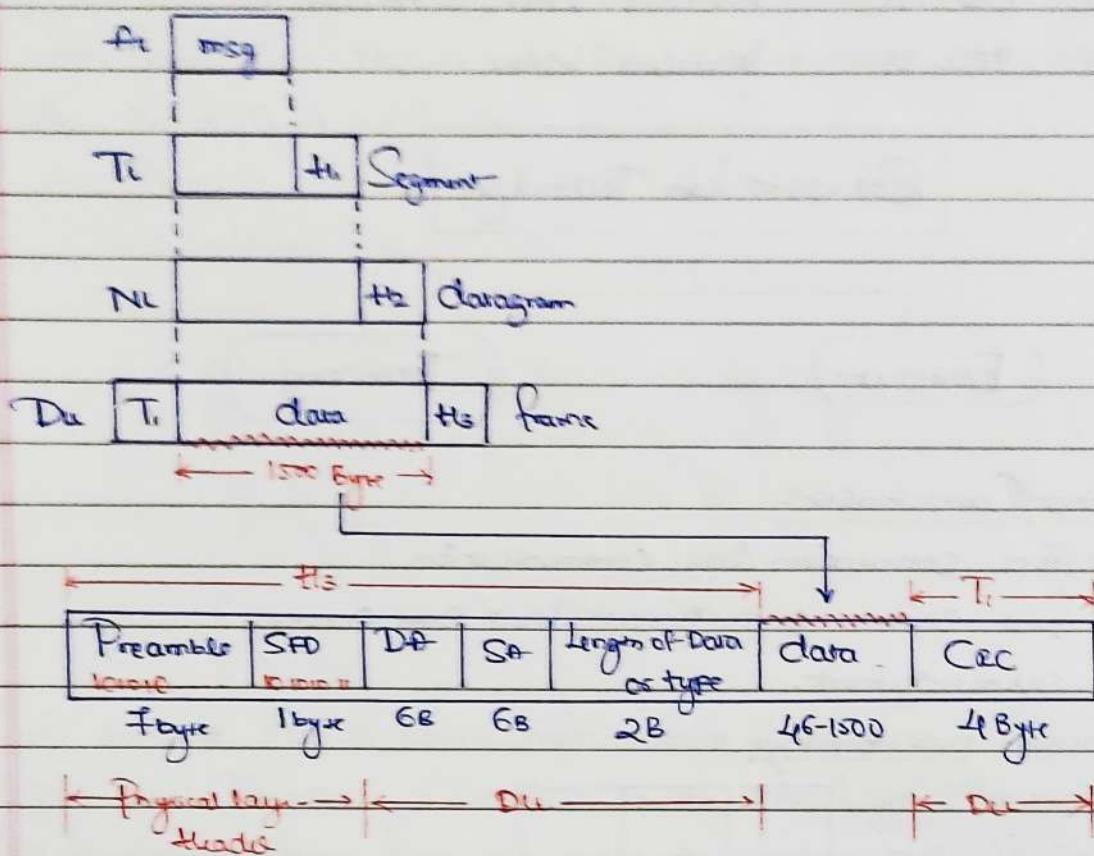
1 Gbps

10 Gigabit

Ethernet

10 Gbps

IEEE 802.3 Ethernet Frame Format:



Preamble (7 Bytes)

- * It is a 7 byte field, it is an alternating pattern of 1's and 0's.
- * It alerts the stations that frame is going to start.
- * It also enables the sender and receiver to establish bit synchronization.

Start Frame Delimiter [SFD]

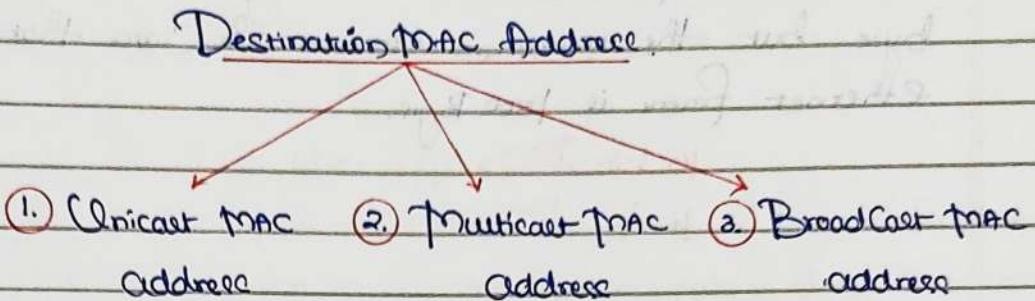
- * It is a one byte field which is always set to 10101011.
- * SFD alerts the station that this is the last for synchronization.
- * The last two bits are '1's' and alert the receiver that the next field is destination address.

Note: The above two fields are added by the physical layer and represent the physical layer header.

- * Sometimes SFD is considered to be a part of Preamble, i.e why at many places Preamble field length is described as 8 bytes.

Destination Address [DA]

- * It is a 6 byte field that contains the MAC address of the destination.



Unicast MAC address: If last bit of the first byte is 0. It indicate Unicast MAC address.

↙ 3A : 2B : C3 : 5A : 9B : F0
 00111 01 | 0 → It indicated unicast MAC address.

Multicast MAC address: If the last bit of the first byte is 1. It indicate multi Cast MAC address.

↙ A3 : 2B : C3 : 5A : 9B : F0
 1010001 | 1 → It indicated multic平 MAC address.

Broadcast MAC address: If all 48 bits are 1. It indicate broadcast MAC address. eg: FF : FF : FF : FF : FF : FF

↓
 11111111

Source Address (6 Byte)

- * It is a 6 byte field that contains the MAC address of source which is sending the data.
- * Source address is always Unicast Address.

Length of Data (2 Byte) :

- * Length is a 2 byte field, which specifies the number of byte present in the data field.
- * In Ethernet data is varying from 46 to 1500 byte, so to keep

track of correct size of data in the packet we need length of data field.

- * The 16 bit field can hold the length value 0 to $2^{16}-1 = 65535$ byte but the maximum amount of data that can be sent in Ethernet frame is 1500 Byte.

$$10 \text{ bit} \xrightarrow{\text{Max.no}} 2^{10}-1 = 1023$$

$$11 \text{ bit} \xrightarrow{\text{Max.no}} 2^{11}-1 = 2047.$$

Type: This field defines the upper layer protocol whose packet is encapsulated in the frame. This protocol can be IP, ARP, OSPF, and so on.

Note: Type field was used in original ethernet. But in IEEE 802.3 this field was replaced by length of data.

Data:

- * It is the variable length field which contains the actual data.
- * It is also known as payload length.
- * The length of this field lies between 46 byte - 1500 byte.
- * To the Ethernet the minimum data has to be 46 byte and maximum data can be 1500 byte.
- * If data coming from the upper layer is more than 1500 byte, it should be fragmented and encapsulated in more than one frame.
- * If it is less than 46 byte it needs to be padded with zeros.

Note:

Minimum size is needed to sense the collision.

Ethernet uses CSMA/CD as an access control method to deal with collisions.

$$T_d(\text{frame}) \geq 2 \times P_d + T_d(\text{jam signal}) \rightarrow \text{min frame size in Ethernet}$$

Maximum size is needed to avoid monopoly of any single station.

If Ethernet allows the frames of big size, then other stations

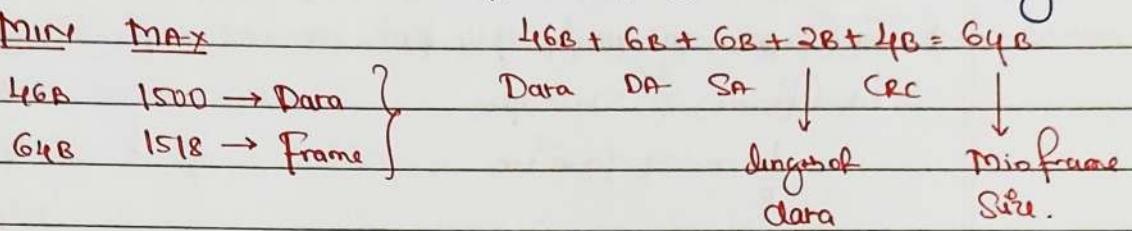
may not get fair chance to send their data.

CRC (4 Bytes)

CRC is used for error detection.

Disadvantages Of Ethernet:

1. In the Ethernet there is restriction on minimum size of the data hence it is not suitable for interactive applications where data size very less.



2. It is not suitable for real time applications. Real time applications require the delivery of data within some time limit. Ethernet is not reliable because of high probability of collision.

3. It is not suitable for Client Server Applications. Client-Server applications require that Server must be given higher priority than Client. In Ethernet there is no facility to set priorities.

Problems on Ethernet:

- Q1. Ethernet when Manchester Encoding is used, the bit rate is:

Ans $\text{Band rate} = 2 \times \text{bit rate}$

$$\text{bit rate} = \frac{1}{2} \text{ Band rate} \quad \therefore \text{Half the band rate}$$

- Q2. What is the Band rate of Standard 10 Mbps 802.3 LAN?

Ans $\text{Bit rate} = 10 \text{ mbps}$

$$\text{Band rate} = 2 \times \text{bit rate} \Rightarrow 20 \text{ mega baud}$$

- Q3. Which of the following statements is True?

Ans Ethernet frame includes a CRC field and IP packet includes a checksum field.

Q4. Suppose the round-trip propagation delay for a 10Mbps Ethernet having 48-bit jamming signal is 46.444s. The minimum frame size is :

Ane

$$B = 10 \text{ Mbps} = 10 \times 10^6 \text{ bits/sec}, \text{ Jam Signal Size} = 48 \text{ bits}$$

$$RTT = 46.444 \text{ s} = 46.444 \times 10^{-6} \text{ sec}$$

\Rightarrow 48 bits

$$T_d(\text{frame}) \geq 2 \times pd + T_d(\text{Jam Signal})$$

$$T_d(\text{frame}) \geq RTT + T_d(\text{Jam Signal})$$

$$T_d(\text{frame}) \geq 46.444 \text{ s} + 4.8 \text{ s}$$

$$T_d(\text{frame}) \geq 51.2 \text{ sec}$$

$$\frac{L}{B} \geq 51.2 \times 10^{-6} \text{ sec}$$

$$L \geq 51.2 \times 10^{-6} \text{ sec} \times B$$

$$L \geq 51.2 \times 10^{-6} \text{ sec} \times 10 \times 10^6 \text{ bits/sec}$$

$$L \geq \underline{\underline{512 \text{ bits}}}$$

Td(Jam Signal) - Jam Signal Bandwidth

$$= \frac{48 \text{ bits}}{10 \times 10^6 \text{ bits/sec}}$$

$$= 4.8 \times 10^{-6} \text{ sec}$$

$$= \underline{\underline{4.8 \text{ sec}}}$$

OR

$$L \geq (2 \times pd + T_d(\text{Jam Signal})) + B$$

$$L \geq (RTT + T_d(\text{js})) \times 8$$

$$L \geq (46.444 \text{ sec} + 4.8 \text{ sec}) \times 8$$

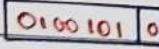
$$L \geq 51.2 \text{ sec} + B$$

$$L \geq 51.2 \times 10^{-6} \text{ sec} \times 10 \times 10^6 \text{ bits/sec}$$

$$L \geq \underline{\underline{512 \text{ bits}}}$$

Q5 Define the type of the following destination address.

CFA:30:10:21:10:1A in the Ethernet Frame Format.

 \rightarrow Unicast MAC address.

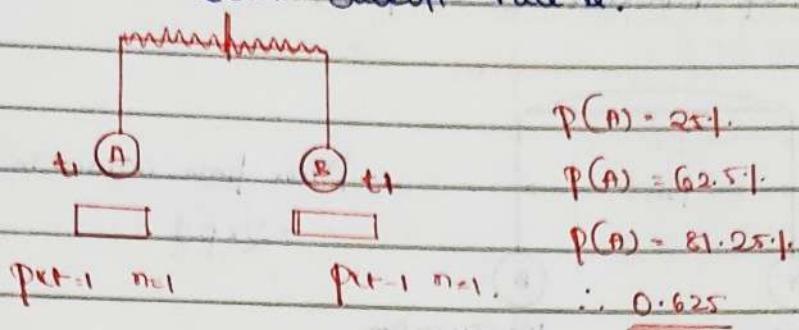
Ane

Unicast MAC address.

Q6. A and B are the only two stations on an Ethernet. Each has a steady queue of frames to send. Both A and B attempt to transmit a frame, collide and A wins the first backoff race. At the end of the successful transmission by A, both A and B attempt to transmit and again collide. The probability that

A) During the second backoff race is:

Ans.



Q7. Suppose the Round-trip propagation delay for 100 Mbps Ethernet has 24.2 usec. The network has 48 bit jamming signal thus current minimum frame size:

Ans

$$2468 \text{ bits}$$

Q8. Determine the maximum length of the cable (in Km) for transmitting data at a rate of 500 Mbps in Ethernet Local Area Frame of size 10,000 bits. Assume the Signal Speed in the cable to be 200,000 Km/sec.

Ans.

$$B = 500 \times 10^6 \text{ bits/sec}, \quad L = 10,000 \text{ bits}$$

$$V = 200,000 \text{ Km/sec}$$

$$P_d(\text{frame}) \geq 2 + p_d$$

$$\frac{L}{B} \geq 2 + \frac{d}{V}$$

$$\frac{10000 \text{ bits}}{500 \times 10^6 \text{ bits/sec}} \geq 2 + \frac{d}{200,000 \text{ Km/sec}}$$

$$\therefore d = 2 \text{ Km}$$

Q9. In an Ethernet local area network, which one of the following statements is true?

Ans

The exponential backoff mechanism reduces the probability of collision on retransmission.

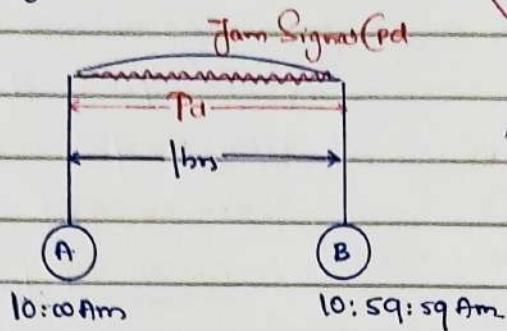
$$P(\text{Collision}) = 100\%$$

$$P(C) = 50\%$$

$$P(C) = 25\%$$

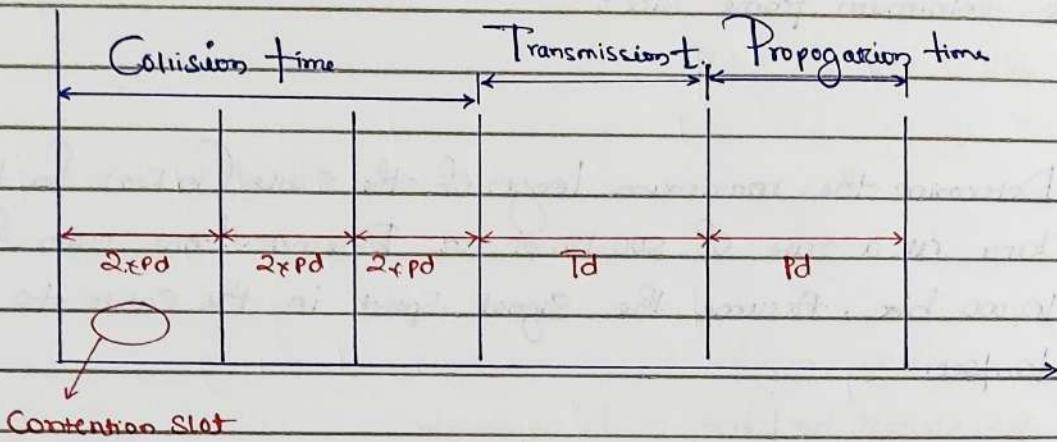
$$P(C) = 12.5\%$$

Efficiency of Ethernet (CSMA/CD)



Max time waited in one collision
 $= 2 \times p_d$

Efficiency Calculation of Ethernet (CSMA/CD)



$$\eta = \frac{\text{Useful time}}{\text{Total time}}$$

$$\eta = \frac{\text{Transmission time}}{\text{Collision time} + \text{Transmission time} + \text{Propagation time}}$$

$$\eta = \frac{T_d}{C \times 2 \times p_d + T_d + p_d} = \frac{T_d}{e \times 2 \times p_d + T_d + p_d}$$

$$\frac{p_d}{T_d} = a$$

$$\eta = \frac{T_d}{T_d [e \times 2 \times p_d + 1 + \frac{p_d}{T_d}]} \Rightarrow \frac{1}{e \times 2 \times a + 1 + a}$$

$$e = 2.72.$$

C = No. of Contention Slot

or

No. of collisions slot.

{ Continued next page! }

$$\eta = \frac{1}{2.72 \times 2.9 + 1 + a}$$

$$\eta = \frac{1}{1 + 6.44a \times \frac{d}{v} + \frac{B}{L}}$$

$$\eta = \frac{1}{5.44a + 1 + a}$$

$$\begin{cases} v - \text{fixed} \\ B - \text{fixed} \end{cases}$$

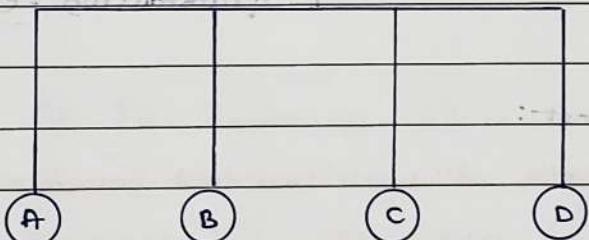
$$\boxed{\eta = \frac{1}{6.44a + 1}}$$

$d \uparrow \eta \downarrow \rightarrow$ Good for LAN not for WAN

$L \uparrow \eta \downarrow \rightarrow$ Good for larger packet size.

Note:

- ① In Ethernet efficiency is high when propagation delay is low and transmission delay is high.
- ② In ethernet efficiency is low when propagation delay is high and transmission delay is low.



→ N = Total number of stations in the ethernet.

→ p = probability of station to transfer data packet

→ $(1-p)$ = probability of station not to transfer the data packet
"For the successful transmission of one station the remaining $(N-1)$ stations should not transfer the data packet".

→ $(1-p)^{N-1}$ = probability of $(N-1)$ stations not to transfer the data packet.

→ $p(1-p)^{N-1}$ = probability of success for a single station.

→ $N \cdot p(1-p)^{N-1}$ = probability of success for any station among 'N' stations.

$$P_{\text{succ}} = N \cdot p \cdot (1-p)^{N-1}$$

→ For Max(P_{succ}): $\frac{d}{dp} (P_{\text{succ}}) = 0$

$$= \frac{d}{dp} [N \cdot p \cdot (1-p)^{N-1}] = N \left[p \cdot \frac{d}{dp} (1-p)^{N-1} + (1-p) \frac{d}{dp} p \right]$$

$$P = \frac{1}{N}$$

$$P_{\text{succ}} = N \cdot p \cdot (1-p)^{N-1}$$

$$= N \times \frac{1}{N} \left(1 - \frac{1}{N}\right)^{N-1} = \underline{\underline{\left(1 - \frac{1}{N}\right)^{N-1}}}$$

* If there are sufficiently large no. of stations i.e. $n \rightarrow \infty$
we have:

$$\lim_{N \rightarrow \infty} (P_{\text{succ}})_{\text{max}} = \lim_{N \rightarrow \infty} \left(1 - \frac{1}{N}\right)^{N-1} = \underline{\underline{e}}$$

* No. of times we need to try before getting the first success = e.

From here we conclude:

Average no. of collision that might occur before a successful transmission = e.

Q1. The efficiency of Ethernet:

Ans Increase when propagation delay is low and transmission delay is high

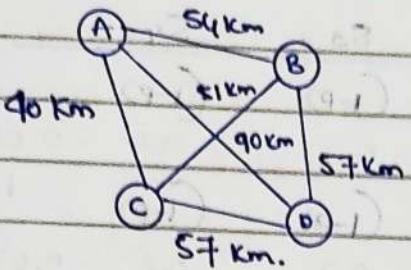
Q2. Which of the following statements is true about CSMA/CD

Ans CSMA/CD is not suitable for a high propagation delay network like satellite network.

$$n = \frac{1}{1+6.4 \mu s} = \frac{1}{1+6.4 \mu s \times \frac{P_d}{T_d}}$$

$$P_d \uparrow \downarrow \quad T_d \uparrow \downarrow$$

Q3. The network consists of 4 hosts distributed as shown below.
Assume this network uses CSMA/CD and signal travels at 3×10^8 km/sec. If send a packet at 1Mbps, what could be minimum size of the packet?



$$V = 3 \times 10^5 \text{ km/sec}$$

$$B = 1 \text{ Mbps} = 10^6 \text{ bits/sec}$$

$$L = ?$$

Ans.

$$T_d(\text{frame}) \geq 2 \times Pd + T_d(\text{jam/Signal})$$

$$Pd = \frac{d}{V}$$

$$\frac{L}{B} \geq 2 \times Pd = L \geq 2 \times Pd \times B$$

$$Pd = \frac{90 \text{ km}}{3 \times 10^5 \text{ km/sec}}$$

$$L \geq 2 \times 30 \times 10^6 \text{ bits/sec}$$

$$L \geq 2 \times 30 \times 10^6 \text{ bits}$$

$$L \geq 600 \text{ bits}$$

$$Pd = 30 \times 10^{-6} \text{ sec}$$

Q4. There are n -stations in slotted LAN. Each station attempts to transmit with a probability P in each time slot. What is the probability that only one station transmits in given time slot?

Ans.

$$N_p(1-p)^{n-1}$$

Q5 Consider a LAN with four nodes S_1, S_2, S_3 , and S_4 . Time is divided into fixed size slots, and a node can begin its transmission only at the beginning of a slot. A collision is said to have occurred if more than one node transmit in the same slot. The probability of generation of a frame in a time slot by S_1, S_2, S_3 and S_4 are 0.1, 0.2, 0.3, and 0.4 respectively. The probability of sending a frame in the first slot without any collision by any of these four stations is 0.4404.

Ans

$$S_1 = 0.1, S_2 = 0.2, S_3 = 0.3, S_4 = 0.4$$

$$P_{\text{out}} = N_p(1-p)^{n-1}$$

Explanation Continued

P.T.O!

| | S_1 | S_2 | S_3 | S_4 | |
|-----------|---------|---------|---------|---------|------------|
| For S_1 | P | $(1-P)$ | $(1-P)$ | $(1-P)$ | |
| | 0.1 | 0.8 | 0.7 | 0.6 | $= 0.0326$ |
| For S_2 | $(1-P)$ | P | $(1-P)$ | $(1-P)$ | + |
| | 0.9 | 0.2 | 0.7 | 0.6 | $= 0.0756$ |
| For S_3 | $(1-P)$ | $(1-P)$ | P | $(1-P)$ | + |
| | 0.9 | 0.8 | 0.3 | 0.6 | $= 0.1296$ |
| For S_4 | $(1-P)$ | $(1-P)$ | $(1-P)$ | P | + |
| | 0.9 | 0.8 | 0.7 | 0.4 | $= 0.2016$ |

0.4404

Q6 Suppose CSMA/CD protocol is used for channel access in an Ethernet LAN and 3 hosts are in LAN. Each host can transmit data in an idle slot (Empty Slot) with probability 0.8. What is the probability that only one host can transmit data in an idle slot?

Ans

$$\text{No. of hosts (N)} = 3$$

Each host can transmitting probability (P) = 0.8

Probability that one host transmits data in an idle slot
(Throughput of the channel) = $N \cdot P \cdot (1-P)^{N-1}$

$$= 0.3 \times 0.8 \times (0.2)^2$$

$$= 0.3 \times 0.8 \times 0.2 \times 0.2$$

$$= \underline{\underline{0.096}}$$

Q7. Suppose CSMA/CD protocol is used for channel access in an Ethernet LAN and each host can transmit data in an idle (Empty) slot with probability 0.75. The total no. of hosts exists in the LAN. When probability that particular host only can transmit in an idle slot is 0.1875.

Ans

Each host can transmit data in a idle host (P) = 0.75

$$\text{Total no. of host in LAN} = N$$

Probability that particular host only transmit in an idle slot

(Throughput of host) = 0.1875.

$$\text{Throughput of the host} = p(1-p)^{N-1}$$

$$0.1875 = 0.75 \times (0.25)^{N-1}$$

N=2

Note: * Throughput of host = $p(1-p)^{N-1}$

* Throughput of the channel = $Np(1-p)^{N-1}$.

Q9. Consider a Simplified time Slotted MAC protocol, where each host always has desire to send and transmit with probability $p=0.2$ in every slot. There is no backoff and one frame can be transmitted in one slot. If more than one host transmits in the same slot, then the transmission are unsuccessful due to collisions. What is the maximum no. of hosts which this protocol can support, if each host has to be provided a minimum throughput of 0.16 frames per time slot.

Ans.

$$P=0.2$$

$$\text{No of host} = N$$

$$\text{Throughput of host} = 0.16$$

$$\text{Throughput of the host} = p(1-p)^{N-1}$$

$$0.16 = 0.2(0.8)^{N-1}$$

$$0.8 = (0.8)^{N-1}$$

$$(0.8)' = (0.8)^{N-1}$$

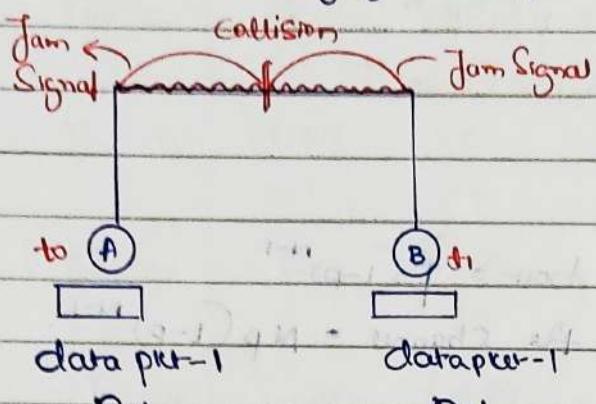
$$N-1 = 1$$

N=2

Q8. Suppose two nodes, A and B are attached to opposite end of the cable with propagation delay of 125 μsec. Both nodes attempt to transmit at time $t=0$. Frame collide and after first collision, A draws $k=0$ and B draws $k=1$ in the exponential backoff protocol. At what time (in 4 seconds) is the packet completely delivered at B, if Bandwidth of the link is 10Mbps and packet size is 1000 bits for the following:

- (a) with purging — 4usec. (b) without purging — 4sec.

Concept of Purging (Cleaning)



$$K \rightarrow Q \rightarrow S^{-1}$$

$$t \mapsto (0,1)$$

$$K \rightarrow O \oplus S^{-1}$$

$$k \rightarrow (0,1)$$

A B

O O → Collision

$$0 \rightarrow a_{\text{wpo}}$$

$$10 \rightarrow B_{1280}$$

$\downarrow \downarrow \rightarrow \text{GDNiCo}$

If we choose $\begin{pmatrix} 0 & 1 \\ k & k \end{pmatrix}$

WT of $A = k^*$ slot duration

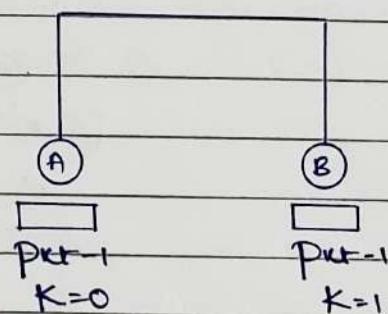
WT of A = 0 \times Slot duration

WT of A = 0

WT of B = K⁺ slot duration

= $\frac{1}{\text{Slot duration}}$

Concept of Purging (Cleaning)

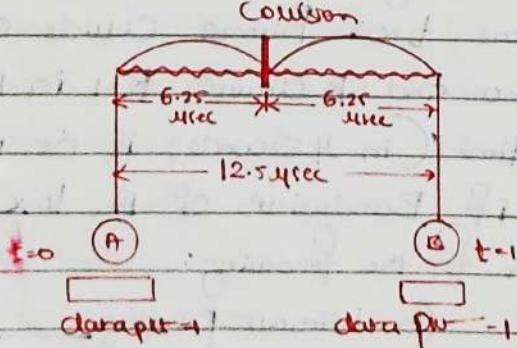


$$WT \text{ of } A = pd$$

WT OF B = K⁺stor duration

F | * slot duration

Ans 8th.

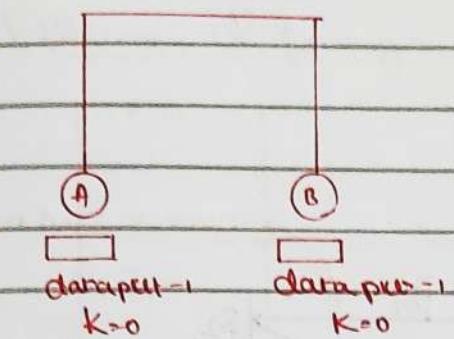


→ At $t=0$ both A & B start transmitting the clear pr.

→ At $t = 6.25$ both A & B data plot has been collided

been colluded

→ At $t = 12.5$ both received collision signal



$$WT = Pd$$

$WT = 12.5 \mu\text{sec}$ → A can't immediately go, has to wait for one proposal delay.

$$t = 12.5 \mu\text{sec} + 12.5 \mu\text{sec} = 25 \mu\text{sec}$$

At $t = 25 \mu\text{sec}$ A starts retransmitting the data pkt.

$$\text{Pkt size} = 1000, B = 10 \times 10^6 \text{ bits/sec}$$

$$T_d(\text{pkt}) = \frac{1000 \text{ bits}}{10 \times 10^6 \text{ bits/sec}}$$

$$= 100 \times 10^{-6} \text{ sec} = 100 \mu\text{sec}$$

$$At t = 25 \mu\text{sec} + 100 \mu\text{sec} = 125 \mu\text{sec}$$

$$At t = 125 \mu\text{sec}$$

A completes its transmission.

→ $t + t = 125 \mu\text{sec} + 125 \mu\text{sec} = 250 \mu\text{sec}$. At packet completely delivered to B

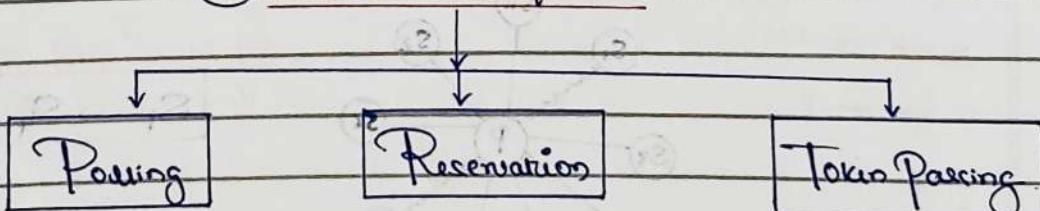
Controlled Access Protocols

It can be done in the following two ways:

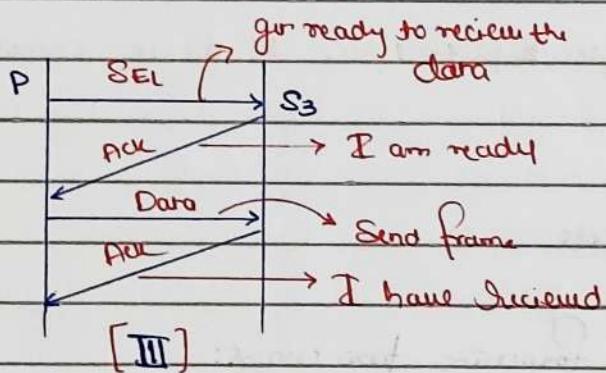
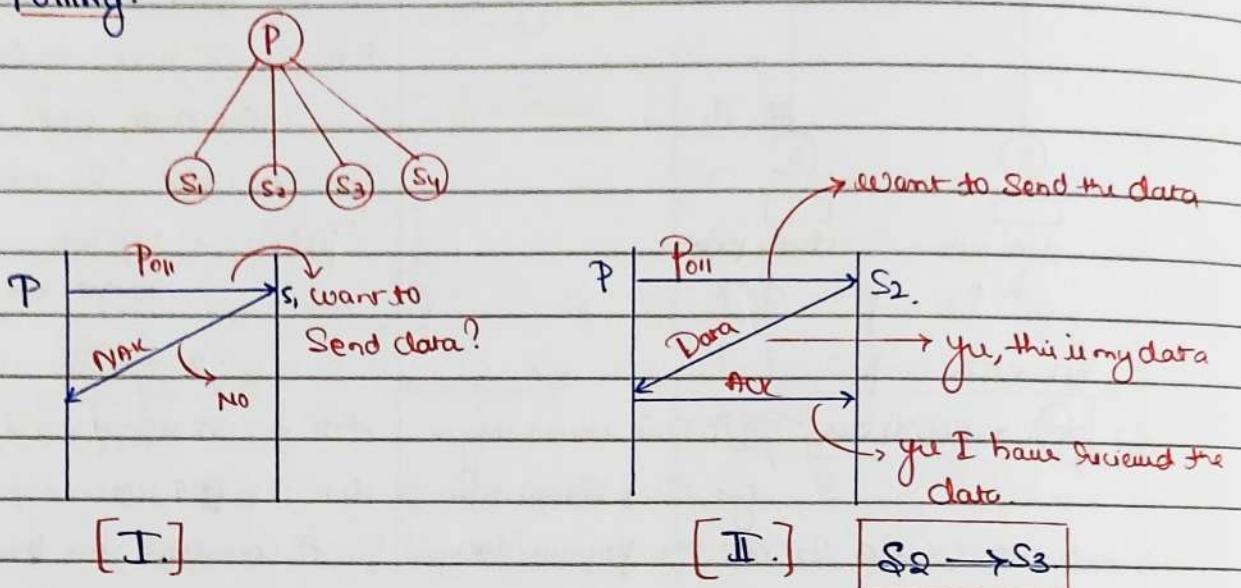
1. We have a concept of primary and secondary stations. Primary stations will control all secondary stations.
2. If concept of primary or secondary station is missing then if any station want to send the data, it can send only if all other stations give permissions to it.

Note: Controlled access protocols are collision free protocol.

Controlled Access Protocols

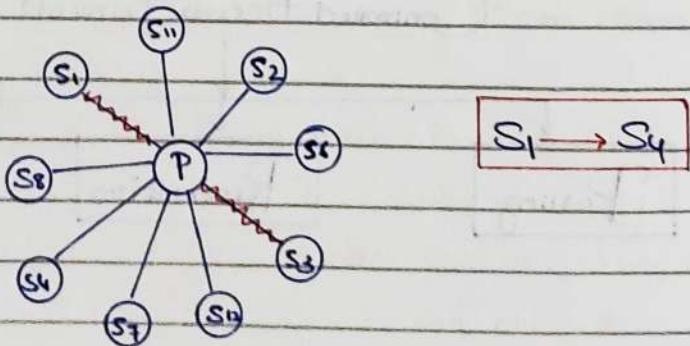


Polling:

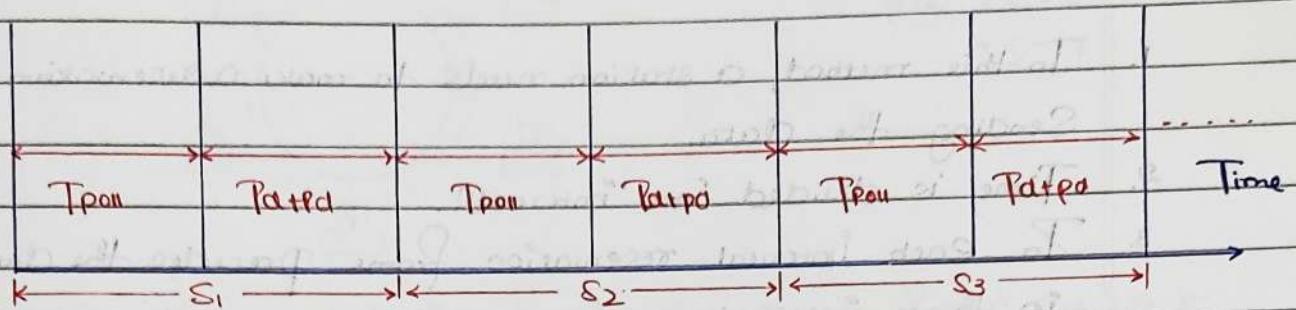


Note:

- * Every station will send the data through primary station.
- * Two Secondary Stations cannot communicate directly.
- * Common topology used in polling mechanism is Star topology.
- * Bandwidth utilization is low because lot of time is wasted by sending the Poll message.
- * Drawback of Polling is if primary station fails, the system goes down.



Efficiency of Polling:



$$\text{efficiency} = \frac{\text{useful time}}{\text{total time}}$$

$$\text{Throughput} = \eta \times B.$$

$$\text{efficiency} = \frac{T_d}{T_{poll} + T_d + T_{pd}}$$

- Q1. A broadcast channel has 10 nodes and total capacity of 10 Mbps. It uses Polling for medium access. Once a node finishes transmission, there is a polling delay of 80 μsec to poll the next node. Whenever a node is polled, it is allowed to transmit a maximum of 100 bytes. The maximum throughput of the broadcast channel is :

Ans.

$$B = 10 \text{ Mbps}$$

$$T_{poll} = 80 \mu\text{sec}$$

$$\text{Frame size} = 100 \text{ Byte}$$

$$T_d = \frac{\text{Frame size}}{\text{Bandwidth}} = \frac{800 \times 8 \text{ bits}}{10 \times 10^6 \text{ bits/sec}} = 800 \times 10^{-6} \text{ sec} = 800 \mu\text{sec}$$

$$\eta = \frac{\text{useful time}}{\text{total time}} = \frac{T_d}{T_{poll} + T_d + T_{pd}}$$

$$\text{Throughput} = \eta \times B$$

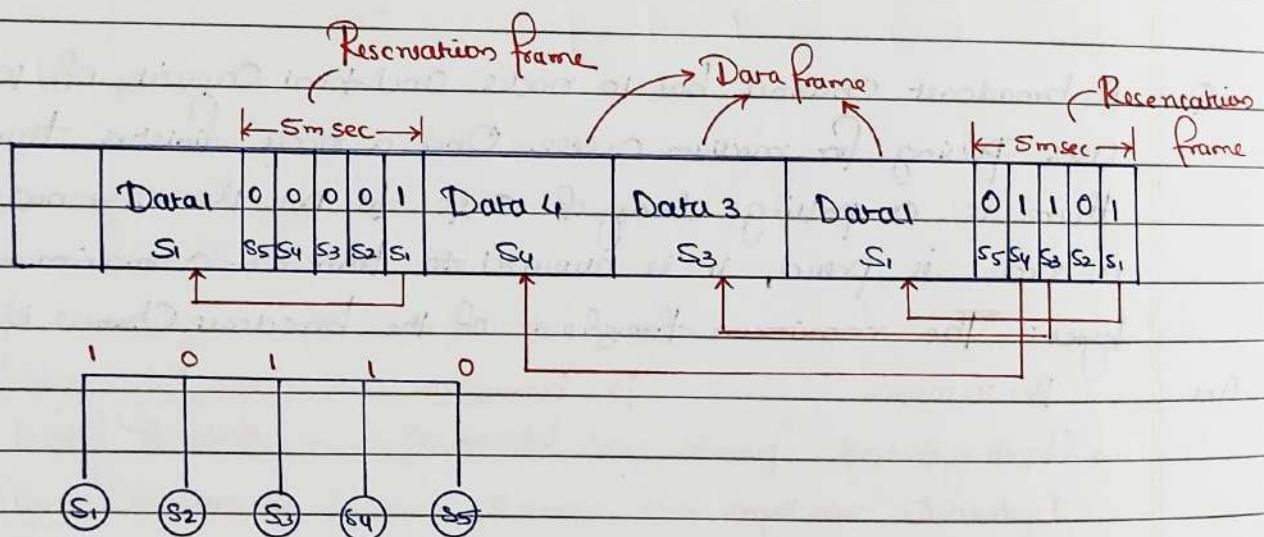
$$= \frac{800 \mu\text{sec}}{800 \mu\text{sec} + 800 \mu\text{sec}} = \frac{10 \times 10^6 \text{ bits/sec}}{11} = 10 \times 10 \text{ Mbps}$$

$$= \frac{10}{11} \text{ Mbps} = \frac{10}{11} \text{ Mbps}$$

$$\Rightarrow \frac{100}{11} \text{ Mbps}$$

Reservation:

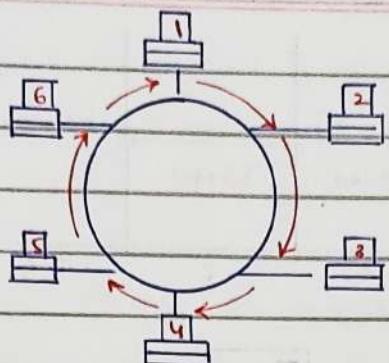
1. In this method, a station needs to make a reservation before sending the data.
2. Time is divided into intervals.
3. In each interval reservation frame precedes the data frame sent in that interval.
4. If there are N stations in the system, there are exactly N reservation minislots in the reservation frame. Means every station has its own minislot.
5. The stations that have made reservations can send their data frames after the reservation frame.



* In the above example we have 5 stations and 5 minislots in the reservation frame. In the first interval only 1, 3 and 4 have made reservations. In the second interval only 1 station has made reservation.

Token Passing:

1. All the stations are logically connected to each other in the form of ring.
2. It uses a special frame called "token" that travels around the ring.



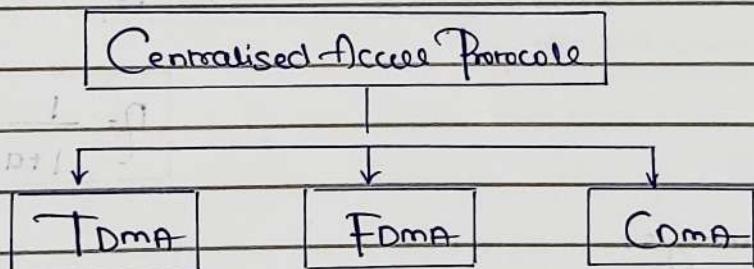
* Priority = 3 bit
 Range = $0 - 2^3 - 1$
 $= 0 - 7.$

3. A station is allowed to transfer the data packet if and only if it has token.
4. Whenever Station has no more data to send, it release the token.

Note:

- * Best technique for broadcasting
- * No acknowledgement.

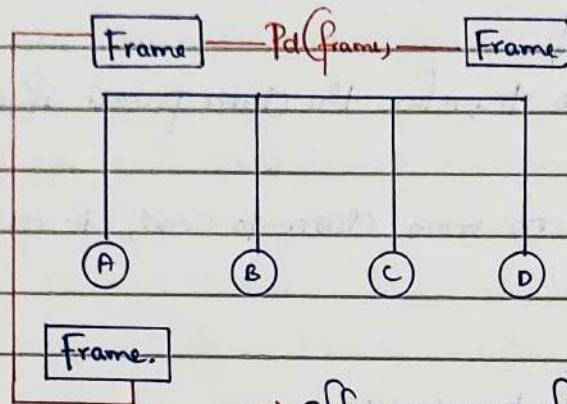
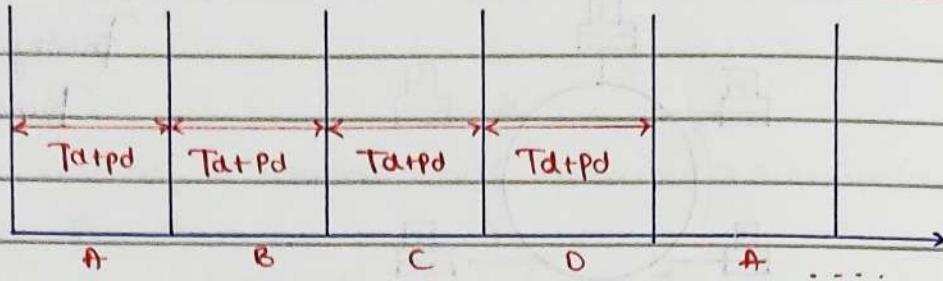
Centralized Access Protocol



TDMA (Time division multiple access).

In time division multiple access:

- * Time of the link is divided into fixed sized intervals called as time slots.
- * Time slots are allocated to the stations in round robin manner.
- * Each station transmits its data during the time slot allocated to it.
- * In case, station does not have any data to send, its time slot goes waste.



$\rightarrow \text{efficiency} = \frac{\text{useful time}}{\text{total time}}$

$$\therefore \text{efficiency} = \frac{T_d}{T_d + p_d} = \frac{T_d}{T_a [1 + \frac{p_d}{T_d}]}$$

$$\eta = \frac{1}{1+a}$$

$$\left\{ \begin{array}{l} p_d - a \\ T_d \end{array} \right.$$

Disadvantages:

- * If any Station does not have data to send during its time slot, then its time slot goes waste.
- * This reduce the efficiency.
- * This time slot could have been allocated to some other Station willing to send data.

Note: * Effective bandwidth / bandwidth, utilization / throughput

$$\text{Throughput} = \text{Efficiency} * \text{Bandwidth}$$

* Maximum available effective bandwidth (throughput)

$$= \text{Total no. of Stations} * \text{Bandwidth requirement of 1 station.}$$

Q1. If transmission delay and propagation delay of a packet in TDM Time division multiplexing is 1 msec each at 8Mbps bandwidth, then,

- What is the efficiency?
- Find the effective bandwidth/throughput?
- How many maximum stations can be connected to the network if each station requires 4Kbps bandwidth?

Ans.

$$T_d = 1 \text{ msec}$$

$$P_d = 1 \text{ sec}$$

$$B = 8 \text{ Mbps} = 8 \times 10^6 \text{ bps/sec}$$

$$\eta = \frac{T_d}{T_d + P_d} = \frac{1}{1+1} = \frac{1}{2}$$

$$\therefore \underline{\eta = 50\%} \quad (i)$$

$$(ii) \text{ Throughput} = \eta \times B$$

$$= \frac{1}{2} \times 8 \times 10^6$$

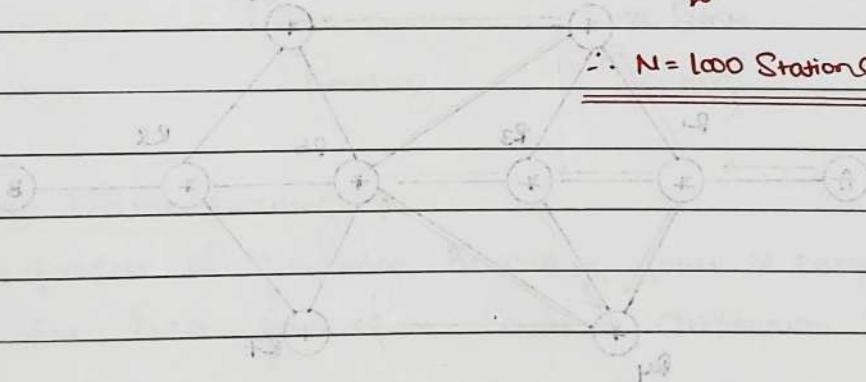
$$= \underline{\underline{4 \text{ Mbps}}}$$

$$(iii) N \times 4 \text{ Kbps} = 4 \text{ Mbps}$$

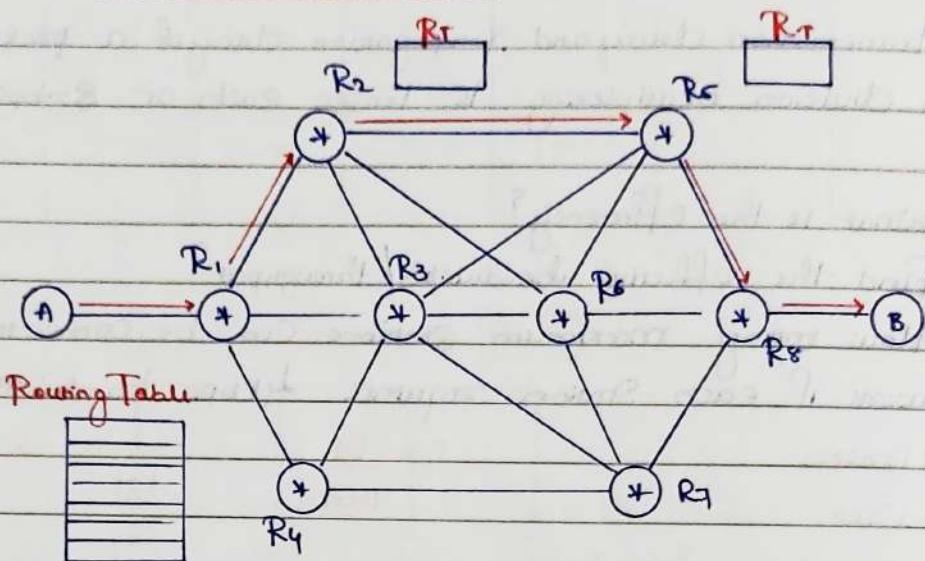
$$N = \frac{4 \text{ Mbps}}{4 \text{ Kbps}}$$

$$N = \frac{10^6}{10^3} = 1000$$

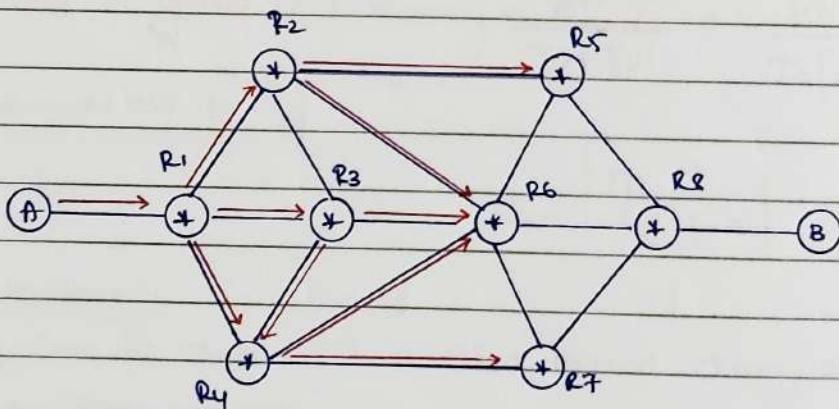
$$\therefore \underline{\underline{N = 1000 \text{ Station}}}$$



ROUTING PROTOCOLS



Flooding: Flooding is simple computer network routing algorithm in which every incoming packet is sent through every outgoing link except one it arrived on.



Advantages of Flooding:

- * No routing is required
- * Shorter Path is always guaranteed i.e. the packet arrives at destination first.
- * It is highly reliable, if one path is down then the packet reaches at the destination by choosing another path.

Disadvantages: * Traffic is very high

- * Many duplicate packets received by recipient.

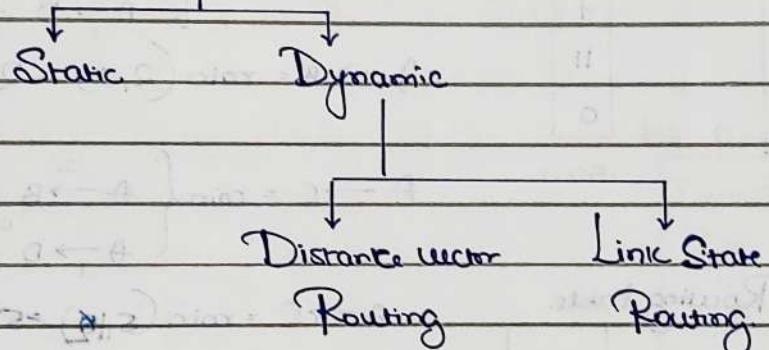
Advantages of Routing:

- * Traffic is very less.
- * No duplicate packet received by the receiver.

Disadvantage of Routing:

- * Routing table is required
- * Chosen path may be down so it is not highly reliable.
- * Shortest path is depends on the algorithm and some algorithms fail to find the shortest path.

Routing Algorithm



Distance Vector Routing (1980)

- * The process of preparing the routing table at every router and finding the best path from source to destination is called "Routing".

Step 1: Prepare the routing table at every Router based on local knowledge.

| Dest | Distr | NH | | Dest | Distr | NH |
|------|-------|----|--|------|----------|----|
| A | 1 | A | | A | ∞ | - |
| B | 7 | B | | B | 3 | B |
| C | 4 | C | | C | 0 | C |
| D | 0 | D | | D | 11 | D |

| Dest | Dis. | NH |
|------|------|----|
| A | 0 | A |
| B | 2 | B |
| C | ∞ | - |
| D | 1 | D |

| Dest | Dis. | NH |
|------|------|----|
| A | 2 | A |
| B | 0 | B |
| C | 3 | C |
| D | 7 | D |

Step 2: calculate new routing table?

At A

A received distance vector from B, D

| From B | From D |
|--------|--------|
| 2 | 1 |
| 0 | 7 |
| 3 | 11 |
| 7 | 0 |

$$AB = 2$$

$$AD = 1.$$

$$A \rightarrow B = \min \left\{ \begin{array}{l} A \xrightarrow{2} B + B \rightsquigarrow B \\ \text{or} \\ A \xrightarrow{1} D + D \rightsquigarrow B \end{array} \right. \quad A \rightarrow B = \min(2, 8) = 2.$$

$$A \rightarrow C = \min \left\{ \begin{array}{l} A \xrightarrow{2} B + B \xrightarrow{3} C \\ \text{or} \\ A \xrightarrow{1} D + D \xrightarrow{11} C \end{array} \right. \quad A \rightarrow C = \min(5, 12) = 5$$

A - New Routing table.

| Destination | Distance | NH |
|-------------|----------|----|
| A | 0 | A |
| B | 2 | B |
| C | 5 | B |
| D | 1 | D |

$$A \rightarrow D = \min \left\{ \begin{array}{l} A \xrightarrow{2} B + B \xrightarrow{7} D \\ \text{or} \\ A \xrightarrow{1} D + D \rightsquigarrow D \end{array} \right. \quad A \rightarrow D = \min(9, 1) = 1$$

Shortcut (AD Rule)

At A : A received distance vector from B, D

From-B

From-D

| | |
|-------|--|
| 2 | |
| 0 | |
| 3 | |
| 7 | |
| 0+2=2 | |
| 3+2=5 | |
| 7+2=9 | |

$$AB = 2$$

$$3+2=5$$

$$7+2=9$$

From-D

| | |
|---------|--|
| 1 | |
| 7 | |
| 11 | |
| 0 | |
| 7+1=8 | |
| 11+1=12 | |
| 0+1=1 | |

A - New Routing Table

| Destination | Distance | NH |
|-------------|----------|----|
| A | 0 | A |
| B | 2 | B |
| C | 5 | B |
| D | 1 | D |

A+B

B received distance vector from A, C, D

B-New Routing Table

| From-A | From-C | From-D |
|--------|--------|--------|
| 0 | ∞ | 1 |
| 2 | 3 | 7 |
| ∞ | 0 | 11 |
| 1 | 11 | 0 |

$BA = 2$
 $0+2=2$
 $∞+2=∞$
 $1+2=3$

$BC = 3$
 $∞+3=∞$
 $0+3=3$
 $11+3=14$

$BD = 7$
 $1+7=8$
 $11+7=18$
 $0+7=7$

| Destination | Distance | NH |
|-------------|----------|----|
| A | 2 | A |
| B | 0 | B |
| C | 3 | C |
| D | 3 | A |

A+C: New Routing Table

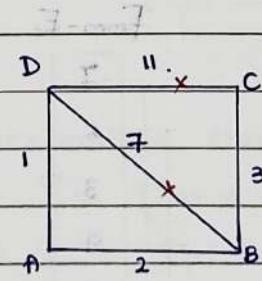
| Destination | Dist. | NH |
|-------------|-------|----|
| A | 5 | B |
| B | 3 | B |
| C | 0 | C |
| D | 10 | B |

A+D: New Routing Table

| Destination | Distance | NH |
|-------------|----------|----|
| A | 1 | A |
| B | 3 | A |
| C | 10 | B |
| D | 0 | D |

Final Routing table in One Step

| Dest. | Dist. | NH |
|-------|-------|----|
| A | 1 | A |
| B | 3 | A |
| C | 0 | C |
| D | 0 | D |

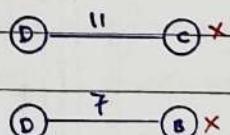


| Dest. | Dist. | NH |
|-------|-------|----|
| A | 5 | B |
| B | 3 | B |
| C | 0 | C |
| D | 6 | D |

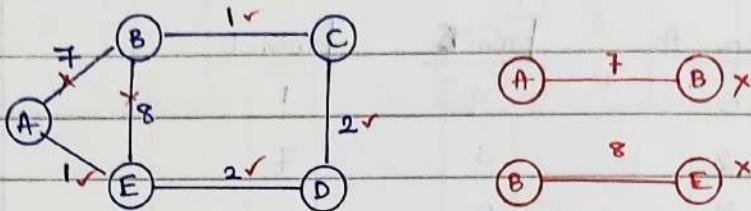
"edges which are
not included in
any routing
table"

| Dest. | Dist. | NH |
|-------|-------|----|
| A | 0 | A |
| B | 2 | B |
| C | 5 | B |
| D | 1 | D |

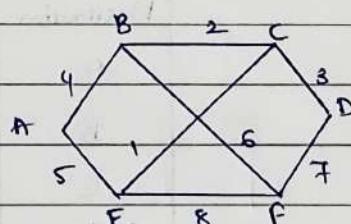
| Dest. | Dist. | NH |
|-------|-------|----|
| A | 2 | A |
| B | 0 | B |
| C | 3 | C |
| D | 3 | A |



Q1. Consider the following subnet. If distance vector routing is used, how many link can never be used after all the routing table are stabilized?



Q2. Consider the network of Figure. Distance Vector Routing is used and the following vectors have just come in to router C: from B: (5, 0, 8, 12, 6, 2); from D: (16, 12, 6, 0, 9, 10); and from E: (7, 6, 3, 9, 0, 4). The cost of links from C to B, D, and E, are 6, 3 and 5 respectively. What is C's new routing table? Give both the outgoing link to use and the cost.



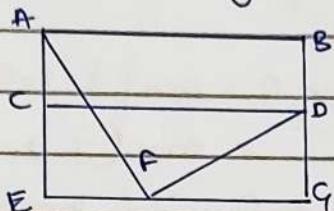
Ans: At C

* C Received Distance Vector from B, D, E.

C - New Routing Table

| From - B | From D | From E | Destination | Distance | NH |
|-------------|--------|--------|-------------|----------|----|
| 5 | 16 | 7 | A | 11 | B |
| 0 | 12 | 6 | B | 6 | B |
| 8 | 6 | 3 | C | 0 | C |
| 12 | 0 | 9 | D | 3 | D |
| 6 | 9 | 0 | E | 5 | E |
| 2 | 10 | 4 | F | 8 | B |
| <hr/> | | | | | |
| CB = 6 | | | | | |
| 5 + 6 = 11 | | | | | |
| 0 + 6 = 6 | | | | | |
| 12 + 6 = 18 | | | | | |
| — | | | | | |
| 6 + 6 = 12 | | | | | |
| 2 + 6 = 8 | | | | | |
| <hr/> | | | | | |
| CD = 3 | | | | | |
| 16 + 3 = 19 | | | | | |
| 12 + 3 = 15 | | | | | |
| 0 + 3 = 3 | | | | | |
| 9 + 3 = 12 | | | | | |
| 10 + 3 = 13 | | | | | |
| <hr/> | | | | | |
| CE = 5 | | | | | |
| 7 + 5 = 12 | | | | | |
| 6 + 5 = 11 | | | | | |
| 9 + 5 = 14 | | | | | |
| 0 + 5 = 5 | | | | | |
| 4 + 5 = 9 | | | | | |

Q3. For the network given in the table below, the routing table of the four nodes A, E, D and G are shown. Suppose that F has estimated its delay to its neighbours A, E, D and G as 8, 10, 12, and 6 msec respectively and update its routing table using distance vector routing technique. New Routing table for F?



Ans. At F

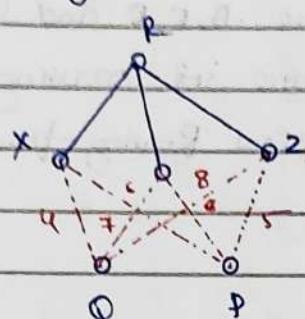
F received Distance Vector from A, D, E, G

| From-A | From-D | From-E | From-G | F → New Routing Table |
|------------|--------|--------|--------|--------------------------|
| 0 | 20 | 24 | 21 | Destination Distance Nbr |
| 140 | 8 | 23 | 24 | A 8 A |
| 14 | 30 | 7 | 22 | B 20 D |
| 7 | 0 | 20 | 19 | C |
| 21 | 14 | 0 | 22 | D |
| 9 | 7 | 11 | 10 | E |
| 24 | 22 | 22 | 0 | F 6 F |
| $F_A = 8$ | | | | G |
| $0+8=8$ | | | | |
| $(4+8)=12$ | | | | |
| $20+2=22$ | | | | |
| $8+2=20$ | | | | |
| $F_D = 12$ | | | | |
| $20+12=32$ | | | | |
| $24+10=34$ | | | | |
| $27+$ | | | | |
| $10=37$ | | | | |
| $F_E = 10$ | | | | |
| $24+10=34$ | | | | |
| $27+$ | | | | |
| $10=37$ | | | | |
| $F_G = 6$ | | | | |
| $21+6=27$ | | | | |
| $24+6=30$ | | | | |

Q4. Consider a Computer network using the distance vector routing algorithm in its network layer. The partial topology of the network is shown below. The objective is to find the shortest-cost path from router R to routers P and Q. Assume that R does not initially know the shortest route to P and Q. Assume that R has three neighbouring routers denoted as X, Y, and Z. During one iteration, R measures its distance to its neighbours X, Y, and Z as 3, 2, and 5 respectively. Router R gets routing vectors from its neighbours that indicate that

The distance to router P from routers X, Y and Z are 7, 6 and 8 respectively.

Ans



$$[I] R \rightarrow P = \min \{ R-X-P, R-Y-P, R-Z-P \}$$

$$= \min (10, 8, 10)$$

$$R \rightarrow P = 8 \text{ (Through Y)}$$

$$[II] R \rightarrow Q = \min \{ R-X-Q, R-Y-Q, R-Z-Q \}$$

$$= \min (7, 18, 13)$$

$$R \rightarrow Q = 7 \text{ (Through X)}$$

Qs The routing vector also indicate that the distance to router Q from routers X, Y, and Z are 4, 6, and 8 respectively. Which of the following statement(s) are correct with respect to new routing table of R, after updating during its iteration?

Ans

The next hop router from for a packet from R to P is Y.

The distance from R to Q will be stored as 7.

Disadvantage of DSR [Count-to-infinity problem]

Bad news spreads slow

Good news spreads fast

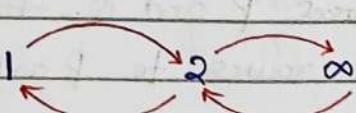
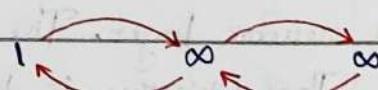
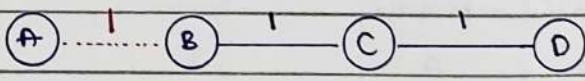
Good News.

Initially A is not connected to B so

$$B \rightarrow A = \infty$$

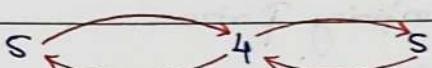
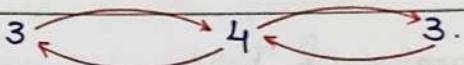
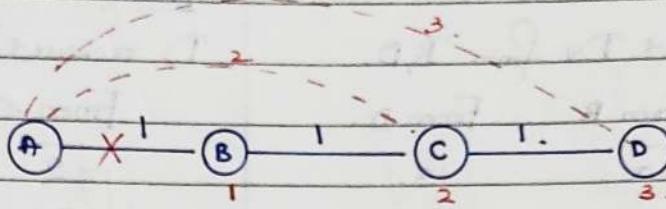
$$C \rightarrow A = \infty$$

$$D \rightarrow A = \infty$$



* After sometime A is connected to B with the cost(1).

1 2 3
(Good News)

Bad News

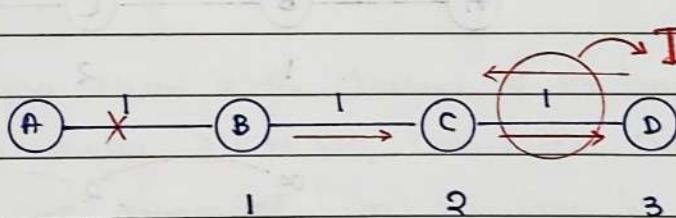
5 6 5
⋮ ⋮ ⋮
∞ ∞ ∞

"Count to infinity"
Problem!

| Dest | Direc. | NH |
|------|----------|---------------|
| A | ∞ | $\frac{A}{C}$ |
| B | 3 | |

| Dest | Direc. | NH |
|------|--------|----|
| A | 2 | B |
| B | 4 | 0 |

| Dest. | Direc. | NH |
|-------|--------|----|
| A | 3 | C |
| B | | |



Infinite Looping

1 2 3

3 4 3
⋮ ⋮ ⋮

Note:

A+B

B received

| Dest | Direc. | NH |
|------|----------|---------------|
| A | ∞ | $\frac{A}{C}$ |
| B | 3 | C |

| Dest | Direc. | NH |
|------|--------|----|
| A | 2 | B |
| B | 4 | D |

| Dest. | Direc. | NH |
|-------|--------|----|
| A | 3 | C |
| B | | |

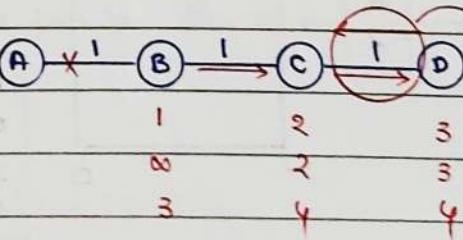
distance vector

from - C.

From C

$$\boxed{2} \quad BC=1$$

$2+1=3$



Infinite Looping

1 2 3
∞ 2 3
3 4 4

At C

C received DV from B, D.

From B

 ∞ $C_B = 1$ $A_B + 1 = \infty$

From D.

3.

 $C_D = 1$ $A_D + 1 = 4$ At D

D received from C.

From C

2

 $D_C = 1$ $A_D + 1 = 3$ Disadvantage of DVR

- * Count to infinity problem
- * Infinite looping
- * Convergence is very slow.

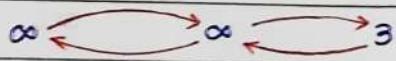
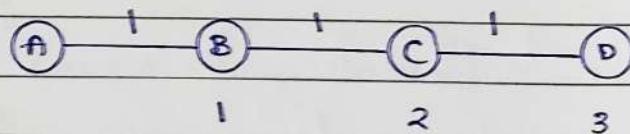
Note: Solution of Count to infinity problem is given by Split Horizon.

Split Horizon Solution.

| Dest | Dvr | NH |
|------|----------|----|
| A | ∞ | - |
| B | 1 | - |
| C | - | - |

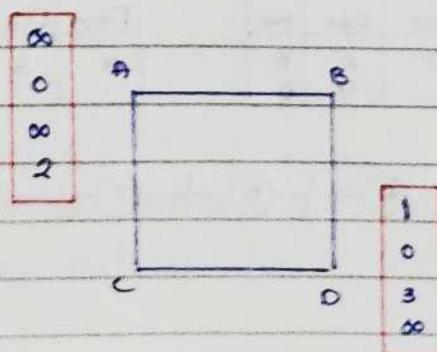
| Dest. | Dvr. | NH |
|-------|------|----|
| A | 1 | B |
| B | 2 | - |
| C | - | - |

| Dest. | Dvr | NH |
|-------|-----|----|
| A | 3 | C |
| B | - | - |
| C | - | - |



∞ ∞ ∞

Q1.



Routing Table of B.

| Dest | Dvr | NH |
|------|-----|----|
| A | 1 | A |
| B | 0 | B |
| C | 3 | A |
| D | 2 | D |

What Distance Vector 'B' will send to 'A' and 'B' by using Split Horizon Concept?

Note:

1. Count to infinity Problem
2. Infinite looping Problem

→ solved by split horizon.

* Convergence Problem is not solved by Split horizon, to solve we use Link State Routing.

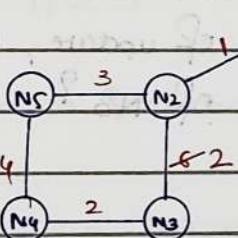
Q2. Consider the network with five nodes, N1 to N5. The network uses a Distance Vector Routing Protocol. Once the route has stabilized the distance vectors at different nodes are as follows:

$$N_1: (0, 1, 7, 8, 4)$$

$$N_2: (1, 0, 2, 7, 3)$$

$$N_3: (7, 6, 0, 2, 6)$$

$$N_4: (8, 7, 2, 0, 4)$$



$$N_5: (4, 3, 6, 4, 0)$$

Each distance vector is the distance of the best known path at the instance to node, N1 to N5, where the distance to itself is 0. Also, all links are symmetric and the cost is identical in both directions. In each round, all nodes exchanged their distance vectors with their respective neighbors. Thus all nodes update their distance vector. In between two rounds, any change in cost of a link will cause the two incident nodes to change only that entry in their distance vectors.

#Q The cost of link N2-N3 reduce to 2 (in both directions). After the next round of update, what will be the new distance vector at node, N3?

Ans

At N3

N3 received distance vector from N2, N4.

From - N2

From - N4

N3 New Routing Table

| 1 | 8 | |
|---|---|--|
| 0 | 7 | |
| 2 | 2 | |
| 7 | 0 | |
| 3 | 4 | |

$$N_3 N_2 = 2$$

$$1+2=3$$

$$0+2=2$$

$$7+2=9$$

$$3+2=5$$

| 1 | 8 | |
|---|---|--|
| 0 | 7 | |
| 2 | 2 | |
| 7 | 0 | |
| 3 | 4 | |

$$N_3 N_4 = 2$$

$$8+2=10$$

$$7+2=9$$

$$0+2=2$$

$$4+2=6$$

| Dest. | Dist. | NH |
|-------|-------|----|
| N1 | 3 | N2 |
| N2 | 2 | N2 |
| N3 | 0 | N3 |
| N4 | 2 | N4 |
| N5 | 5 | N2 |

$$\therefore \underline{(3, 2, 0, 2, 5)}$$

- #Q. After the update in the previous question, the link N1-N3 goes down. N2 will reflect this change immediately in its distance vector as cost 0. After the next round of update, what will be the cost to N1 in the distance vector of N3?

Ans N3

N3 Received DV From N2, N4

N3 - New Routing Table

From N2

From N4

| |
|---|
| ∞ |
| 0 |
| 2 |
| 7 |
| 3 |

$$N_3 N_2 = 2$$

$$0+2=\infty$$

| |
|---|
| 8 |
| 7 |
| 2 |
| 0 |
| 4 |

$$N_3 N_4 = 2$$

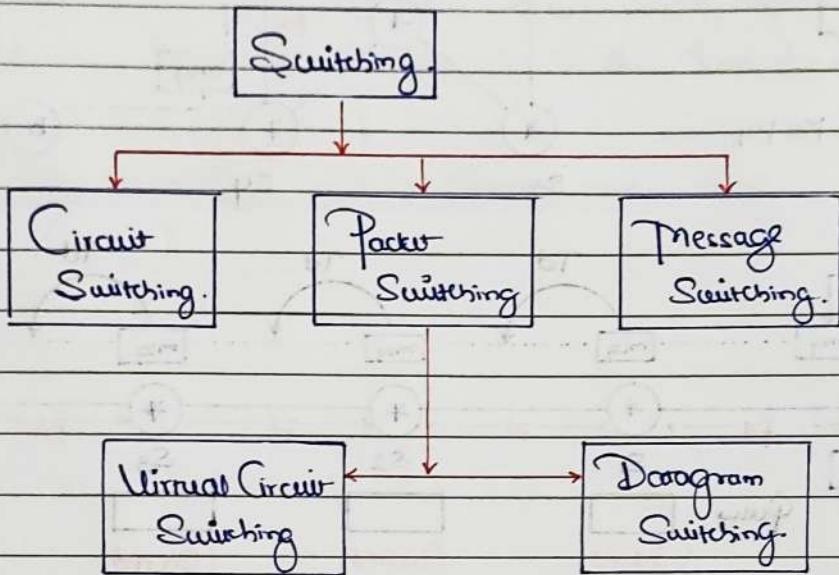
$$8+2=10$$

| Dest. | Dist. | NH |
|-------|-------|----|
| N1 | 10 | N4 |
| N2 | | |
| N3 | 0 | N3 |
| N4 | | |
| N5 | | |

$$\therefore \underline{\text{Ans} = 10}$$

SWITCHING.

Switching: The process of forwarding packets from one port to another port is called switching.

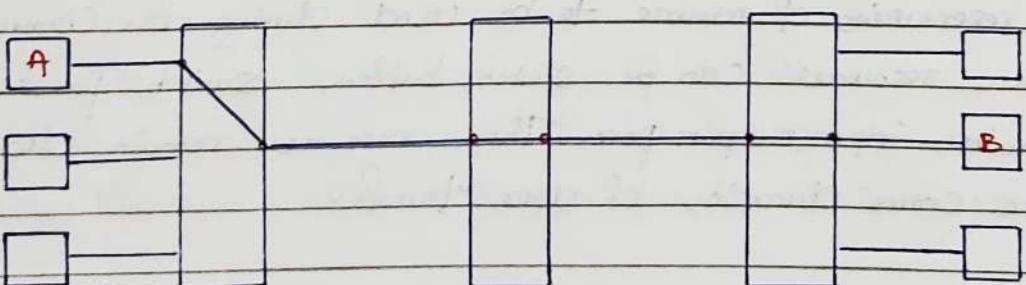


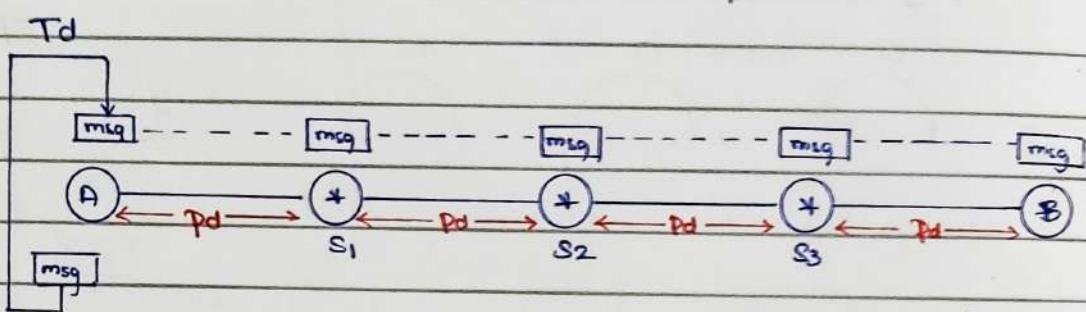
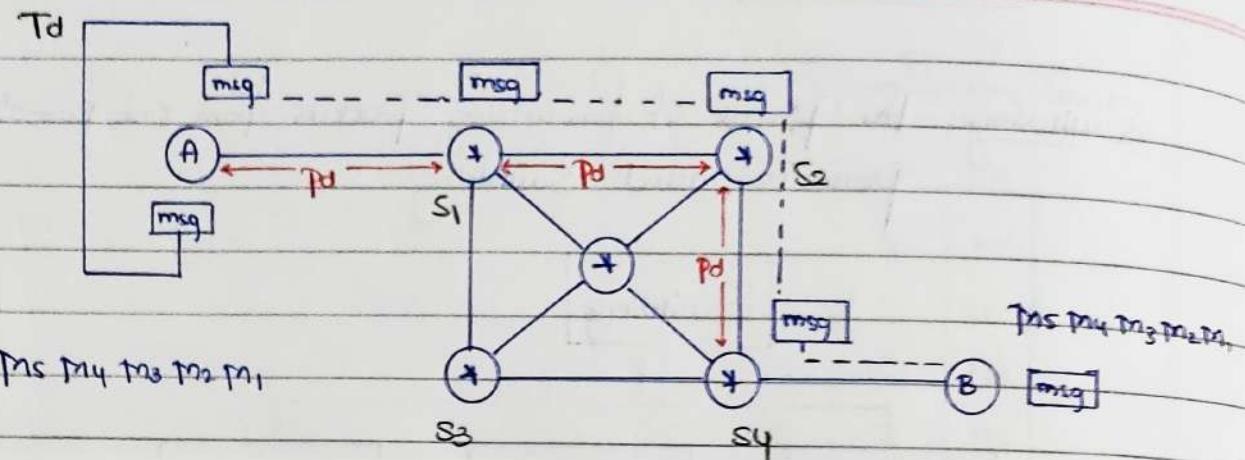
- * Switching is done at Network layer but circuit switching is not done at Network layer.
- * Circuit switching was designed for telephone network.
- * When circuit switching was invented there was no concept of osi layer or TCP/IP layer.

Circuit Switching:

The communication in a circuit switched network take place in 3 phases:

1. Circuit establishment or setup phase
2. Data transfer phase
3. Circuit disconnects or teardown phase





Total time taken to send msg from source to destination
 \Rightarrow Setup time + Transmission time + Propagation time +
 Tear down time

$$\text{Total time} = S + \frac{m}{B} + \frac{x.d}{v} + T$$

Msg size = M
 Bandwidth = B
 Velocity = v
 No. of hops = x
 Length of each hop = d

I.

Circuit Establishment or Setup Phase:

- * In Circuit Switched network before actual data transfer take place a dedicated circuit or physical path is established between sender and receiver.
- * The dedicated path existing between sender and receiver is maintained for entire duration of connection.
- * Before starting the connection/communication the station must make a reservation of resource to be used during the communication.
- * These resources can be switch, buffer, switch processing time, switch input output port. These resources remain dedicated during the entire duration of data transfer.

2. Data Transfer Phase:

- * After the circuit is established, the entire data travels over the dedicated path from sender to receiver.
- * The data flows are continuous b/w sender and receiver.
- * There is no addressing involved in the data transfer i.e. no header.

3. Circuit Disconnection or tear down phase

After the data transfer is completed, the circuit is disconnected.

When sender needs to disconnect, a signal is sent to each station to release the resources.

Note: Circuit Switching is implemented at physical layer.

Advantages of Circuit Switching:

- * A well defined and dedicated path exists for the data to travel.
- * There is no waiting time at any switch once the circuit is established data is transferred without any delay.
- * There is no header overhead.
- * Data always reaches the receiver end in order.
- * No re-recording is required.

Disadvantages of Circuit Switching:

- * As the connection is dedicated it cannot be used to transmit any other system data even if channel is free.
- * It is inefficient in terms of utilization of system resources. As resources are allocated for the entire duration of connection, these are not available to other connections.
- * Dedicated channels require more bandwidth.
- * Time required to establish a physical link b/w two stations is too long.
- * Routing decisions cannot be changed once the circuit is established.

Q1 Consider a circuit switched network. The circuit setup time is 's' sec, the propagation delay is 'd' sec per hop, and the data rate is 'b' bps. What is the delay in sending an x bit message over a k -hop path?

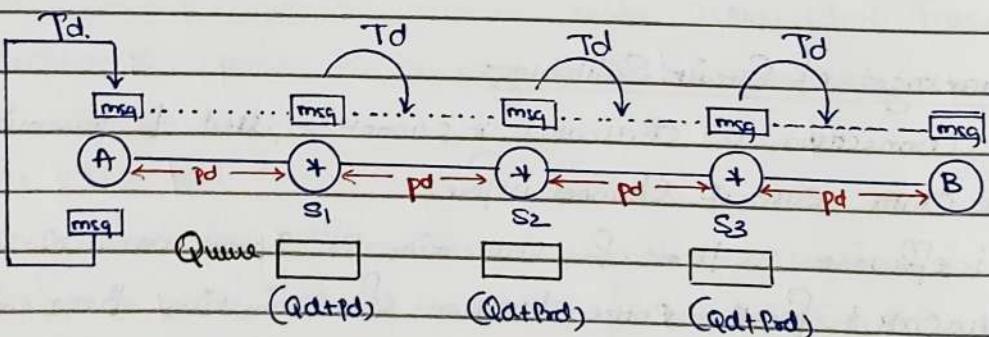
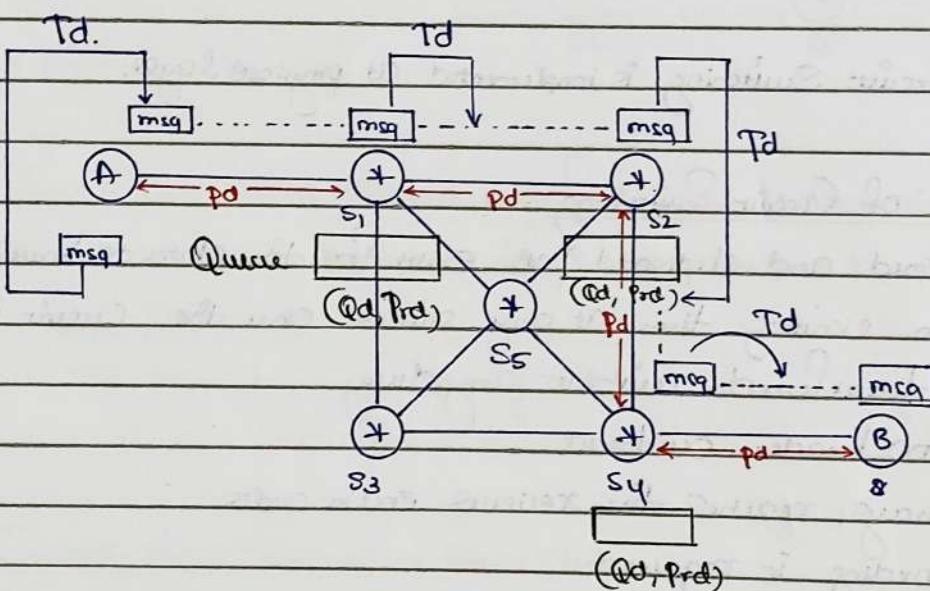
Ans.

Circuit Switching

$$\text{Total time} = S + T_I + P_I + P^0$$

$$\rightarrow \text{Total time} = S + \frac{x}{b} + k d$$

Packet Switching



$$\text{Msg Size} = m$$

$$\text{Bandwidth} = B$$

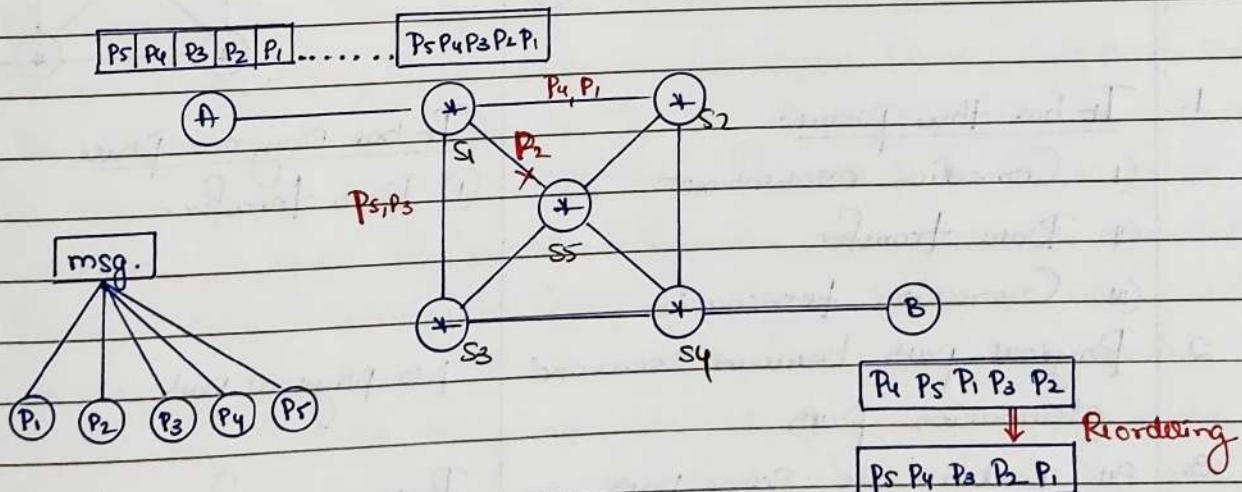
$$\text{No. of hops} = x$$

$$\text{length of each hop} = d$$

Total time = Transmission time + Propagation time + Queuing delay + Processing delay

$$\text{Total time} = \frac{x m}{B} + x \cdot d + x - 1 (q_d - P_d)$$

- * Packet Switching is a method of transferring the message to a network in the form of packets.
- * The message is broken into small pieces (fixed or variable size) called packet.
- * At the destination, all these small parts have to be reassembled belonging to same message.
- * No Pre Setup or reservation of resource is needed.
- * Packet Switching uses store and forward technique.
- * More than one path is possible b/w a pair of source and destination.
- * Each packet contains source and destination address using which they independently travel through the network.
- * Packets belonging to same network message may travel different paths to reach their destination.
- * If there is a congestion at some path, packets are allowed to choose different paths over an existing network.
- * Packet switched networks were designed to overcome the weakness of circuit switched networks since circuit switched networks were not effective for small messages.



Advantages of Packet Switching

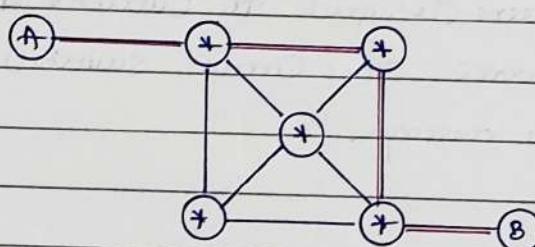
- * More fault tolerant because packets may follow different paths in case link down.
- * There is no setup or teardown phase.
- * Efficiency of packet switching is better than that of circuit switching.

- More reliable as destination can detect the missing packet.
- Cost effective and comparatively cheaper to implement.

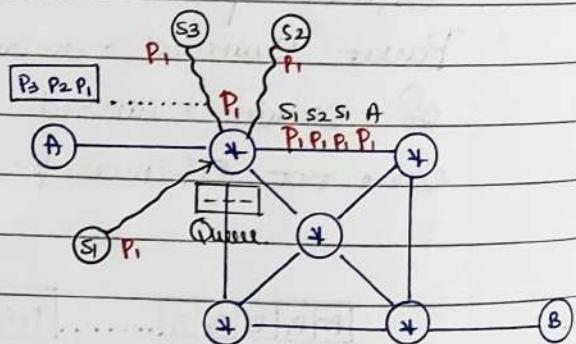
Disadvantage of Packet Switching:

- Packet switching doesn't give packets in order, whereas circuit switching provides ordered delivery of packets because all the packets follow the same path.
- Since the packets are unordered, we need to provide sequence numbers for each packet.
- Transmission delay is more in packet switching.
- Packet switching is beneficial only for small messages, but for large messages circuit switching is better.

Circuit Switching



Packet Switching



- It has three phases:
 - Connection establishment
 - Data transfer
 - Connection termination
- Physical path between source and destination path
- All packets use same path
- Reserve the entire bandwidth in advance
- Bandwidth wastage

- It has only one phase
- Data transfer.

No physical path

Packets may follow different paths
(travel independently)
Does not reserve.

No bandwidth wastage

| | | |
|-----|--|---|
| 6. | No Store and forward transmission. | Support Store and forward transmission. |
| 7. | Congestion can happen during Connection establishment phase. | Congestion can happen during data transfer phase. |
| 8. | It is reliable. | Not reliable. |
| 9. | Better for sending large message. | Better for sending small message. |
| 10. | Not fault tolerant technique. | Fault tolerant technique. |

Packitzation in Packet Switching:

- * The process of dividing a single message into small size packets is called as Packitzation.
- * These smaller size packets are sent one after another.
- * It gives the advantage of pipelining and reduce the total time taken to transmit the message.

Q1. Consider the store and forward Packet switched network given below. Assume that the bandwidth of each link is 10^6 byte/sec. A user on host A sends a file of size 10^3 byte to host B through routers R₁ and R₂ in three different ways. In the first case a single packet containing the complete file is transmitted from A to B. In the second case, the file is split into 10 equal parts, and these packets are transmitted from A to B. In the third case, the file is split into 20 equal parts and packets sent from A to B. Each packet contains 100 byte of header information along with the user data. Consider only transmission time and ignore processing, queuing and processing delays. Assume for there are no errors during transmission. Let T₁, T₂ and T₃ be the times taken to transmit the file in the first, second and third case respectively. Which of the following is correct?

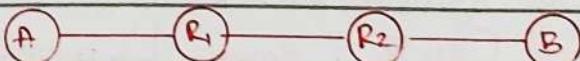
$$\text{No. of bytes (x)} = 3$$

Ans.

$$B = 10^6 \text{ Byte/sec}$$

$$\text{File size} = 10^3 \text{ Byte} / 1000 \text{ Byte}$$

$$\text{Header size} = 100 \text{ Byte}$$



Case I.

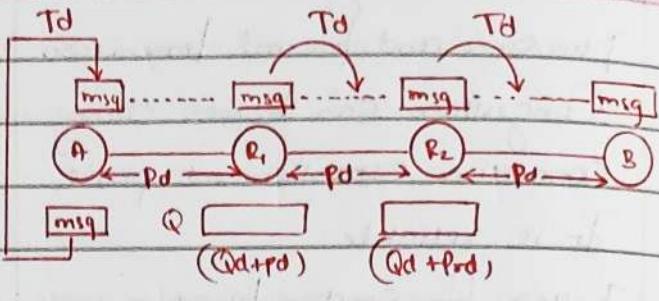
Packet size = Data + Header

$$\rightarrow 1000 \text{ B} + 100 \text{ B} = 1100 \text{ B}$$

$$T_d(\text{per}) = \frac{\text{pktsize}}{\text{bandwidth}} = \frac{1100 \text{ byte}}{10^6 \text{ byte/sec}}$$

$$= 1.1 \times 10^{-4} \text{ sec}$$

$$= 1.1 \text{ msec}$$



$$\begin{aligned} \text{Total time} &= x \cdot T_d + x \cdot Q_d + (x-1) [Q_d + Q_d] \\ &\Rightarrow 3 \times 1.1 = 3.3 \text{ msec } (T_1) \end{aligned}$$

Case II : Sending file in 5 packets.

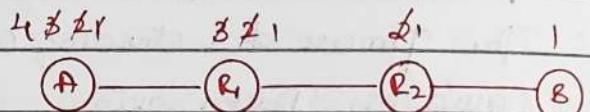
$$\text{Data in each packet} = \frac{1000 \text{ B}}{5} = 200 \text{ B}$$

Header size = 100 Byte

One packet size = Data + Header

$$= 200 \text{ B} + 100 \text{ B} = 300 \text{ B}$$

$$\begin{aligned} T_d(\text{per}) &= \frac{\text{pktsize}}{\text{bandwidth}} = \frac{300 \text{ byte}}{10^6 \text{ byte/sec}} \\ &= 3 \times 10^{-4} \text{ sec} = 0.3 \times 10^{-3} \text{ sec} \\ &= 0.3 \text{ msec} \end{aligned}$$



$$\begin{aligned} \text{Time taken to reach 1st packet from} \\ \text{Source to destination} &= 3 \cdot T_d = 3 \times 0.3 \text{ msec} \\ &= 0.9 \text{ msec} \end{aligned}$$

$$\begin{aligned} \text{Time taken to reach remaining '4' pkts to} \\ \text{reach from Source to destination} &= 4 \cdot T_d \\ &= 4 \times 0.3 \text{ msec} = 1.2 \text{ msec} \end{aligned}$$

$$\begin{aligned} \text{Total time} &= 0.9 \text{ msec} + 1.2 \text{ msec} \\ &= 2.1 \text{ msec} \end{aligned}$$

Case III : Sending file in 10 packets.

$$\text{Data in each packet} = \frac{1000 \text{ B}}{10} = 100 \text{ Byte}$$

Header size = 100 Byte

One packet size = data + header

$$= 100 \text{ B} + 100 \text{ B} = 200 \text{ B}$$

$$\begin{aligned} T_d(\text{per}) &= \frac{\text{pktsize}}{\text{bandwidth}} = \frac{200 \text{ B}}{10^6 \text{ B/sec}} \\ &= 2 \times 10^{-4} \text{ sec} = 0.2 \times 10^{-3} \text{ sec} \\ &= 0.2 \text{ msec} \end{aligned}$$

$$\begin{aligned} \text{Time taken to reach 1st packet from Source to} \\ \text{destination} &= 3 \cdot T_d = 3 \times 0.2 \text{ msec} = 0.6 \text{ msec} \end{aligned}$$

$$\begin{aligned} \text{Time taken to reach remaining 9 pkts from} \\ \text{Source to destination} &= 9 \cdot T_d = 9 \times 0.2 \\ &= 1.8 \text{ msec} \end{aligned}$$

$$\begin{aligned} \text{Total time} &= 0.6 \text{ msec} + 1.8 \text{ msec} \\ &= 2.4 \text{ msec } (T_2) \end{aligned}$$

Case IV : Sending file in 20 packets.

$$\text{Data in each packet} = \frac{1000 \text{ Byte}}{20} = 50 \text{ Byte}$$

Header size = 100 Byte

One packet size = Data + header

$$= 50B + 100B = 150 \text{ Byte}$$

$$T_d(\text{pkt}) = \frac{\text{pkt. size}}{\text{bandwidth}} = \frac{150 \text{ B}}{10^6 \text{ Byte/sec}} = 150 \times 10^{-6} \text{ sec} = 0.15 \text{ msec}$$

Time taken to reach 1st packet from source to destination = $3 \times T_d = 3 \times 0.15 = 0.45 \text{ msec}$

Time taken to reach remaining 19 pkt from source to destination = $19 \times T_d = 19 \times 0.15 = 2.85 \text{ msec}$

$$\text{Total time} = 0.45 \text{ msec} + 2.85 \text{ msec} = 3.3 \text{ msec} (T_3)$$

| T_1 | T_2 | T_3 |
|-------|-------|-------|
| 3.3 | 2.4 | 3.3 |

$$T_1 = T_3 > T_2$$

Or

$$T_2 < T_1 = T_3$$

Case I

Single msg



$$3.3 \text{ msec}$$

Case II

5 pcts



$$2.1 \text{ msec}$$

Case III

10 pcts



$$2.4 \text{ msec}$$

Case IV

20 pcts



$$3.3 \text{ msec}$$

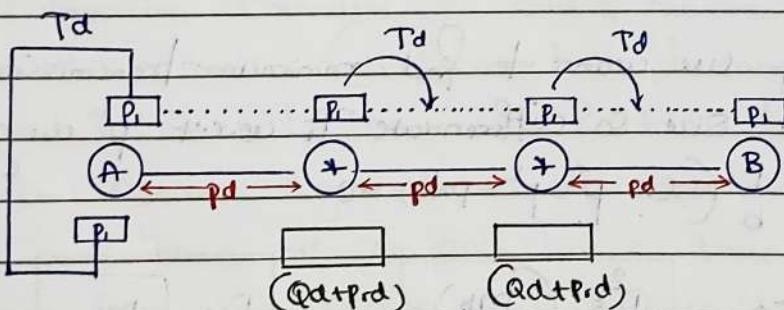
Case V

30 pcts



$$7.3 \text{ msec}$$

Total time for 'x' hops and 'n' packets.



Total time = Time for 1st packet to reach + time for remaining ($N-1$ packets) to reach

$$\text{Total Time} = x [T_d + P_d] + x - 1 [Qd + Pd]$$

Optimal Packet Size: If the packet size is not chosen properly then it might increase the total time taken to transmit the message. So it is important to choose the size properly.

Generalised formula for optimal packet size.

Suppose, M = message size

b = header size

p = payload / packet data size

assume bandwidth is ' b ' bits/sec

No. of hops = x

Packet Size (p) = $p+b$.

Capital
"P".

Total no. of packets = M/p .

* When message is Packets then these are sent in a Pipelined manner to reduce transmission time but there is a threshold on packet size ' p '. Hence it may not be large or small, it must be optimum.

* Now we first derive transmission delay (1st packet takes transmission delay by all the intermediate nodes and source transmission delay on all hops and rest all packets take only one hop transmission delay due to pipeline).

$$\begin{aligned} T_d(\text{pkt}) &= \text{Parsue} \\ &\quad \text{Bandwidth} \\ &= x \left(\frac{p+b}{b} \right) \end{aligned}$$

$$\begin{aligned} \text{Transmission time } T_d &= \left(\frac{p+b}{b} \right) x + \left(\frac{M-1}{p} \right) \left(\frac{p+b}{b} \right) \\ &= \frac{1}{b} \left[(p+b)x + \frac{1}{p} (M-p) (p+b) \right] \end{aligned}$$

So resultanty we want to find minimum transmission delay at Optimal Packet size so differentiate T_d w.r.t ' p ' we get

$$\frac{d}{dp} T_d = \frac{1}{b} \left(x * p^2 - p^2 - pb \right) = 0$$

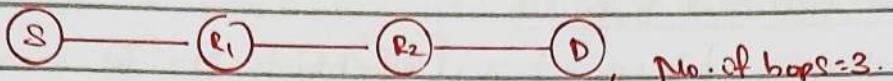
$$\text{So } p^2 = \left(\frac{Mb}{x-1} \right)$$

$$p = \sqrt{\frac{Mb}{x-1}}$$

So Optimum packet size $p = p+b$

Q.2 In a packet switching network, packets are routed from source to destination along a single path having two intermediate nodes. If the message size is 24 bytes and each packet contains a header of 3 bytes, then Optimum packet size is 9.

Ans



Message size (m) = 24 byte

Header size = 3 byte

$$P = \sqrt{\frac{mb}{x-1}} = \sqrt{\frac{24 \times 3}{8}} = \sqrt{36} = 6$$

$$\underline{P = 6}$$

Packet size (P) = $p+h$

$$= 6+3 = \underline{9}$$

Total no. of packets = $\frac{m}{P} = \frac{24}{6} = \underline{4}$

Short solution for Q1. using the formula:

$$P = \sqrt{\frac{mb}{x-1}} = \sqrt{\frac{1000 \times 100}{3-1}} = \sqrt{50000}$$

$$\underline{P = 223.6}$$

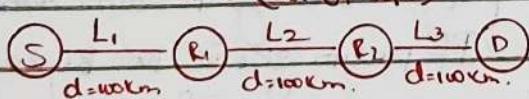
$$\text{Total no. of packets} = \frac{m}{P} = \frac{1000}{223.6} = 4.47 \approx \underline{5 \text{ pkts}}$$

- Q3. Consider a Source Computer (S) transmitting a file of size 10^{16} bit to a destination Computer (D) over a network of two routers (R1 and R2) and three links (L_1 , L_2 and L_3). L_1 connects S to R1, L_2 connects R1 and R2 and L_3 connects R2 to D. Let each link be length 100 km. Assume signal travel at a speed of 10^8 m/second. Assume that the link bandwidth on each link is 1mbps. Let the file be broken down into 1000 packets each of size 1000 bits. Find the total sum of transmission and propagation delay in transmitting the file from S to D?

Ans.

File size = 10^{16} bits

$x = 3$ (no. of hops)



$$V = 10^8 \text{ m/s} = 10^5 \text{ Km/sec.}$$

$$B = 1 \text{ mbps} = 10^6 \text{ bits/sec}$$

No. of packets = 1000 (N)

Packet size = $\underline{1000 \text{ bits}}$

$$T_d = \frac{\text{Pkt size}}{\text{Bandwidth}} = \frac{1000}{10^6 \text{ bits/sec}} = \underline{1 \text{ msec}}$$

$$P_d = \frac{d}{V} = \frac{100 \text{ km}}{10^5 \text{ Km/sec}} = \underline{1 \text{ msec}}$$

For 'x' hops and 'N' packets

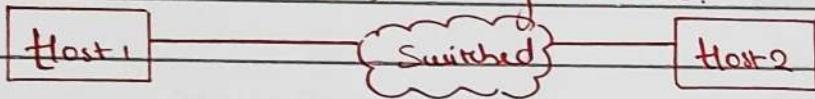
$$\begin{aligned}\text{Total time} &= x[T_d + P_d] + x-1[Q_d + P_d] + N-1(T_d) \\ &= 3[1+1] + 999x \\ &= 6 + 999 \Rightarrow 1005 \text{ msec}\end{aligned}$$

Q4 Two hosts are connected via a packet switch using 10^7 bits/second link. Each link has a propagation delay of 20 microseconds. The switch begins forwarding a packet 35 microseconds after it receives the same. If 1000 bits of data are to be transmitted between the two hosts using a packet of size of 5000 bits, the time elapsed between the transmission of first bit of data and the reception of the last bit of the data in microseconds is _____

3.54 sec delay at switch.

$x=2$.

Ans



$$\begin{aligned}B &= 10^7 \text{ bits/sec} \\ P_d &= 20 \mu\text{sec.}\end{aligned}$$

$$\text{Packet size} = 5000 \text{ bits}$$

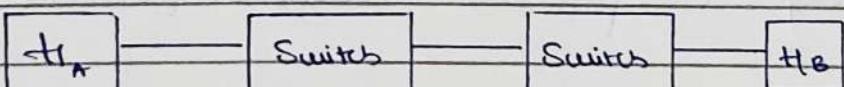
$$\text{No. of packets} = (N) = \frac{10000 \text{ bits}}{5000 \text{ bits}} = 2$$

$$\begin{aligned}T_d(\text{per}) &= \frac{\text{per size}}{\text{bandwidth}} = \frac{5000 \text{ bits}}{10^7 \text{ bits/sec}} \\ &= 500 \times 10^{-6} \text{ sec} \\ &= 500 \mu\text{sec}\end{aligned}$$

For 'x' hop & 'N' packets.

$$\begin{aligned}\text{Total time} &= x[T_d + P_d] + x-1[Q_d + P_d] \\ &= 2(500 + 20) + 1 \times 35 + 1 \times 500 \\ &= 1000 + 40 + 35 + 500 \\ &= 1575 \mu\text{sec}\end{aligned}$$

Q5 Suppose two hosts are connected through two intermediate switches.



Suppose each link (one-way) propagation delay is 20ms and each link data transfer rate is 1Mbps. If packet size is 1000 Bytes then the amount of time required to send one file of 5000 Bytes from sender to receiver. (Consider for processing overhead at switches is negligible)

i.e. 116 msec.

Ans

$$P_d = 20 \text{ msec}, B = 1 \text{ Mbps} = 10^6 \text{ bits/sec}$$

$$\text{No. of packets (N)} = \frac{s}{\text{packet size}} = \frac{5}{8000 \text{ bits}}$$

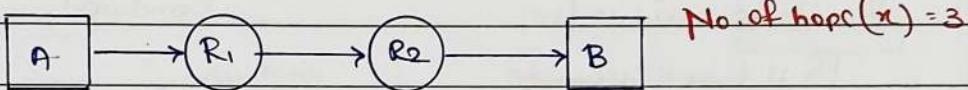
$$\text{Packet size} = 1000 \text{ Byte} = 8000 \text{ bits}$$

$$\text{Fwd size} = 5000 \text{ Byte}$$

$$T_{d(pkt)} = \frac{\text{pkt size}}{\text{bandwidth}} = \frac{8000 \text{ bits}}{10^6 \text{ bits/sec}}$$

$$\begin{aligned} \text{Total time} &= x(T_d + P_d) + x-1(Q_d + P_{rd}) + (N-1)T_d \\ &= 3(8 + 20) + 4 \times 8 \\ &= 24 + 60 + 32 \\ &= 84 + 32 \\ &= \underline{\underline{116 \text{ msec}}} \end{aligned}$$

Q6. Consider two hosts A and B are connected through two Routers R₁ and R₂



Each link has Propagation delay (one way) 20 ms, data transfer rate is 1 Mbps and Processing delay at each router is 2 ms. Host A uses pipeline protocol for flow control. The time required (in ms) to transmit a file of size 12000 Byte from host A to host B, using packet size 1000 Byte is 176 msec.

Ans

$$P_d = 20 \text{ msec}, B = 1 \text{ Mbps} = 10^6 \text{ bits/sec}$$

$$\text{Fwd size} = 12000 \text{ Byte}$$

$$P_{rd} = 2 \text{ msec}$$

$$\text{Packet size} = 1000 \text{ Byte}$$

$$T_{d(pkt)} = \frac{\text{pkt size}}{\text{bandwidth}}$$

$$\text{No. of packets (N)} = \frac{12000 \text{ B}}{1000 \text{ B}} = 12$$

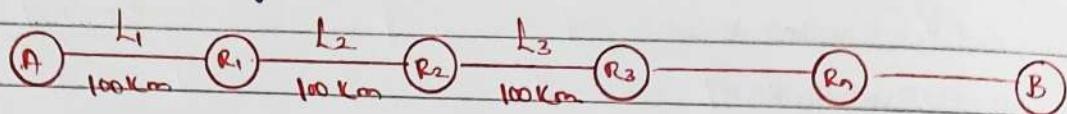
$$= \frac{8000 \text{ bits}}{10^6 \text{ bits/sec}} = \underline{\underline{8 \times 10^{-3} \text{ sec}}}$$

$$\begin{aligned} \text{Total time} &= x(T_d + P_d) + x-1(Q_d + P_{rd}) + (N-1)T_d \\ &= 3(8 + 20) + 2(2) + 11 \times 8 \\ &= 24 + 60 + 4 + 88 \\ &= \underline{\underline{176 \text{ msec}}} \end{aligned}$$

Q7. Consider a host computer (A) transmitting a file of size 10^5 bits to a host computer (B) via a network of routers (R₁, R₂...R_n) and links (L₁, L₂, ..., L_n). L₁ connects A to R₁, L₂ connects R₁ to R₂. L₃ connects R₂ to R₃ and L_n connects R_{n-1} to B. Let each link be of length 100 km. Assume Signal travel over each link at a speed of 10^8 meter/second. Let the file be broken into 100 packets.

of each of size 1000 bits. Assume bandwidths on each links is 1 Mbps. The total sum of T_d and P_d in transmitting the file from A to B is 119 msec. Assume y is the no. of routers between A and B and x is number of minimum links between A and B then find $x+y$?

Ans.



$$v = 10^8 \text{ m/sec} = 10^5 \text{ km/sec}$$

$$\text{No. of packets (N)} = 100$$

$$\text{Packet size} = 1000 \text{ bits}$$

$$B = 1 \text{ Mbps} = 10^6 \text{ bits/sec}$$

$$\text{Total time} = 119 \text{ msec.}$$

$$P_d = \frac{d}{v} = \frac{100 \text{ km}}{10^5 \text{ km/sec}} = 10^{-3} \text{ sec} = 1 \text{ msec}$$

$$T_d(\text{pkt}) = \frac{\text{pkt-size}}{\text{bandwidth}} = \frac{1000 \text{ bits}}{10^6 \text{ bits/sec}} = 1 \text{ msec}$$

For 'x' hops and 'N' packets

$$\text{Total time} = x[T_d + P_d] + (x-1)(Q_d + P_d) + N(T_d)$$

$$119 = x(1+1) + 99x$$

$$119 = 2x + 99$$

$$119 - 99 = 2x$$

$$20 = 2x$$

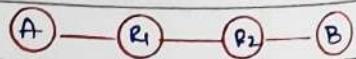
$$\boxed{x=10}$$

\hookrightarrow no. of hops

$$y = 10-1$$

$$y = 9$$

$$x+y = 10+9 \\ = 19.$$



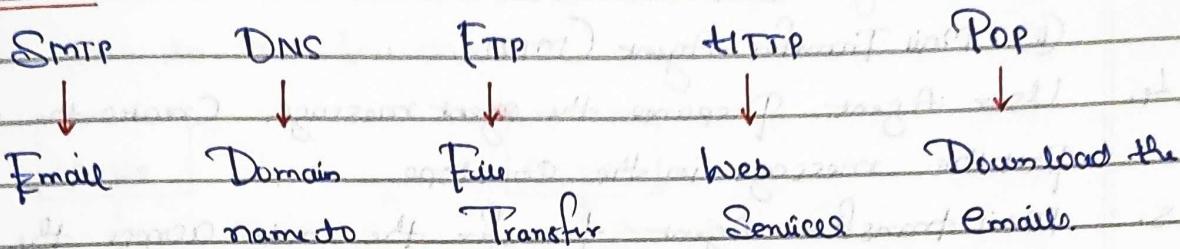
No. of hops or no. of link
= 3

No. of routers = 2

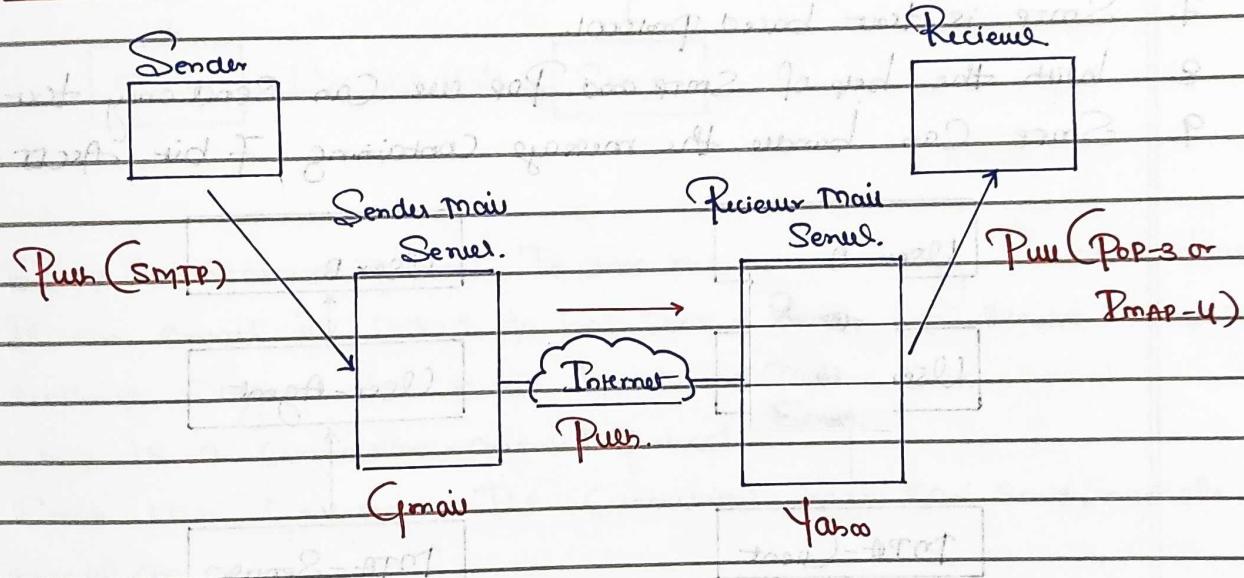
* If no. of hops/link = x
then no. of routers = $x-1$.

APPLICATION LAYER PROTOCOL

Protocols:



Email [Electronic Mail]



- SMTP transfers the mail from Sender's mail Server to receiver's mail Server.
- While sending the email, SMTP is used two times:
 - (i) Between the Sender and Sender's mail Server.
 - (ii) Between Sender's mail Server and receiver's mail Server.
- To download or review the email another protocol is needed between receiver's mail Server and receiver.
- The most commonly used protocols are POP3 and IMAP-4.

SMTP [Simple Mail Transfer Protocol]

1. The objective of SMTP is to transfer the email reliably and efficiently.
2. It uses port number - 25 at TCP.

3. In Smtp there are two Components:

(I) User Agent (UA)

(II) Mail Transfer Agent (MTA)

4. User Agent Prepare the agent message, Create the envelope and Put the message in the envelope.

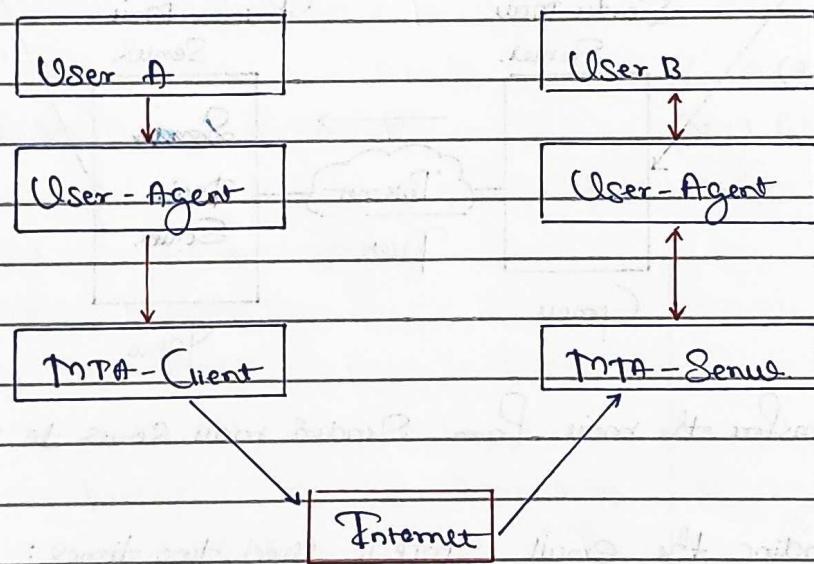
5. Mail transfer Agent transfer the mail across the internetwork. Actual mail Transfer is done through MTA

6. To Send mail, System must have a Client MTA and to receive the mail, it must have a Server MTA.

7. Smtp is text based protocol.

8. With the help of Smtp and Pop we can send only text messages.

9. Smtp Can handle the message containing 7 bit ASCII text.



10. Smtp Cannot transfer other type of data like images, videos, audio etc.

11. Smtp Cannot transfer binary files or executable files.

12. Smtp Cannot transfer the text data for the language other than English.

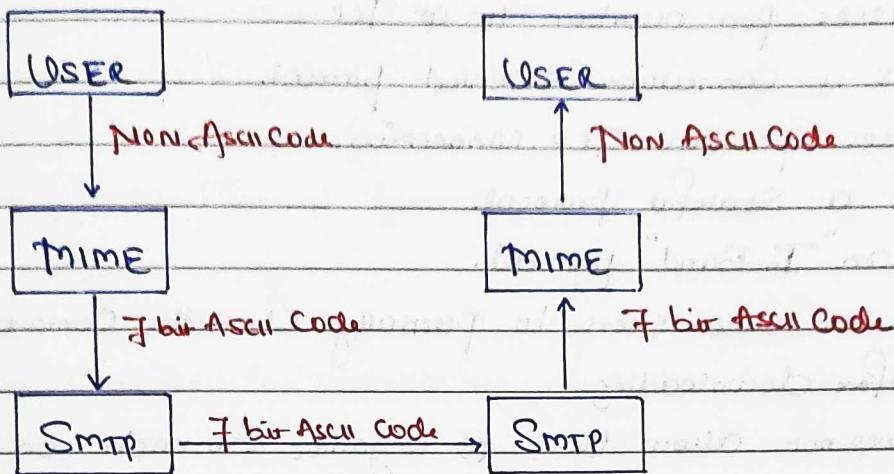
13. Only Smtp is not sufficient to send binary files or send videos or audio so we require MIME (Multi-purpose Internet Mail Extension).

14. MIME is a Supplementary Protocol that allows non-ASCII data to send through Smtp.

15. MIME is a set of Software function that transforms non-ASCII

Data to ASCII Data or vice versa.

16. MIME is used to convert non-text data to text data and text data to non-text data.



17. Smtp is Stateless Protocol. It does not maintain any information of user. If an email is asked to be sent twice, then Server resends it without saying that email has already been sent.
18. Smtp is a Connection-oriented Protocol
19. Smtp uses Persistent TCP Connections, So it can send multiple emails at once.
20. Smtp is an "In-Band" Protocol.
21. Smtp is used for Push the emails.
22. Smtp Push the mail from Client to server. On other hand it needs a pull protocol (Download).
23. POP3 and IMAP4 are used for Pulling the emails.

Note:

Transfer the message from sending mail server is done through Smtp. Finally the message from receiving server to our browser is done through http only.

Pop3 (Post Office Protocol Version-3)

1. It is a message access protocol.
2. It is a pull protocol.
3. Pop3 uses port number -110 or TCP
4. Pop3 is a Connection-Oriented Protocol.
5. Pop3 uses persistent TCP connections.
6. Pop3 is a Stateful Protocol.
7. It is an "In-Band" protocol.
8. It does not allow users to partially check the content of the mail before downloading.
9. Pop3 does not allow user to organise the mail on the mail server.
10. Pop3 has two modes: the deletemode and keep mode, in delete mode, the mail is deleted from mailbox after each retrieval.
11. In the keep mode, the mail remains in the mailbox after retrieval.

IMAP-4 (Internet Mail Access Protocol Version-4)

- IMAP-4 is similar to Pop3 but it has more features. It is more powerful and complex.
- IMAP-4 provides the following extra functions:
 - * A user checks the email header prior to downloading.
 - * A user can search the content of email for specific string of characters prior to downloading.
 - * A user can partially download the email.
 - * A user can create, delete, or rename the mailbox on the mail server.
 - * A user can create a hierarchy of mailbox in a folder for email storage.

Characteristics of IMAP

- * IMAP is a Pull Protocol.
- * It uses Port number - 143 or TCP.
- * It is a Connection-oriented Protocol.
- * It uses Persistent TCP Connection.
- * IMAP is a Stateful Protocol.
- * IMAP is an "Inband" Protocol.

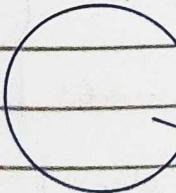
POP3

1. Mail can only be accessed from a single device.
2. Download the email from server to a single computer and the copy at the server is deleted.
3. User cannot organise the mail in the mailbox of the mail server.
4. It does not allow user to sync emails.
5. It is unidirectional i.e. all the changes made on a device does not effect the content present on the server.

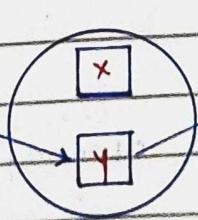
IMAP-4

- Mail can be accessed from multiple devices. The email message is stored on the mail server itself.
- User can organise mails on the mail server.
- It allows users to sync their emails. It is bidirectional i.e. all the changes made on the server or device are made on other side too.

Client-X

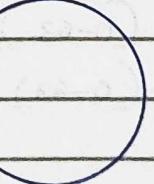


Push
(SMTP)



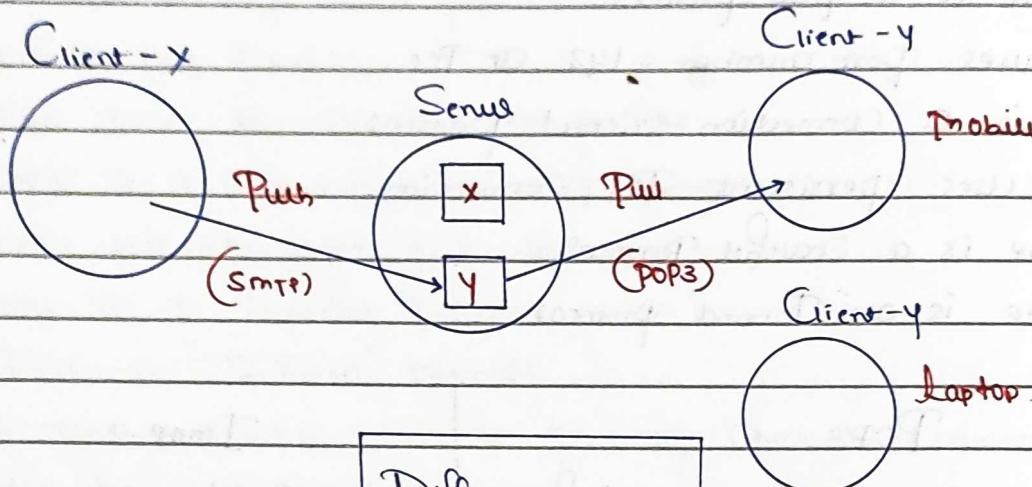
Server

Client-Y

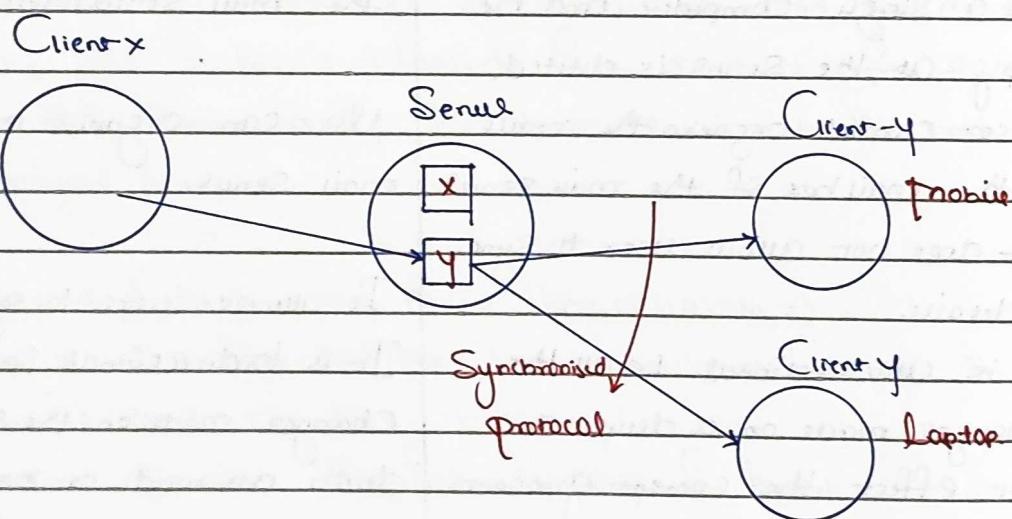


Pull
(POP3)

Client X → Client Y

POP3IMAP4

Difference
between
POP3 & IMAP4



→ SMTP uses Base 64 Encoding

$$(xy)_{64}$$

$$x \rightarrow (0-63)$$

$$y \rightarrow (0-63)$$

6 bit

$$000000 \rightarrow 0$$

$$\vdots$$

$$111111 \rightarrow 63$$

Text Data: "And"

↓
65
↓
110
↓
100
↓
an 8 bit

| | | | |
|--------|--------|--------|--------|
| 6bit | 6bit | 6bit | 6bit |
| 010000 | 110110 | 111001 | 100100 |
| ↓ | ↓ | ↓ | ↓ |
| 16 | 22 | 57 | 36 |
| Q | W | S | K |

'And' Base by Encoding → QWSK → ourshead
Input Output

| | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 |
| a | b | c | d | e | f | g | h | i | j | k | l | m |
| 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 | |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | + | / | |

$$(0-25) \rightarrow \{A-2\}$$

ASCII Codes:

$$(26-51) \rightarrow \{a-2\}$$

$$(97-122) \rightarrow \{a-z\}$$

$$(52-61) \rightarrow \{0-9\}$$

$$(65 - 90) \rightarrow \{A-Z\}$$

$$(62, 63) \rightarrow \{+, /\}$$

e.g. Input = And PgG ZPLg

011 001 11 0000

6bit 6bit

↓ ↓

25 48

↓ ↓

z w

1985-1986

HR cm

• 100 •

103

~~103~~ 109 ~~109~~

Elliott

0.58

6bit | 6bit | 6bit
011001 | 110110 | 110100
↓ ↓ ↓
25 54 52

$$2 \quad 2 \quad 0 =$$

SMTP Commands.

1. HELO : identify itself
2. MAIL FROM : identify sender of message
3. RCPT TO : identified recipient of message.
4. DATA : Send the actual message
5. QUIT : Terminate the message
6. RSET : Abort the current mail transaction.
7. VRFY : Verify the address of recipient.
8. NOOP : Checks the status of recipient.
9. TURN : Switches the sender and recipient.
10. EXPN : Ask the recipient to expand the mailing list.
11. HELP : Ask the recipient to send information about the command
12. SEND FORM
13. SMOL FROM
14. SMAL FROM.

Q1. Consider different activities related to email

m1: Send an email from a mail client to mail server.

m2: Download an email from mailbox server to a mail client.

m3: Checking emails in a web browser

What is the Application-level Protocol used in each activity?

Ans. m1: SMTP m2: POP m3: HTTP

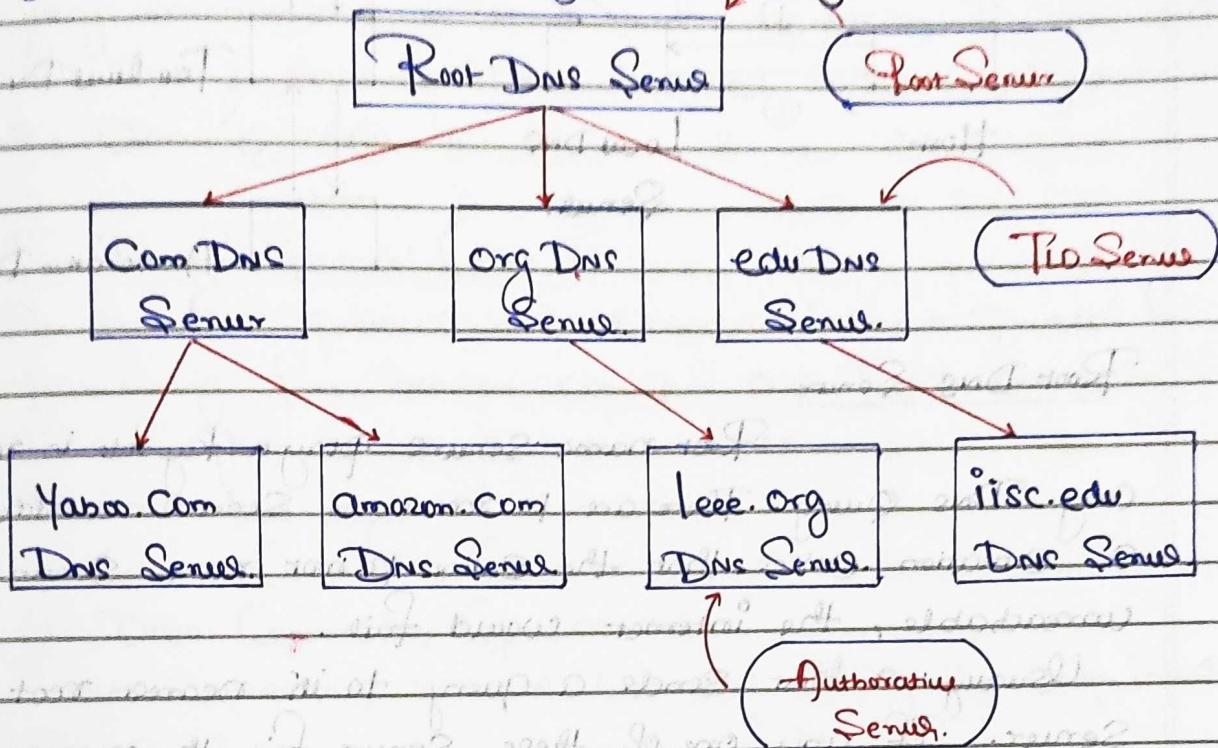
Domain Name System (DNS)

- * Easy to remember the domain names
- * IP addresses are not static
- * DNS is a protocol used to convert domain name to IP address.

Most Commonly used domain are:

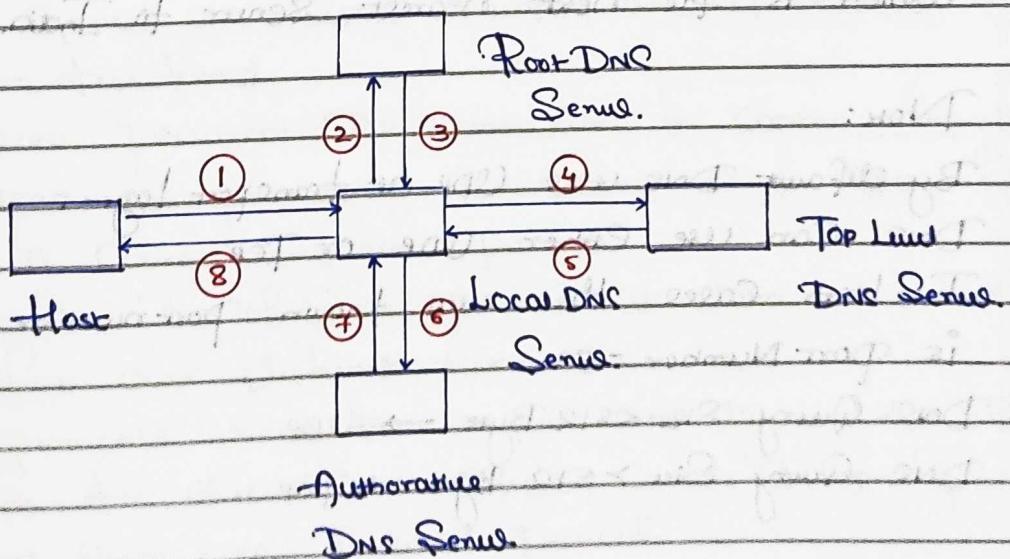
1. Com : usually used by Commercial Organisation. eg: yahoo.
2. Edu : Usually used by Educational institutions
3. Org : Used by non profit organisations.

4. mil: Used by military Organisation
5. net: It is open public for any Commercial Organisation
6. gov: Used to represent government Organisation.

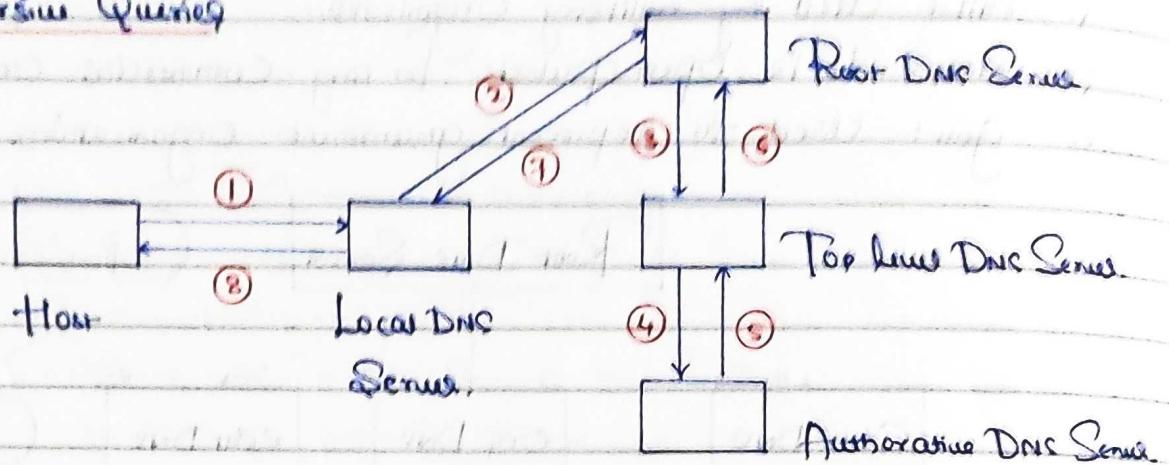


Iterative Queries

DNS Use UDP → Port no. 53.



Recursive Queries



Root DNS Server

Root name Servers play a key role in resolving any DNS Query. There are 13 root name servers worldwide. If a situation arises that the entire 13 root name servers are unreachable, the internet would fail.

- Usually a host sends a query to its nearest root name server. If any one of these servers fail, the requests are diverted to another nearest server.
- Eg: If you are in India the nearest root name server is at Tokyo. If the root name server at Tokyo is down, all the DNS queries or traffic is diverted to servers at Europe, which is the next nearest server to India.

Notes:

- * By default DNS uses UDP at transport layer.
- * DNS can use either UDP or TCP.
- * In both cases the well-known port number used by the server is Port Number - 53.
- * DNS Query Size < 512 Byte \rightarrow UDP
- * DNS Query Size > 512 Byte \rightarrow TCP

Q1. Consider the resolution of the domain name www.govt.org.in by a DNS resolver. Assume that no resource records are cached anywhere across the DNS Service and that iterative query mechanism is used in the resolution. The number of DNS query-response pairs involved in completely resolving the domain name is 4.

File Transfer Protocol (FTP)

1. File transfer protocol is a standard internet protocol for transferring files between computers over TCP/IP connection.
2. It uses port numbers 20 and 21 on TCP.
3. It has two types of connections:
 - (i) Control Connection (port no-21)
 - (ii) Data Connection (port no-20)
4. Control Connection remains connected during the entire interaction session.
5. The data connection is opened and closed for each file transfer activity.
6. When user starts an FTP session, the control connection opens. While the control connection is open, the data connection can be opened and closed multiple times if multiple files are transferred.
7. FTP uses persistent TCP connections for control information.
8. FTP uses non-persistent TCP connections for data information.
9. FTP is a connection-oriented protocol.
10. FTP is an "out-of-band" protocol as data and control information flow over different connections.
11. Some protocols send their request and data in the same TCP connection for this reason they are called 'In-band' protocols.
12. HTTP and SMTP are 'In-band' protocols.
13. FTP is 'Stateful' protocol.

→ Transmission Mode: FTP can transfer a file across the data connection using one of the following three transmission modes.

1. Stream mode: It is a default mode, data are delivered from FTP to TCP as a continuous stream of bytes.

2. Block mode: In this mode, data can be delivered from FTP to TCP in blocks. In this case, each block is preceded by a 3 byte header. The first byte is called the block descriptor, the next two bytes define the size of block (in bytes).

3. Compressed mode: In compressed mode, if file is big, the data can be compressed. In the text file it is usually spaces (blanks). In binary file, null character are usually compressed.

→ File Type: FTP can transfer one of the following file types across the data connection:

1. ASCII file
2. EBCDIC file (file format used by IBM)
3. Image file.

→ Data Structure: FTP can transfer a file across the data connection using one of the following interpretations of the structure of data:

1. File Structure: It is used by default. It is a continuous stream of bytes.

2. Record Structure: In the record structure the file is divided into records. This can only be used using text files.

3. Page Structure: In the page structure, the file is divided into pages, with each page having a page number and page header. The page can be accessed randomly/sequentially. (page can be stored).

Commands in FTP

1. USER : User information.
2. PASS : Password
3. ACCT : Supply accounting information.
4. CWD : Change to Another Directory.
5. REIN : Remove all authentication information and parameter settings.
6. QUIT : Log out of the System
7. PORT : Client Chooses a Port.
8. PASV : Server Chooses a Port.
9. TYPE : Default file type (A: ASCII, E: EBCDIC, I: Images).
10. MODE : Data Transmission Mode (S: Stream, B: Block, C: Compressed)
11. PROMPT : Turn on (or turn off) file transfer prompting.
12. STRU : Define data organisation (F: file, R: record, P: page).

HTTP Protocol

- * HTTP protocol used mainly to access data on world wide web (www).
- * It is Client Server Protocol using Port No - 80 on TCP.
- * HTTP is "In-Band" protocol i.e. both request and data are sent only in one connection.
- * HTTP is a stateless protocol i.e. It does not maintain any information of user.
- * There are two types of HTTP protocol
 - i) Non Persistent (1.0)
 - ii) Persistent (1.1)

Non Persistent (1.0)

In a Non-persistent Connection, One TCP Connection is made for each request/response. This strategy follows steps:

- (1). The Client Opens a TCP Connection and Sends a request.
- (2). Server Sends the response and Closes the Connection.
- (3). In this strategy, if a file contains link to N-different

Pictures in different file (all located on same Server) the connection must be opened and closed N times.

Persistent (1.1)

- In a Persistent Connection, the Server leaves the connection open for more request after sending a response.
- The Server closes the connection at the request of Client or time out has been reached.

HTTP Commands

- GET - Request a document from Server.
- HEAD - Request information about a document but not the document itself.
- PUT - Send a documentation from Client to Server.
- POST - Send some information from Client to Server.
- TRACE - It is used for debugging.
- DELETE - Delete the web page.
- CONNECT - It is not currently used. It is reserved for future purpose.
- OPTIONS - Inquires about available Options.

| Application | Port Number | Trans. Protocol |
|-------------|---|-----------------|
| DNS | 53 | UDP |
| HTTP | 80 | TCP |
| FTP | 20 (Data Connection) 21 (Control Connection) | TCP |
| SMTP | 25 | TCP |
| Pop | 110 | TCP |
| SNmp | 161, 162 | UDP |
| TFTP | 69 | UDP |
| IMAP | 143 | TCP |
| Telnet | 23 | TCP |
| DHCP | 67 (DHCP S), 68 (DHCP C). | UDP |

Q2. Which one of the following use UDP as the transport protocol?

Ans DNS

| | |
|--------|---------------|
| TCP | UDP. |
| Snmp | DNS |
| HTTP | Snmp |
| FTP | TFTP |
| Pop | DHCP |
| IMAP | All realtime |
| Telnet | & multimedia. |

Q3. Which of the following transport layer protocols is used to support electronic mail?

Ans TCP

Q4. The transport protocols used for realtime multimedia, file transfer, DNS and email respectively are

Ans UDP, TCP, UDP and TCP

Q5. Match the following.

| Protocol | Port Number |
|----------|-------------|
| DNS | 23 |
| DHCP | 53 |
| IMAP | 67 |
| POP3 | 68 |
| | 110 |
| | 143 |

Q6.

| App. Layer Protocol | Port no. |
|---------------------|----------|
| FTP data | 80 |
| FTP Control | 20 |
| HTTP | 23 |
| TFTP | 21 |
| | 25 |
| | 69. |

Q7. Which of the following is/are example of stateful application layer protocols?

Ans FTP
POP3

| Stateless | Stateful |
|-----------|----------|
| DNS | POP |
| HTTP | IMAP |
| SNMP | FTP. |

Q8. Which of the following protocol Pairs can be used to send and receive retrieve mail (in that order?).

Ans **SMTP, POP3**

Q9. The Protocol(s) that uses a connectionless UDP.

Ans **DNS**

Q10. In one of the pairs of protocols given below, both the protocols can use multiple TCP connections between the same Client and the Server. Which one is that?

Ans **HTTP, FTP**

| HTTP | FTP | SMTP |
|---------|--------|-----------|
| GET | USER | HELO |
| HEAD | PASS | MAIL FROM |
| PUT | ACCT | RCPT TO |
| POST | CWD | DATA |
| TRACE | REIN | QUIT |
| DELETE | QUIT | RCPT |
| CONNECT | PORT | VERFY |
| | PASV | NOOP |
| | TYPE | TURN |
| | MODE | EXPN |
| | PROMPT | HELP |
| | STRU | SEND FROM |
| | | SMPL FROM |
| | | SMPL FROM |

All Commands:

Q11. Consider the three Commands : PROMPT, HEAD, RCPT. Which of the Options indicate a correct association of these commands with protocols where they are used?

Ans **FTP, HTTP, SMTP**

Q12. HELO And Port respectively are Commands from the Protocol:
 Ans. SMTP and FTP

Q13. Identify the Correct Sequence in which the following Packets are transmitted on the network - by a host when a browser requires a web page from a remote Server, assuming that the host has just been restarted.
 Ans. DNS Query, TCP SYN, HTTP GET request

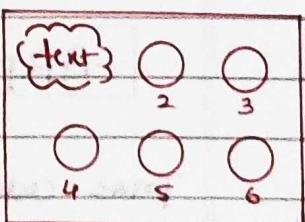
Q14. Which one of the following is not a HTTP 'request method'?
 Ans. SEND

Q15. HTTP command from the below list is Post.
 a. REIN
 b. PSTRU
 c. CWD
 d. Post

Q16. Match the following

- | | |
|----------|---|
| I. HTTP | Uses both TCP and UDP |
| II. FTP | Uses two ports for its operation. |
| III. DNS | TMIME to deal with non ASCII data |
| IV. Smtp | Used to get the mail. |
| V. POP3 | Trace method loop back request message. |

Q17. Assume that you have made a request for a web page through your web browser to a web server. Initially the browser cache is empty. Further the browser is configured to send HTTP requests in non-persistent mode. The web page consists one text & 5 small images. The min no. of TCP connections required to display the web page completely in your browser 6.



web page ↑

IP SUPPORT PROTOCOL

IP/NL (i) Limited Broadcast Address

255.255.255.255

(ii) Direct Broadcast Address

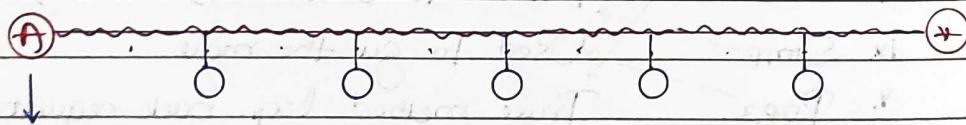
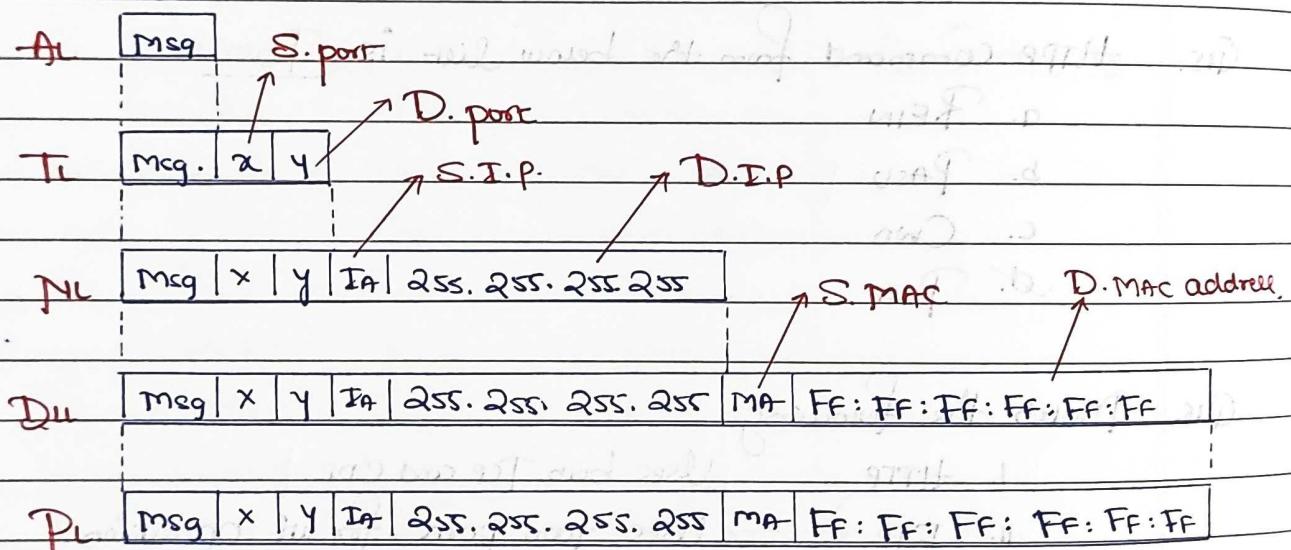
NID = 10.0.0.0

DBA = 10.255.255.255

DLL \rightarrow Broadcast MAC Address (48 bit)

FF:FF:FF:FF:FF:FF

Limited Broadcasting:



IP Address : To.

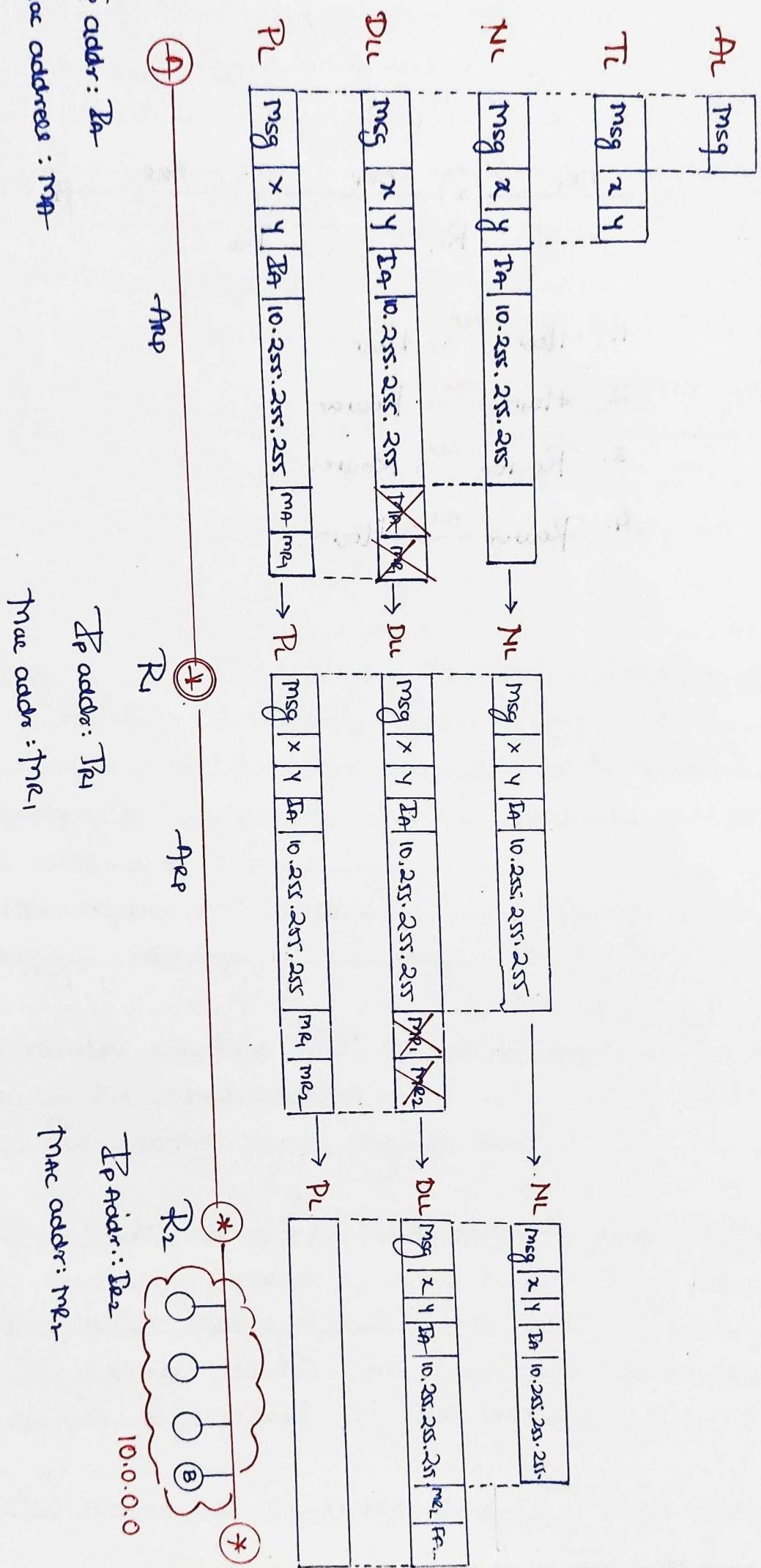
MAC Address : MA.

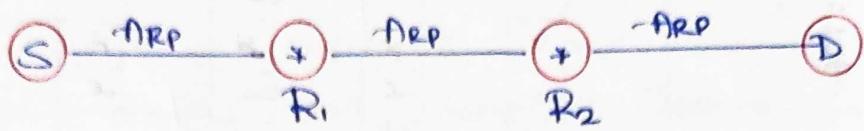
ARP.

ARP is a communication protocol used to find the MAC address of a device from its IP address.

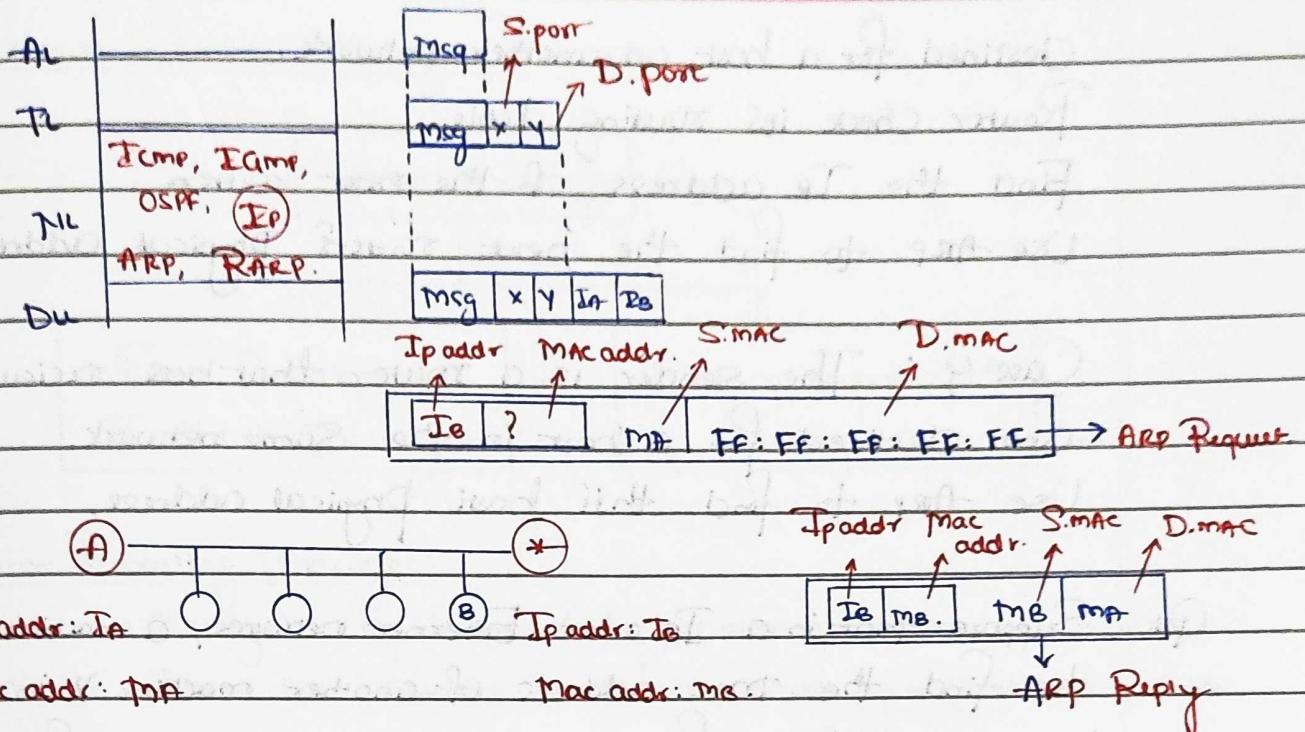
IP Address $\xrightarrow{\text{ARP}}$ MAC address

Direct Broadcasting:





1. Host $\xrightarrow{\text{ARP}}$ Host
2. Host $\xrightarrow{\text{ARP}}$ Router
3. Router $\xrightarrow{\text{ARP}}$ Router
4. Router $\xrightarrow{\text{ARP}}$ Host.



The important terms associated with ARP are:

1. ARP Cache: After resolving MAC address, the ARP Sender stores it in the source cache in a table for future reference. Subsequent communications can use the MAC address from the table.
2. ARP Cache Timeout: It indicates the time for which the MAC address is stored in the ARP Cache.
3. ARP Request: ARP request is broadcasting.
4. ARP response/reply: ARP reply is unicasting.

Case 1: The sender is a host and wants to send a packet to another host on the same network.

Use ARP to find another host's physical address.

Case 2: The sender is a host and wants to send a packet to another host on another network.

Sender looks at its routing table.

Find the IP address of the next hop (router) for this destination.

Use ARP to find the router's physical address.

Case 3: The sender is a router and received a datagram.

Destined for a host on another network.

Router checks its routing table.

Find the IP address of the next router.

Use ARP to find the next router's physical address.

Case 4: The sender is a router that has received a datagram destined for a host in the same network.

Use ARP to find this host's physical address.

Q1. Suppose that in a TCP over Ethernet network, a machine X wishes to find the MAC address of another machine Y in its subnet. Which one of the following techniques can be used for this?

- Ans X sends an ARP request packet using broadcast MAC address in its local subnet.

Q2. The address resolution protocol (ARP) is used for

- Ans Find the MAC address that corresponds to an IP address

Q3. Which one of the following protocols is not used to resolve one form of address into another one?

- Ans DHCP

Q4. Consider the following two statements:

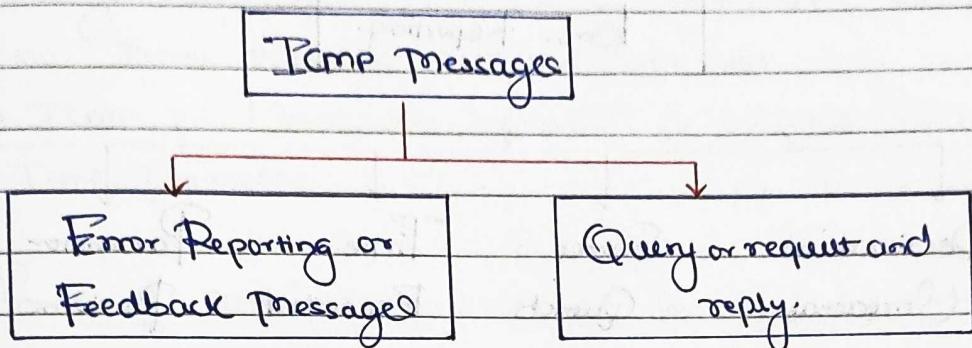
S₁: Destination MAC address of an ARP reply is a broadcast address.

S₂: Destination MAC address of an ARP request is a broadcast address.

Which one of the following choice is correct?

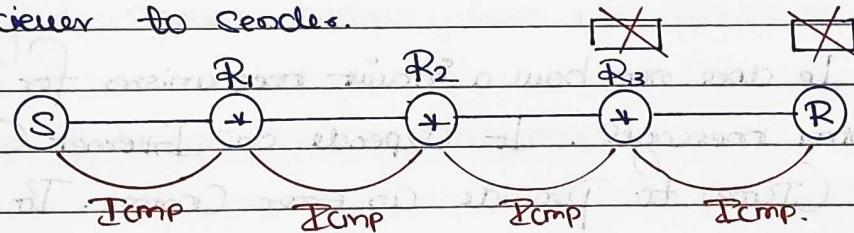
- Ans S₁ is false and S₂ is true.

Internet Control Message Protocol



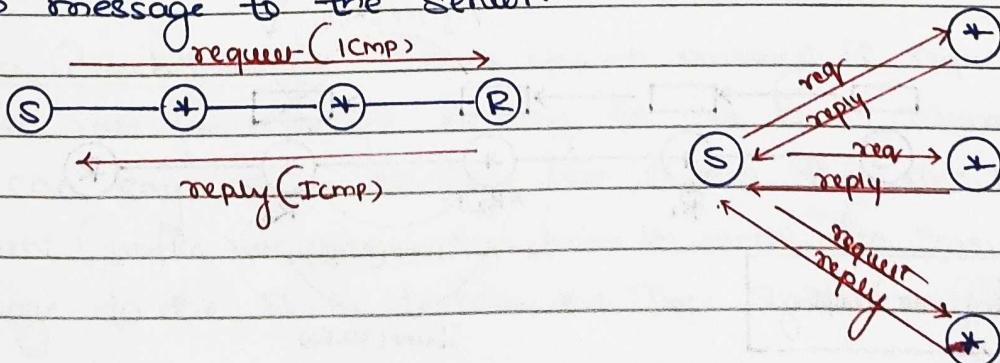
Error Reporting Messages:

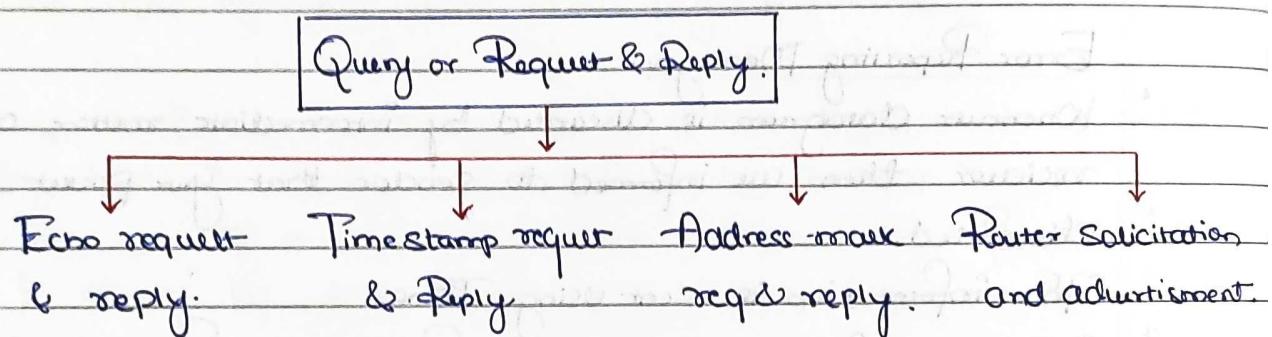
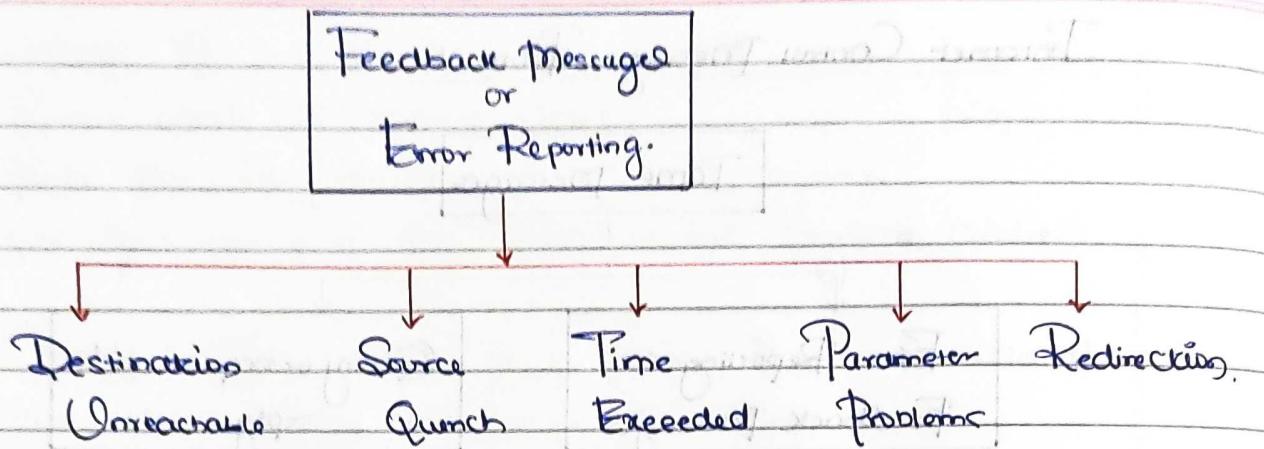
- * Whenever datagram is discarded by intermediate router or end receiver then we informed to sender that your packet has been discarded.
- * This information is sent using ICMP.
- * Direction of packet movement for ICMP is from router to sender or receiver to sender.



Query Message:

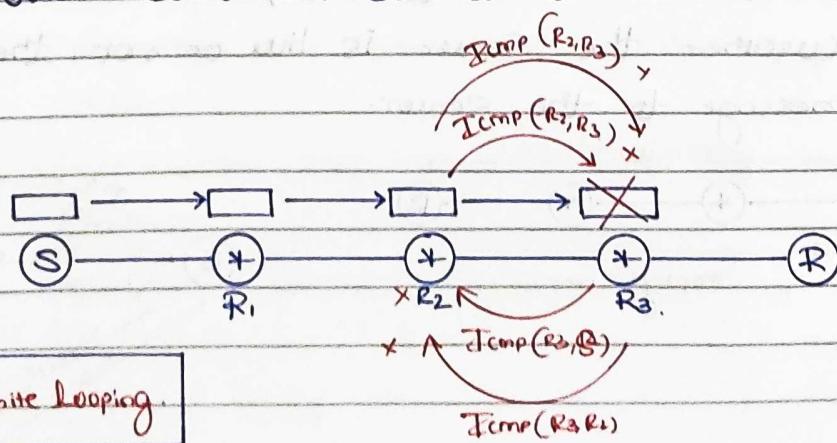
The query messages are those messages that help the host to get the specific information of another host. For eg: suppose there are a Client and a Server, and the Client wants to know whether the Server is live or not, then it sends the ICMP message to the Server.





Since IP does not have a built-in mechanism for sending error and control messages. It depends on Internet Control Message Protocol (ICMP) to provide an error control. It is used for reporting errors and management queries. It is a supporting protocol and used by network devices like routers for sending the error messages and operations information.

e.g.: the requested service is not available or that a host or router could not be reached.



To infinite looping.

Note: Whenever any IP packet is discarded initially, ICMP packet will be generated and otherwise, ICMP packet will be discarded then no ICMP message will be generated.

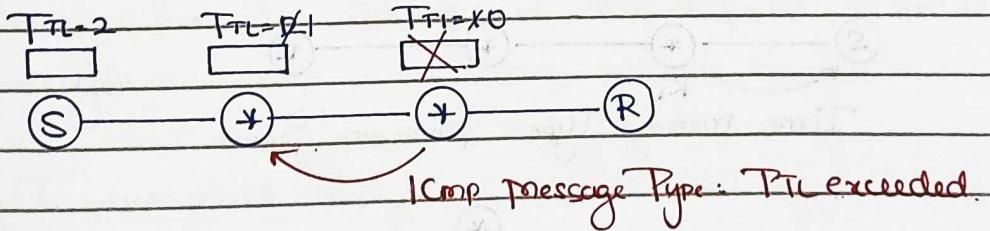
IP + ICMP → Unreliable because there is no ICMP message of ICMP Protocol.

The following are important points about ICMP error messages:

- * No ICMP error message will be generated in response to a datagram carrying an ICMP.
- * No ICMP error message will be generated for a fragmented datagram that is not the first fragment.
- * No ICMP error message will be generated for a datagram having a multicast address.
- * No ICMP error message will be generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.1.

Feedback Messages or Error Reporting

- ① TTL exceeded: whenever TTL becomes 0, router will discard the packet and send an ICMP message to source.

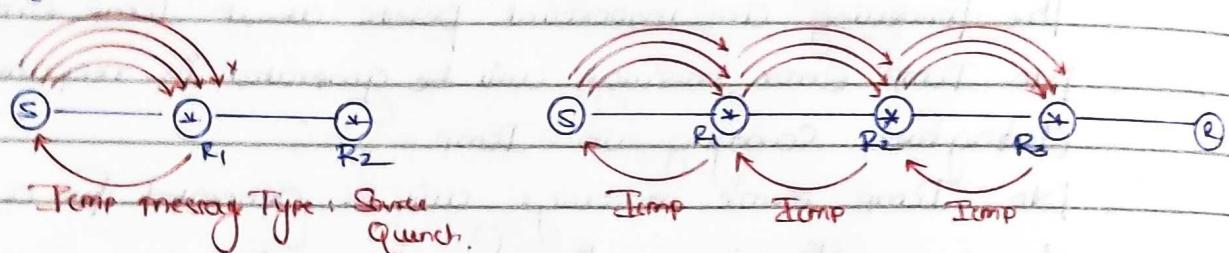


- ② Source Quench Message: Source Quench message is request to decrease traffic rate for message sending to the host (decreasing). Or we can say, when receiving host detects that rate of sending packets (traffic rate) it is too fast it sends the Source Quench message to the source to slow the pace so that no packet can be lost.

ICMP will take same IP from the discarded packet and

informs to source by sending Source quench message. Then source will reduce the speed of transmitting so that router will free from congestion.

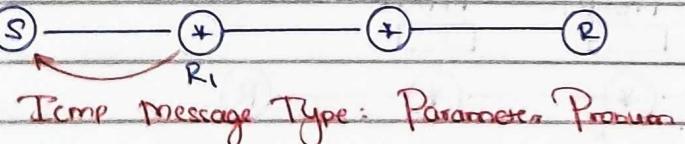
When the congestion router is far away from the source the ICMP will send hop by hop source quench message so that every router will reduce the speed of transmission.



3. Parameter Problem:

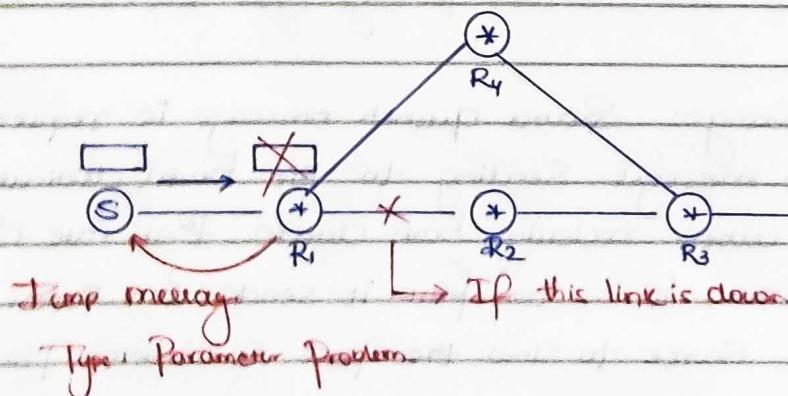
- * Whenever packet come to the router then calculated header checksum should be equal to received header checksum then only packet is accepted by router.
- * If there is a mismatch packet will be dropped by router.
- * ICMP will take the source IP from discarded packet and informs to source by sending Parameter Problem message.

$$\text{Checksum} = x \quad \text{Checksum} = x_{R1}$$



Strict-Source Routing

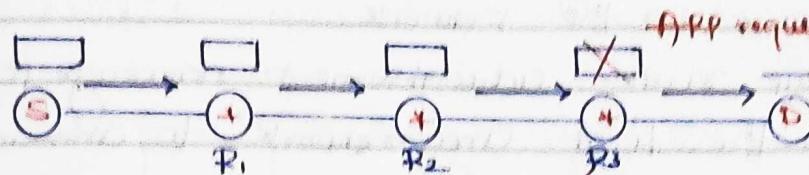
D R1 R2 R3



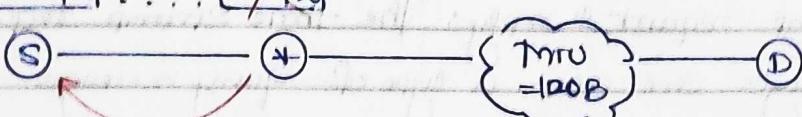
(4) Destination Unreachable:

→ Destination host unreachable

→ Destination port unreachable.



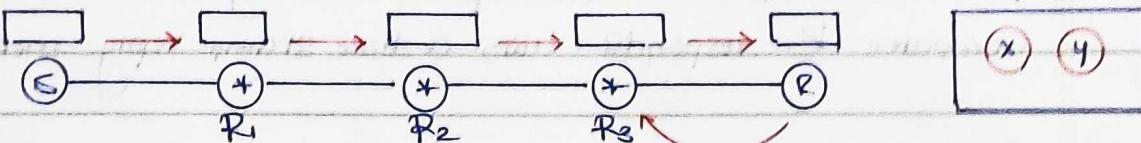
$D_F = 1$
 $\begin{matrix} 30 & 20 \end{matrix} \dots \begin{matrix} 30 & 20 \end{matrix}$



Temp message Type: destination unreachable

Port No. 200

Host



Temp message Type: destination port unreachable.

Host

- (5) Redirection Message: The redirection message is used when the source uses a wrong neighbor router to send out its message. The router redirects the message to appropriate router, but informs the source that it needs to change its default route in the future. The IP address of the default route is sent in the message.

Query Request and Reply

- (1) Echo request and reply: A router or a host can send an echo-request message. It is used to ping a message to another host that "Are you alive". If the other host is alive, then it sends the echo-reply message. An echo reply message is sent by the router or the host that receives an echo request message.

- (2) Power, Solicitation & Advertisement: The Temp router solicitation

message is sent from a Computer host to any routers on the local area network to request that they advertise their presence on the network.

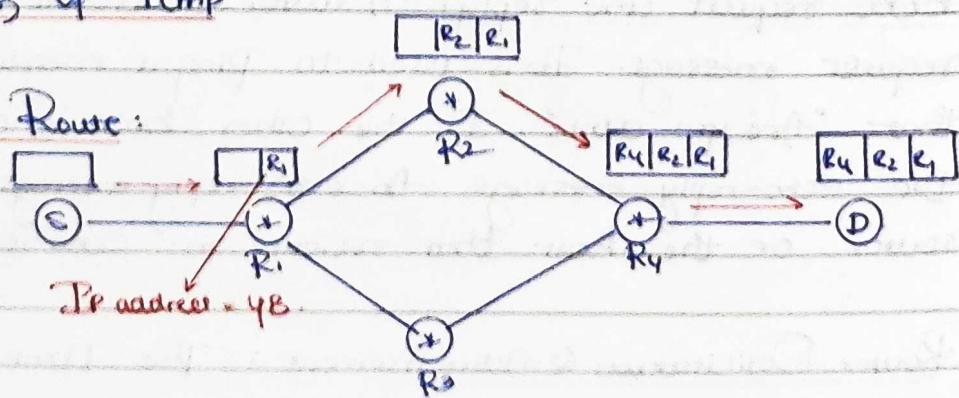
The ICMP router advertisement message is sent by a router on the local area network to announce its IP address as available for routing.

3. Time Stamp request & reply: The time stamp request & timestamp reply messages are also a type of query message. Suppose the computer A wants to know the time of computer B, so it sends the time stamp request message to computer B. The computer B responds with a time stamp reply message.

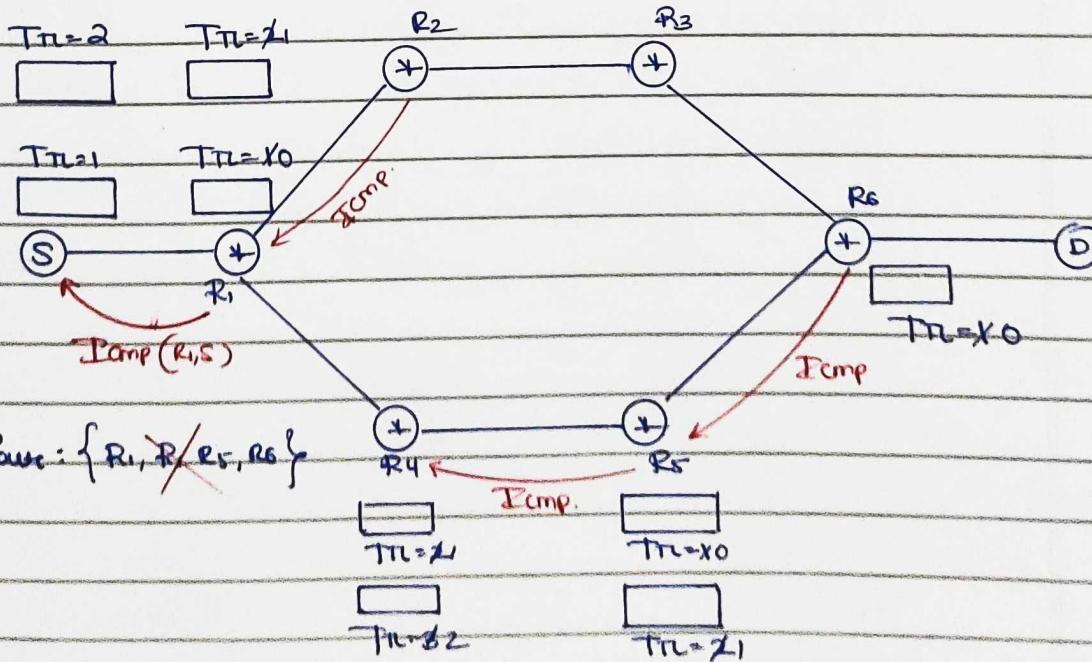
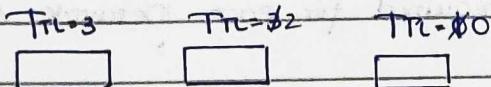
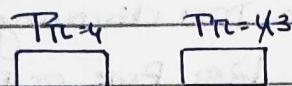
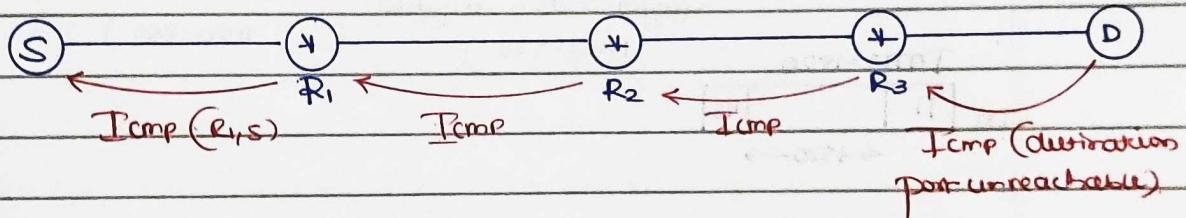
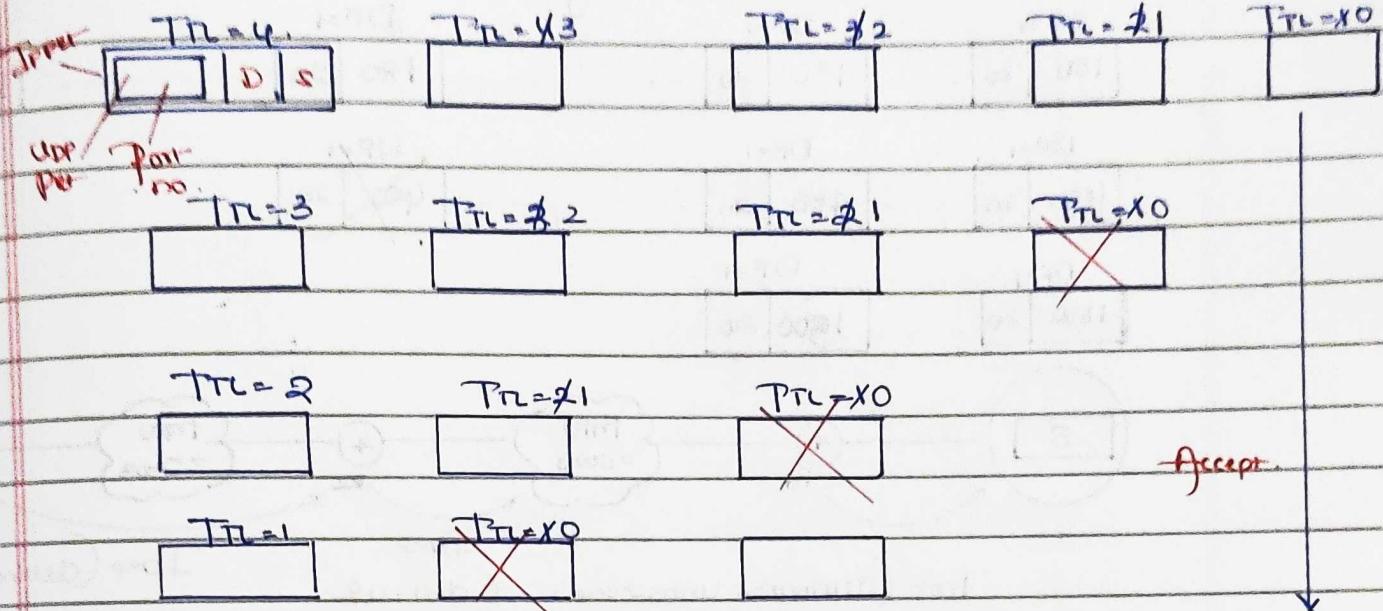
4. Address-mask request & reply: A host may know its IP address, but it may not know the corresponding mask. For example, a host may know its IP address as 192.31.17.24, but it may not know that the corresponding mask is /24. To obtain its mask, a host sends an address-mask request message to a router on the LAN. If the host knows the address of the router, it sends the request directly to the router. If it does not know, it broadcasts the message. The router receiving the address-mask-request message responds with an address-mask-reply message providing the necessary mask for the host. This can be applied to its full IP address to get its subnet address.

Application of ICMP

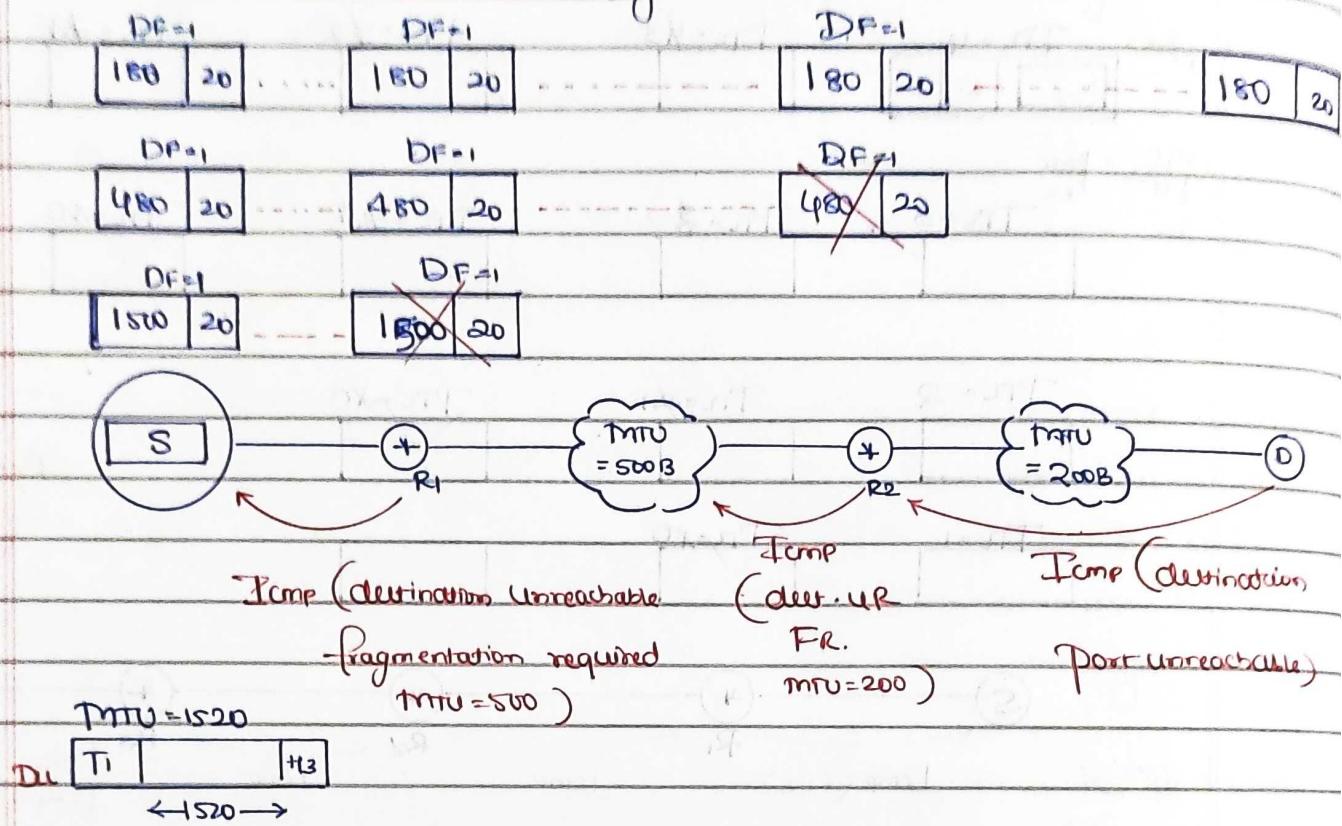
Record Route:



Trace Route: $\{R_1, R_2, R_3\}$



Path MTU Discovery:



Note: If a Source does not use Path MTU discovery technique. It fragment the datagram to a size of 1280 Byte or smaller. This is the minimum size MTU required for each network connected to Internet.