IPV4 ADDRESSING

Basics of IP addressing

$2^1 = 2$	$2^{40} = 1T$ (Tera)
$2^2 = 4$	$2^{50} = 1P$ (Peta)
⋮	$2^{60} = 1E$ (Exa)
$2^9 = 512$	$2^{70} = 1Z$ (Zetta)
$2^{10} = 1024 = 1K$ (Kilo)	$2^{80} = 1Y$ (Yotta)
$2^{20} = 1024 \times 1024 = 1M$ (Mega)	
$2^{30} = 1G$ (Giga)	

Conversions:

1 Byte = 8 bits	1 PB = 1024 TB (Tera Byte)
1 KB = 1024 Bytes	1 EB = 1024 PB (Peta Byte)
1 MB = 1024 KB (kilo byte)	1 ZB = 1024 EB (Exa Byte)
1 GB = 1024 MB (Mega byte)	1 YB = 1024 ZB (Zetta Byte)
1 TB = 1024 GB (Giga byte)	

2 bit	3 bit
00	000
01	001
10	010
11	011
	100
	101
	110
	111

(fixed bit)

1 bit $\longrightarrow$ 2 parts $= 2^1$ part

2 bit $\longrightarrow$ 4 parts $= 2^2$ parts

⋮

K bit $\longrightarrow$ 2^k parts

$\xleftrightarrow{\text{n bit}}$

K	n-K
↓	↓
2^k parts	2^{n-k} (Size of each part)

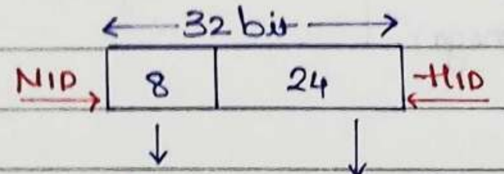
$$\boxed{\begin{aligned} 2^k \text{ parts} &\longrightarrow 2^n \\ 1 \text{ part} &\longrightarrow \frac{2^n}{2^k} \\ &= 2^{n-k} \end{aligned}}$$

$\xleftrightarrow{\text{3 bit}}$

2	1
↓	↓
2^2 parts	$2^1 = 2$ (size of each part)

Introduction to IP Addressing

IPV4 Address = 32 bit
Total number of IPV4 addresses = 2^{32} = 4,294,967,296
Initially in 1980s IP addresses was divided into two fixed parts i.e NID = 8 bit and HID = 24 bit.



2^8 parts $\quad$ 2^{24} (size of each part)

= 256 Network $\quad$ = 2^{24} Hosts / Network

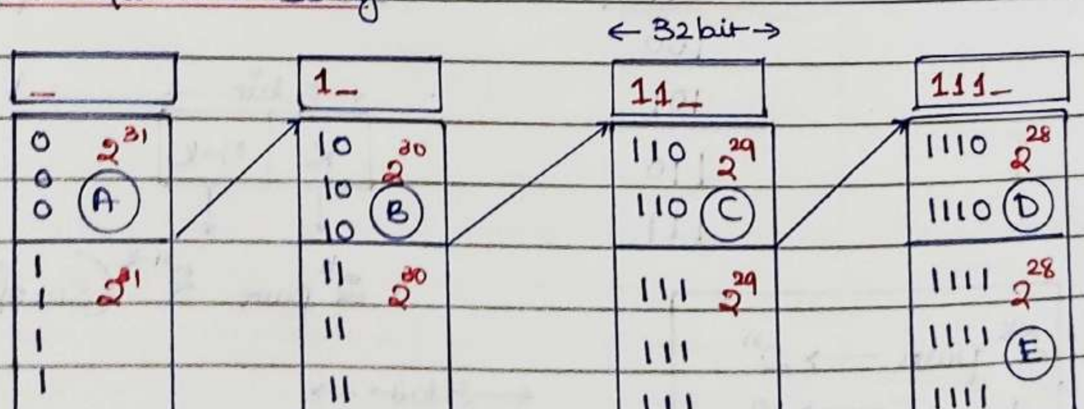
$= 2^4 \times 2^{20}$ = 16 m Host / Network

≅ 1.6 Cr Host / Network

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:

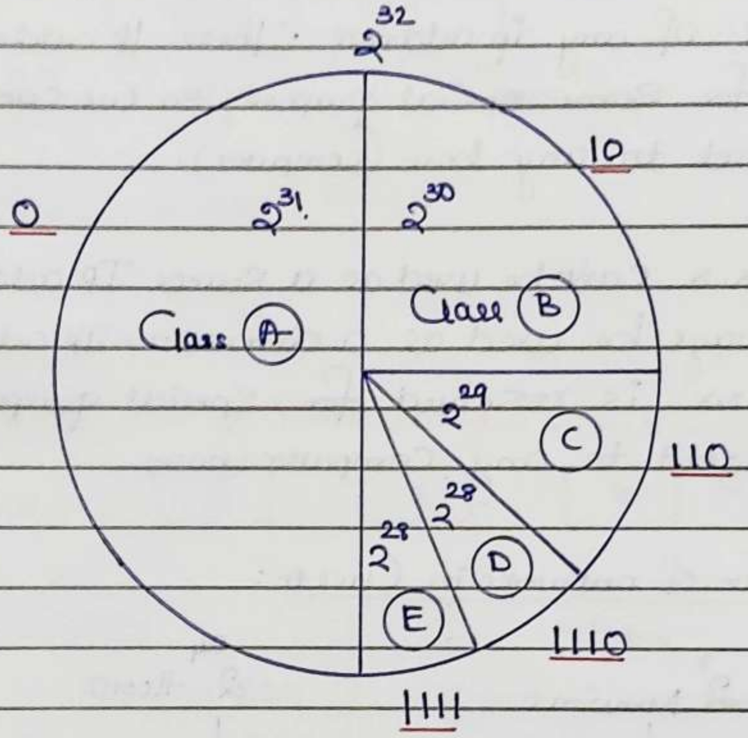


No. of IP address present:

Class A = 2^{31}
Class B = 2^{30}
Class C = 2^{29}
Class D = 2^{28}
Class E = 2^{28}

Class A : 0
Class B : 10
Class C : 110
Class D : 1110
Class E : 1111

{ Fixed bits }



Class A : 50%
Class B : 25%
Class C : 12.5%
Class D : 6.25%
Class E : 6.25%

IP address representation:

Binary :- 11001000. 11111100. 00111111. 11110111
Decimal :- 200. 252. 63. 247
Hexadecimal :- C8. FC. 3F. F7

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

NID	HID		
8 bit	8 bit	8 bit	8 bit

↓

0	7 bit

first bit fixed

00000000 — 0 ✗
0000001 — 1
00000010 — 2
⋮
0111110 — 126
01111111 — 127 ✗

1-126 Range

classmate
Date ____
Page ____

* $\boxed{0.0.0.0}$ default route or DHCP Client

* $\boxed{127.x.x.x}$ Self connectivity / loopback testing / interprocess communication.

* Whenever we have all zero's or all one's 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.IP). 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:

2^8 Networks ↓ $2^7 - 2 = 126$ Networks

2^{24} Hosts ↓ $2^{24} - 2$ Host/Network

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

NID = 16 bit   NID = 16 bit

| 8 | . | 8 | . | 8 | . | 8 |

↓

| 10 | 6 bit |

$10000000 \rightarrow 128$
$10000001 \rightarrow 129$
⋮
$10111111 \rightarrow 191$

128-191 Range

NID = 16 bit
2^{16} N/w's
↓
2^{14} Networks

HID = 16 bit
2^{16} Host/Network
↓
$2^{16} - 2$ Host/Network

Class C : 110 → 2^{29}

NID = 24 bit, HID = 8 bit

| 8 | . | 8 | . | 8 | . | 8 |

↓

| 110 | 5 bit |

110 00000 → 192
110 00001 → 193
⋮
110 11111 → 223

192-223 Range

2^{24} Network → 2^{21} Networks

2^{8} Host/Network → $2^{8}-2$ Host/Networks

Class D : 1110 → 2^{28}

← No NID and No HID →

| 8 bit | . | 8 | . | 8 | . | 8 |

↓

| 1110 | 4 bit |

1110 0000 → 224
1110 0001 → 225
⋮
1110 1111 → 239

224-239 Range

Note:
* No NID and no HID in Class D
* Class D is reserved for multicasting.

Class E : 1111 → 2^{28}

| 8 | . | 8 | . | 8 | . | 8 |

↓

| 1111 | 4 bit |

1111 0000 → 240
1111 0001 → 241
⋮
1111 1111 → 255

240-255 Range

Note:
* No NID and no HID in Class E
* Class E is reserved for research and future purpose.

Q1. Find the class B address from the following:

Ans: 10001111.00000011.11111100.00111100

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

2^{24} IP addresses
= 16 M IP addresses

127.0.0.0 ×
127.255.255.255 ×

Q4. The dotted decimal notation (DDN) format for given Hexadecimal notation C22F1582 is

Ans 192.47.21.130

Q5. The dotted decimal notation (DDN) 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}, $2^{12}-2$

classmate
Date
Page

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:

Ans $8m = 7n$

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

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?

Ans 2^{14}.

Q9 How many hosts can be present in class C?

Ans $2^8 - 2$.

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

Ans 8, 24

Q11 In classful addressing a large part of available addresses are <u>Wasted</u>

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

Ans $2^{14}, 2^{16}$.

No. of IP addresses per network $= 2^{16}$

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

Q13 IP address: 200.198.32.65 which class?

Ans Class C

Q14 Percentage of Addresses occupied by class D are <u>6.25%</u>

Q15 In IPv4 addressing format, the number of networks are allowed under class C address is

Ans 2^{21}

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 127.1.100.1

Class A – 2^{24} IP Addresses in one Network
Class B – 2^{16} 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 problem 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.

eg:: Some protocol might accept the first 8 bit of the data to be the address of sender, the second 8 bit to be the address of reciever 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 produces data at 100 mbps but reciever can process data at any 1 mbps, the transmission will overload the reciever and some data will be lost.

(2) Identification Problem: To send a packet from Source to destin-ation, we need 3 identification steps
a. Identify the network
b. Identify the host with in the network i.e among all computers one Computer is identified.
c. Identify the process within the host.

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

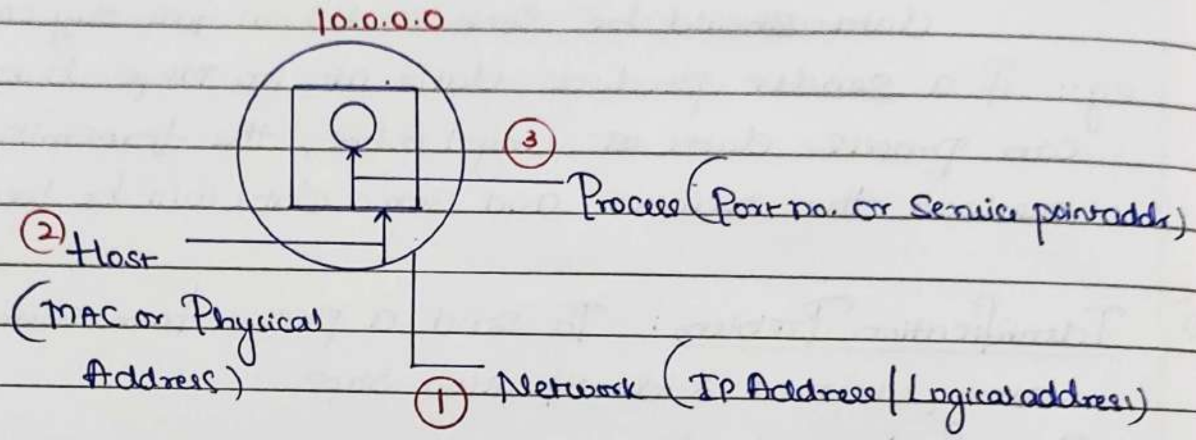
a. Solution for identification of network is IP address or logical address. Now we get destination IP using DNS
b. Solution for identification of Host within the Network is physical address or MAC Address, given an IP address we get MAC address using ARP (Address resolution protocol).
c. Solution for 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 ~~mu~~ unicasting

SIP	DIP
?	10.32..15.73

NID = 10.0.0.0



3 Connection problem: There are various ways to connect the System.

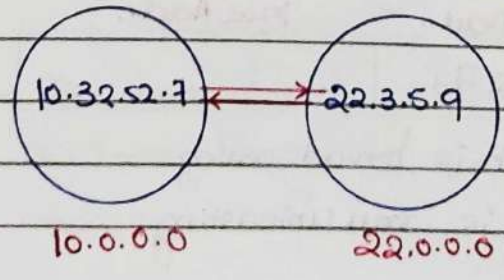
(i) Bus topology
(ii) Rising topology
(iii) Mesh topology
(iv) Tree topology
(v) Star topology

Types of Communication

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

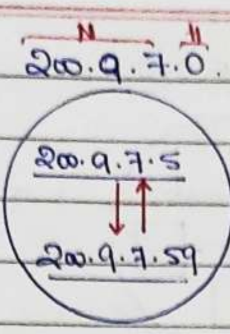
Unicast Communication: Transmitting the data from one Computer to another Computer is called as unicast communication. It is one to one communication.

eg::



SID : 10.32.52.7
DIP : 22.3.5.9 (also vice versa possible)

eg::



Note:
In unicast communication both Source and destination can be present in same network or different network.

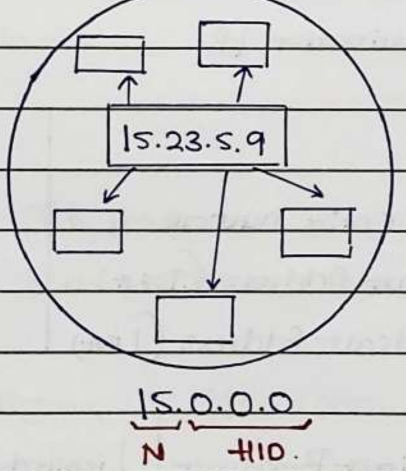
Broadcast Communication

(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::



SID : 15.23.5.9

DIP : 255.255.255.255

Also called as "Limited Broadcast Address".

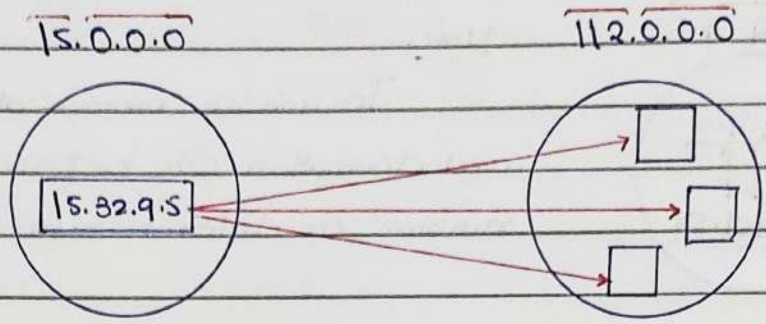
* Limited Broadcast Address cannot be used as a Source address

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

* Dosen'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::



S.I.P - 15.32.9.5

D.I.P - 112.255.255.255

↳ all "one's" in the HID part, it represents direct broadcast address.

Note:

* Whenever we have all 1's in the HID 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 — Direct Broadcast Address (DBA)
1's	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	×	×	×
243.2.3.5	×	×	×

Network Mask:

A network mask helps you to know which portion of the address identifies the network-id and which portion 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 1s indicate NID part and No. of 0's indicate the HID part.

	NID	HID
Class A :	11111111.	00000000. 00000000. 00000000

255 . 0.0.0

Class B : 11111111. 11111111. 00000000. 00000000

255.255.0.0

eg:: IP Address = 200.200.200.96

Network mask = 255.255.255.0 [NID: 200.200.200. HID: 96]

IP Address : 11001000. 11001000. 11001000. 01100000

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 LBA - 255.255.255.255.

Q6 One host having IP addresses 200.187.96.0, Sends 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 as a host?

Ans 157.54.255.254

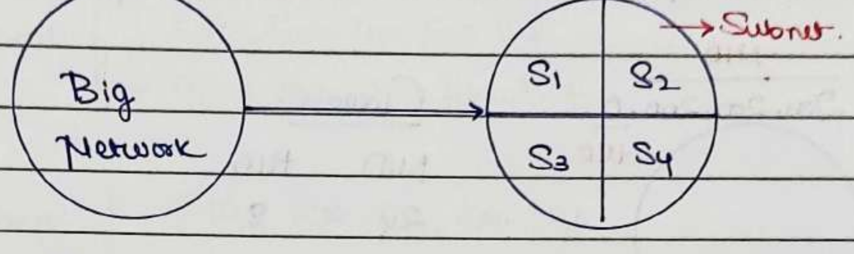
Classful Addressing

Class A : 2^{24} IP Addresses in one network

Class B : 2^{16} IP Addresses in one network

Class C : 2^{8} IP Addresses in one network.

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



Advantages of Subnetting:

1. Maintainence 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 Complicate 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 within the host.

2. In case of single network only two IP addresses are wasted to represented 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 requires an experienced network administator. This adds to the overall cost as well.

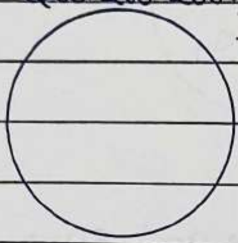
Note: * The process of borrowing bits from HID to generate the subnet ID is also called as Subnetting.

* The number of borrowed bits depends upon the requirement.

NID

200.200.200.0

HID.



Class C

NID	HID
24	8

4 Subnets:

2 6

SID HID

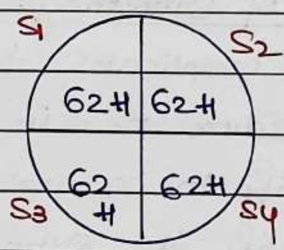
$2^2 = 4$ Subnets $2^6 - 2 = 62$ Hosts / Subnet.

S1 : 00

S2 : 01

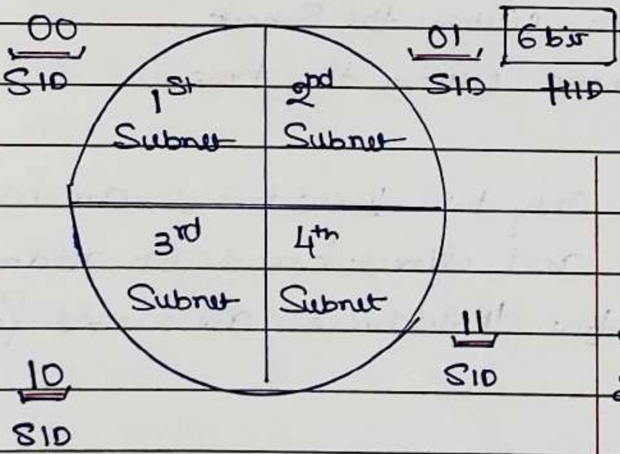
S3 : 10

S4 : 11



NID

200.200.200



1st Subnet

SID HID

200.200.200.00 | 6 bit |

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

DBA: 200.200.200.63

First Host: 200.200.200.1 } Valid hosts from 1-62

Last Host: 200.200.200.62

1 Subnet. SID : 200.200.200.0
DBA : 200.200.200.63.

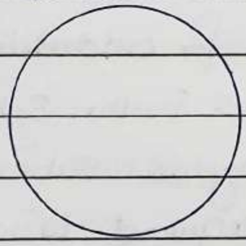
2nd Subnet SID : 200.200.200.64
DBA : 200.200.200.127

3rd Subnet SID : 200.200.200.128
DBA : 200.200.200.191

4th Subnet SID : 200.200.200.192
DBA : 200.200.200.255.

eg:: 2

200.200.200.0



Class C

NID	HID
24	8

8 Subnets

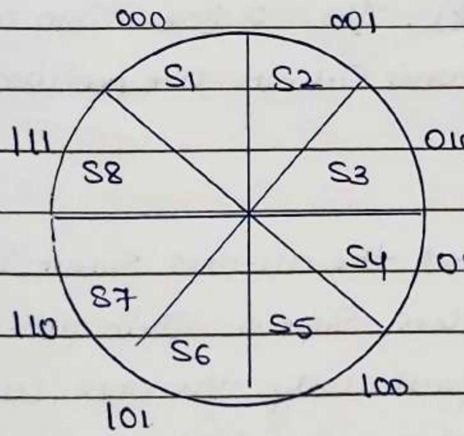
3	5
SID	HID

$= \frac{2^8}{8} = \frac{2^8}{2^3} = 2^5$ IP in one network.

no of Subnets $= 2^3 = 8$

no of IP/Subnet $= 2^5 = 32$

no of Host/Subnet $= 2^5 - 2 = 30$



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

Date 7/3/23
Page

Subnetting Category 1

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

S_{ID} = 2 bit

× 00

01 } valid subnet.

10 } No. of Subnets = $2^2 - 2$ = 2

× 11

Problem with Subnet zero and the All-ones Subnet:

Traditionally it was strongly recommended that subnet zero and the all-one's 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 engineers 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-one's 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 their 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 HID part

Default Subnet mask:	For Class A:
Class A: 255.0.0.0	255.0.0.0
Class B: 255.255.0.0	11111111.00000000.00000000.00000000
Class C: 255.255.255.0	NID+SID = 8, HID = 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 ids: 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 = $2^2 = 4$

Host/Subnet = $2^6 - 2$

= 62

Subnet ids - 200.200.200.-- . ------

AD Rule

128	64	
0	0	0
0	1	64
1	0	128
1	1	192

200.200.200. 00 . 00000000 → 200.200.200.0

200.200.200. 01 . 000000 → 200.200.200.64

200.200.200. 10 . 000000 → 200.200.200.128

200.200.200. 11 . 000000 → 200.200.200.192

255.255.255.224

Q2. If NID = 200.200.200.0 and Subnet Mask = [redacted] then identify.

(i) No of bits borrowed from Host ID = 3.

(ii) No. of Subnets possible and their Subnet ids : $2^3 = 8$

(iii) No of Host/Subnet : $2^5 - 2 = 30$

SID = 3 bit, HID = 5 bit

Subnet ID's : SID = 3 bit

128	64	32	
0	0	0	0
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

Subnet id's (AD rule)

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

(i) Number of bits borrowed from Host-id = 3

(ii) Number of subnets possible and their Subnets id's = 8

(iii) Number of Hosts/subnet. = 30

SM = 11111111.11111111.11111111.00101100

No. of 1's = 27

NID+SID = 27

SID = 3, Subnets = $2^3 = 8$

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

Subnet ids -

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 = 255.255.255.200 then identify.

1. No of bit borrowed from Host-id : 3
2. No of Subnet possible and their Subnet ids : 8
3. No of Hosts/subnet : 30

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

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

Subnet ids :

$173.173.\underset{S}{\_}\underset{HID}{\_\_\_\_\_\_\_}.\underset{S}{\_}\underset{HID}{\_\_\_\_\_\_\_}$

173.173. 0.0000000 · 00000000 — 173.173.0.0
173.173. 0.0000000 1.0000000 — 173.173.0.128
173.173. 1.0000000 0.0000000 — 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 bit 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 HID = 11 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 $HID = 6$ bit, $2^6 - 2$

$= \underline{62}$

Q10 If a class B network on the internet has SM 255.255.240.0 What is max no. of hosts?

Ans $HID = 12$ bit, $2^{12} - 2$

$= 4096 - 2 = \underline{4094}$

Q11. An organization has a class B network and wishes to form Subnets for 64 depts. The subnet mask would be

Ans 64 Subnets

$= 64 = 2^6$, SID = 6 bit

255.255.252.0

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 $2^{HID} - 2$

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

100 host in each lan.

= 7 bits should be HID, remaining 9 bits - SID

= 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 HID, 8 bit SID

= 255.255.255.0

classmate

Date 13/3/23

Page

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 (SID) 5 (HID).

$= 2^3 = 8$ subnet

$2^5 - 2 = 30$ hosts/subnet.

= 255.255.255.224. (first 3 bits borrowed from HID)

= 255.255.255.7 (if last 3 bits borrowed) – 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 200 hosts per subnet. An appropriate Subnet mask for this network?

Class B.

$180 \times 200 \leq 2^{16} - 2$

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

NID HID

16 16

180 subnets $\leq 2^8$. (256)

8 bits to borrow.

SID HID

8 8.

Hosts/subnet $= 2^8 - 2 = 254$

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

Q17 Consider a class C network with 15 subnets and 20 hosts/subnet. An appropriate mask for this network.

Class C

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

$300 \leq 254$ (Not possible)

NID HID

24 8.

15 Subnets

4 4

SID HID. $2^4 - 2 = 14$ 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. NID HID
24 8

A - 120
B - 60
C - 60

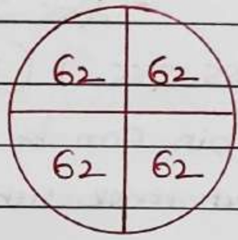
$240 \le 2^8 - 2$ (yes)

Case I: for 3 Subnet:

2 6
SID HID.

$2^2 = 4$ Subnets

$2^6 - 2 = 62$ Hosts | Subnet (Not Possible)



A doesn't fit

Case II:

NID HID
24 8

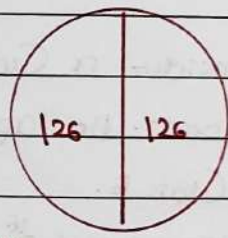
1 7
SID HID.

$2^1 = 2$ Subnets

$2^7 = 128 - 2 = 126$ Hosts | Subnet

(Not possible)

2^8



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

NID HID
24 8

1 7
SID HID

$2^1 = 2$ Subnet.

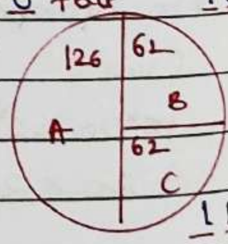
$2^7 - 2 = 126$ Host | Subnet

HID - 7
1 6
SID HID.

$2^1 = 2$ Sub.

$2^6 - 2 = 62$ Host | Subnet

SID 0 7bit



10 6 bit

11 6 bit

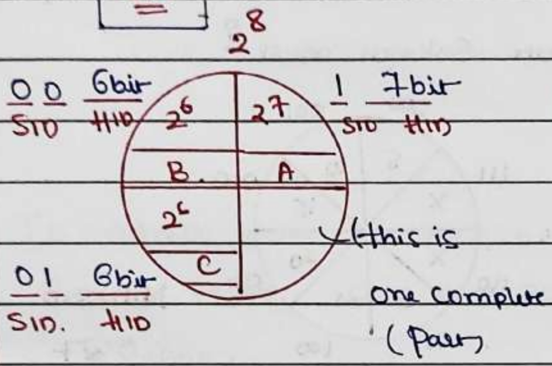
(A) SID :- 200.200.200.0
DBA :- 200.200.200.127
SM :- 255.255.255.128.

(B) SID → 200.200.200.128
DBA → 200.200.200.191
SM → 255.255.255.192

(C) SID → 200.200.200.192
DBA → 200.200.200.255
SM. → 255.255.255.192.

$\left.\right\}$ 1st way of finding the Subnets masks of 3 networks. Also Subnet and masks of B and C can be replaced (both have same Subnet masks).

$\boxed{\text{OR}}$



(A) SID → 200.200.200.128
DBA → 200.200.200.255
SM → 255.255.255.128

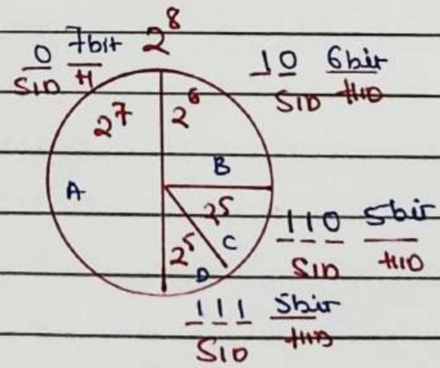
(B) SID → 200.200.200.0
DBA → 200.200.200.63
SM → 255.255.255.192

(C) SID → 200.200.200.64
DBA → 200.200.200.127
SM → 255.255.255.192

$\left.\right\}$ Subnets of B and C can be inter changed $\}$

Q2. Consider a class C network with 4 Subnets and 75, 35, 25, 20 hosts per subnet. An appropriate Subnet mask is?

Class C Network
$75+35+25+20 = 155 \le 2^8 - 2$
(Yes possible)



A → 255.255.255.128
B → 255.255.255.192
C → 255.255.255.224
D → 255.255.255.224.

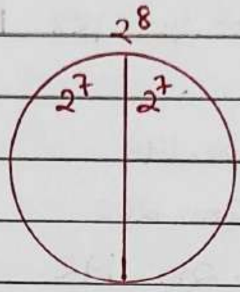
Q3. Consider a Class C network with 3 Subnets and 130, 150, 50 hosts per subnet. An appropriate Subnet mask is?

Ans A = 130

B = 50 $\quad 230 \le 2^8 - 2$

C = 50 $\quad$ (possible)

280



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?

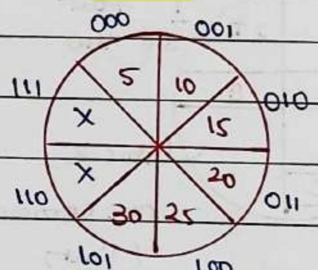
Ans $5+10+15+20+25+30$

$= 105 \le 2^8 - 2$

(possible).

Class C.

6-Subnets



3 $\quad$ 5

SID $\quad$ HID.

$2^3 = 8$ Subnets $\quad 2^5 - 2 = 30$ Hosts/Subnet.

NID+SID = 27

HID = 5

Subnet mask = 255.255.255.224 (Best)

HW

Q5. An organization is granted a block of address with beginning address 14.24.74.0/24. The organisation need to have 3 Sub blocks of addresses to use in its three Subnets: one block of 10 addresses, one subblock of 60 addresses and one sub block of 120 addresses. Find the first and last address of each sub block

Date 13/3/23

Subnetting Category-5.

Q1 IP address: 200.200.200.126

Subnet Mask = 255.255.255.192 then find SID and HID?

IP address = 200.200.200.01111110

Subnet mask = 255.255.255.$\underbrace{11}_{\text{SID}}\underbrace{000000}_{\text{HID}}$

First way (direct)

SID = 64

HID = 62 (of IP address).

mark the 0 place, and write.

Another way:

Host Id = IP address − SID.

HID = 126 − 64

HID = 62

Q2 IP address = 200.200.200.120

Subnet Mask = 255.255.255.240 then find SID and HID.

3rd way:

IP address : 200.200.200.01110

AND AND

Subnet mask : 255.255.255.11110000

200.200.200. 01110000

= 200.200.200.112

3rd method

Q3 IP address = 200.200.200.120

Subnet Mask = 255.255.255.41 then find SID and HID?

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.

Ip address : 200.34.22.~~x~~ 10011100
AND.
Subnet mask : 255. 255 255. 11110000
200. 34. 22. 10010000
= 200. 34. 22. 144

Subnetting Category - 6

Q1. If Subnet mask is 255.255.255.224 the 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^{11}
(e). " " " class C 2^3

255. 255. 255. 224 = 11111111. 11111111. 11111111. 11100000
No. of 1s = 27, No. of 0s = 5
HID = 5 bit, no of subnets = 2^5 = 32
Class A. Host/subnet = 2^5-2 = 30
NID + SID = 27
SID = 19

Class B	Class C
NID+SID = 27	NID+SID = 27
SID = 11.	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
(iii) No of Subnets in class A 2^{20}
(iv) " " " " class B 2^{12}
(v) " " " " class C 2^4

AO Rule
11111111. 11111111. 11111111.
11110000

classmate
Date 14/3/24
Page

Q3 If Subnet mask is 255.255.252.0 then find:

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

No of Host / subnet: $2^{10}-2$ 11111111.11111111.11111100.00000000

No of subnet in Class A 2^{14} Only for A, B

" " " Class B 2^{6}

" " " Class C not possible

Q4 If Subnet mask is 255.252.0.0 the find

No of IP addresses / subnet possible 2^{18}

No of Host / subnet : $2^{18}-2$ 11111111.11111100.0.0

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 - 200.200.200.00011111

HID can be last 5 bits / 4 / 3 / 2 / 1 bit also

Correct options: HID Can be max 5 bit. (HID ≤ 5)

255.255.255.224.

255.255.255.248

255.255.255.252

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

Class B - 168.7.00000111.11111111.

HID Can be maximum 11 bit. (HID ≤ 11)

255.255.~~255~~.248.0

255.255.252.0 } All of the above

255.255.254.0

classmate
Date
Page

Q.3. A Subnetted class B network has the following broadcast address : 144.16.95.255 It's Subnet mask.

Ans Class B. 144.16. 01011111. 11111111.

HID can be maximum of 13 bit. (HID ≤ 13)

255.255.224.0

255.255.240.0

255.255.248.0

Q4. Given DBA: 125.25.63.255 what can be the mask for this Subnetwork.

Ans DBA: Class A.

125. 00011001. 00111111. 11111111.

HID Can be maximum 14 bit. (HID ≤ 14)

255.255. ~~255.~~ 192.0 } Both are
255.255.224.0 } Correct.

Q5. If DBA is 200.200.200.31 which of them Can be Subnet mask?

Ans Class C : 200.200.200.00011111

HID Can be maximum 5 bit (HID ≤ 5)

255.255.255.224 ✓

255.255.255.248 ✓

255.255.255.198. ×

↳ HID ≤ 5 but not Sequential. so not possible

Q6. 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 ✓

classmate

Date

Page

Subnetting Category - 8.

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

Class C : 255.255.255.11111000

Last 3 bits are HID part.

200.32.64.135 ✓

200.32.64.240 ✗

200.32.64.207 ✓

200.32.64.231 ✓

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 bit represents HID 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 bit represent HID

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

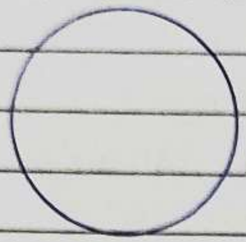
Last 5 bit represent HID part.

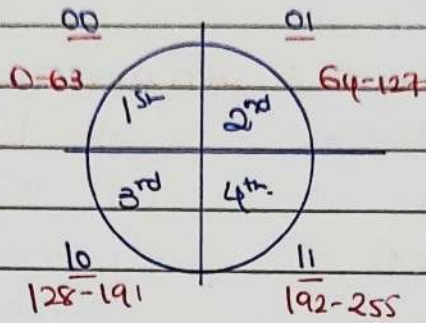
202.15.19.127 } Both are

202.15.19.63 } Correct.

Subnetting Category - 9

eg:: 200.200.200.0



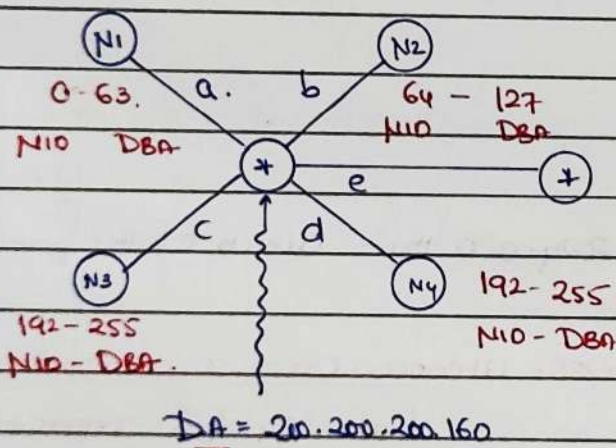


NID	HID
24	8

4 Subnets

2	6
SID	HID

$2^2 = 4$ $\quad$ $2^6 - 2 = 62$ Hosts/Subnet



Routing Table

NID	Subnet Mask	I/F
200.200.200.0	255.255.255.192	a
200.200.200.64	255.255.255.192	b
200.200.200.128	255.255.255.192	c
200.200.200.192	255.255.255.192	d
0.0.0.0	0.0.0.0.	e

default entry.

Note: If destination IP address matched with more than one interface then router will forward the packet will forward ed to the interface with the longest Subnet mask.

Q1. The routing table of a router is shown below:
On which interface will router forward packets addressed to destinations 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. Ao rule: first start with longest 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
144.16.0.0	255.255.255.0	eth0
144.16.64.0	255.255.224.0	eth1
144.16.68.0	255.255.255.0	eth2 ✓
144.16.68.64	255.255.255.224	eth3

A packet bearing a destination address 144.16.68.117 arrives at router, which interface will the packet forwarded?

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 Eth 2.

Q3. A forwarding table of a router shown below:

200.150.0.0	255.255.0.0	1
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

A packet with destination address 200.150.68.118 arrives at router and forwarded to interface 3

classmate
Date ____
Page ____

Ans

DIP: 200.150.68.118	DIP: 200.150.68.118.
AND	AND.
Sm: 255.255.255.224	Sm: 255.255.255.0
200.150.168.96	200.150.68.0
Not matched with I.4.	Matched with interface 3

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

Prefix	SM	Output Int. Ident.
131.16.0.0/12	255.240.0.0	3
131.28.0.0/14	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 ✓

The identifier on the output interface on which packet will the forwarded is 1.

Ans Start with the longest Subnet mask.

DIP: 131.23.151.76	DIP: 131.23.151.76
AND	AND.
Sm: 255.255.0.0	Sm: 255.254.0.0
131.23.0.0.	131.22.0.0
not matched with Int.(2)	Matched with interface (1)

Subnetting Category - 10

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

eg: A. IP_A = 200.200.200.15 B. IP_B = 200.200.200.132.

Sm_A = 255.255.255.128.

NID_A = 200.200.200.0

IP.B = 200.200.200.132
AND
IP.A SM.A = 255.255.255.128
NID.BA = 200.200.200.128.

NID AA ≠ NID BA so 'A' assume that 'B' is present in different network.

eg:: 2. A

IP.A = 200.200.200.15 (AND)
Sm.A = 255.255.255.128.
NID.AA = 200.200.200.0

B.

IP.B = 200.200.200.66 (AND)
Sm.B = 255.255.255.192
NID.BB = 200.200.200.64.

IP.B = 200.200.200.66 (AND)
S.m.A = 255.255.255.128
NID.BA = 200.200.200.0.

* NID.AA = NID.BA = 200.200.200.0 then A assume that B is present in same network.

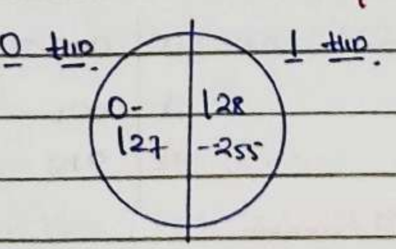
I.P. A = 200.200.200.15 (AND)
S.m.B = 255.255.255.192
NID.AB = 200.200.200.0.

* NID BB ≠ 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 = 255.255.255.1 0000000
SID. HID.

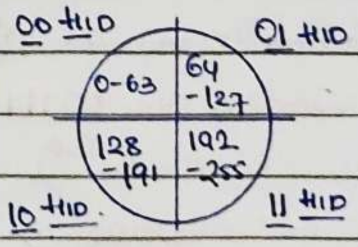
NID SID HID
24 , 1 7. → $2^7 - 2 = 126$
$2^1 = 2$ Subnets. Host/Subnet.



B.

IP. B = 200.200.200.66
S.m.B = 255.255.255.192
NID = 200.200.200.64 [01 000000]
SID.

NID. SID HID
24 , 2 6. $2^6 - 2 = 62$ Host/Subnet
$2^2 = 4$ Subnets.



Date
Page

Q1. Two computers C_1 and C_2 are configured as follows. C_1 has IP address 203.197.2.53 and mask 255.255.128.0 C_2 has IP address 203.197.75.201 and mask 255.255.192.0 which one of following statements is true?

Ans

C_1	C_2
IP.C_1 : 203.197.2.53. (ANDing)	IP.C_2 = 203.197.75.201
Mask.C_1 = 255.255.128.0.	Sm.C_2 = 255.255.192.0
NID C_1C_1 = 203.197.0.0	NID C_2C_2 = 203.197.64.0

IP.C_2 = 203.197.75.201 (ANDing)	IPC_1 = 203.197.2.53
S.m.C_1 = 255.255.128.0	Sm.C_2 = 255.255.192.0
NIDC_2C_1 = 203.197.0.0.	NID.C_1C_2 = 203.197.0.0
* NID C_1C_1 = NID C_2C_1, so C_1 assume C_2 present in same network ✓	* NIDC_2C_2 ≠ NIDC_1C_2, so C_2 assume C_1 is present in different network ✓

Problem Solving on Subnetting:

Q 1. If subnet mask is 255.255.224 then no. of subnets are

Ans 2^{11}, 2^3.

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

Ans 2^{18}, 2^{10}, 2^2.

Q3 IP address in a block = 200.200.200.60 (32+16+8+4) and the subnet mask = 255.255.255.224 (192+64+32) then find

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

(ii) Subnet number = 2^{nd}.

200.200.200.00111100

(SID) 3bit

value = 3 so 2^{nd} Subnet

0	000 - 1^{st} subnet -
1	001 - 2^{nd} subnet
2	010 - 3^{rd} 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

(ii) Subnet number = 3rd subnet

200.200.200.01000000

(decimal value = 2, (3rd subnet)

SM = 255.255.255.224 (128+64+32)

80 (64+16) → 64

Q5 IP address in a block = 200.200.200.122 and SM = 255.255.255.240 then find

(64+32+16

(i) Subnet id = 200.200.200.112

(ii) Subnet number = 8th subnet.

112

01110000 — decimal value = 7 (8th subnet)

SM = 255.255.255.240

11110000

SID.

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

(ii) First host = 157.157.32.1

(iii) Last host = 157.157.63.254

(iv) DBA = 157.157.63.255

157.157.00100000.0

SID.

(32+16+4)

157.157.52.80

255.255.11100000.0

(128+64+32)

SID = 157.157.32.0

157.157.00100000.00000000 → 157.157.32.0 (SID)

157.157.00100000.00000001 → 157.157.32.1 (First Host)

⋮

157.157.00111111.11111110 → 157.157.63.254 (Last host)

157.157.00111111.11111111 → 157.157.63.255 (DBA)

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

(i) Subnet Id: 157.157.0.0

(ii) First host: 157.157.0.1

157.157.52.80

255.255.11000000.00000000

SID = 157.157.0.0

(iii) Last host: 157.157.63.254
(iv) DBA. 157.157.63.255

157.157.000.00000.0 → 157.157.0.0 (SID)
157.157.00.000000.00000001 → 157.157.0.1 (first H)
157.157.00111111.11111110 → 157.157.63.254 (last host)
157.157.00111111.1111111 → 157.157.63.255 (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.

$SM = 255.255.255.\underbrace{111}_{SID - 3bit}00000$

3rd subnet, so decimal value should be 2 = 255.255.255.01000000
= 255.255.255.64.

7th subnet, decimal → 6. = 255.255.255.110.00000.00000000
= 255.255.255.192

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
(ii) 6th subnet id = 200.200.200.80

$SM: 255.255.255.\underbrace{1111}_{SID.}0000$

4th subnet = 0011.
6th subnet = 0101

classmate

Date 16/3/23

Page

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. $\underline{111111}$00. 00000000.00000000

SID. HID.

2nd Subnet. 3rd host: 255. 00000100 . 00000000.00000111.

= 125.4. 0.3.

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

= 125.~~16~~ 8.0.4

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~~ 32.3.

ii. 4th host in 3rd Subnet = 157.157.64.4

iii. 1st host in 4th Subnet = 157.157.128.1.

Ans

SM = 255.255. $\underline{111}$00000.00000000

SID. 2nd subnet → dec value (1). then Calculate.

HW

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. $\underline{1111}$0000

SID.

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 = 255.255.11000000.00000000

M = 157.157.38.90 Check for 3rd octate SID. part.
N = 157.157.48.90 M : 38 00100110 } M, N belong to
P = 157.157.68.90 N : 48 00110000 Same Subnet.
P : 68 01000100 (same bits in SID)

∴ 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 = 255.255.11110000.0
SID.

128 64 32 16
AD Rule: M : 38 : 0 0 1 0 } M, N, P belong
N : 48 : 0 0 1 1 } to 3 diff
P : 68 : 0 1 0 0 } Subnets

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
AD. Rule : 40 : 001
48 : 010 } N and P belong to same network.
68 : 010 }

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? $SM = 255.255.255.\underbrace{111}_{SID}00000$

Ans. M: 200.40.38. $\underbrace{001}_{\substack{\text{d.value} \\ = 1. \\ (2^{nd}\text{ sub})}}\underbrace{10010}_{\substack{\text{d value} \\ 18 \\ (18^{th}\text{ host})}}$

N: 200.92.48. 001 01000

1 → (2^{nd} subnet), HID = 8 → 8^{th} host.

P: 200.80.68. ~~0010 00100~~ 00111100

~~2 → (3^{rd} subnet)~~ 1 → (2^{nd} subnet), HID. = 28, 28^{th} H.

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. $SM = 255.255.\underbrace{111111}_{SID}00.00000000$

M: 157.157. $\underbrace{00101000}_{\text{dvalue} = 10\ (11^{th}\text{ subnet})}$. $\underbrace{00110010}_{\text{dvalue} = 50\ (50^{th}\text{ host})}$

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 = 255.252.0.0 find which host of which subnet.

Date 21/3/23

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 set to 255.255.255.252 for all the three machines.

SM: 255.255.255.11111100

M: 2 = 000000

N: 5 = 000001 } N and P belong to same subnet.

P: 6 = 000001.

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 Option (d)

	128.8.129.43	128.8.161.55
	AND	AND
	255.255.31.0	255.255.31.0
NID =	128.8.1.0 ✓	128.8.1.0 ✓

Q2 Suppose computers A and B have IP address 10.105.1.113 and 10.105.1.91 respectively and they both use the same netmask 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.

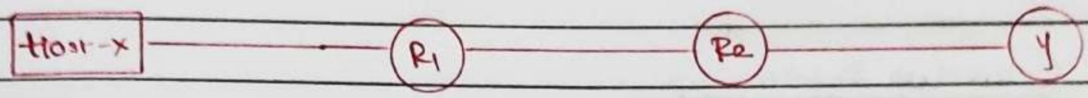
∴ 255.255.255.224

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 → 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.

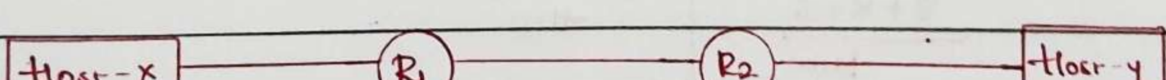


192.168.1.97   192.168.1.135   192.168.1.67   192.168.1.80

192.168.1.110   192.168.1.155.

(AND)						
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 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.
Which IP address should X configure its gateway as?



(b) 192.168.1.110.
AND.
255.255.255.224

192.168.1.96

Disadvantage of Classful Addressing:

1. Wastage 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.

Prefix	Suffix
NID	HID

← 32 bit →

eg:: 10.32.96.64/22

NID = 22 bit, HID = 32-22 = 10 bit

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

No. of Host possible = $2^{10}-2$

$\underbrace{10.32.010111}_{\substack{8+8+6 \\ NID}} \mid \underbrace{10.01000000}_{HID}$

CIDR (Classless Inter Domain Routing)

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

Rules to be followed by IANA for creating the block.

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

classmate
Date
Page

2. Block Size must be a power of 2

$\longleftarrow$ n-bit $\longrightarrow$

n-k	k bit
Q	R

/ 2^k

Block Size = 2^5

32 bit

27 bit	5 bit
Q	Rem.

/ 2^5

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

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

eg:: One of the address of the Block is 100.100.100.68/27 then find
1. Number of address in a block : 2^5.
2. Range of IP address :

NID = 27 bit
HID = 32-27 = 5 bit

100.100.100.010|00100
$\underbrace{8+8+8+3}_{NID}$, $\underbrace{5}_{HID}$

~~100.100.~~

100.100.100.010|00000 — Block id
F.Host — 100.100.100.010|00001
⋮
100.100.100.010|11111 — DBA
Range

3. Block id | Network id : 100.100.100.64
4. First host : 100.100.100.65,
5. Last host : 100.100.100.95.
6. DBA : 100.100.100.96.

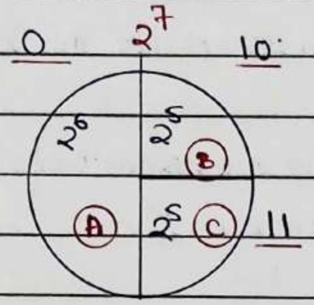
eg:: One of the address of the Block is given as 167.199.128.3/20, Find.
1. Number of addresses in a block = 2^{12}.
2. Range of IP addresses :
3. Network id and DBA
= 168.199.128.0, 168.199.143.255
4. First and last host.
= 168.199.128.1, 168.199.143.254

167.199.1000	000000000000	— 168.199.128.0
167.199.1000	0000.00000001	— 168.199.128.1
⋮		⋮
167.199.1000	1111 0000.11111110	— 168.199.143.254
167.199.1000	1111 0000.11111111	— 168.199.143.255

VLSM in CIDR

1. 100.100.100.14/25
NID = 25 bit
HID = 32 − 25 = 7 bit
No. of IP addresses = $2^7 = 128$
No of Host = $2^7 - 2 = 126$
100.100.100.0 0001110
↳ NID = 25. ↳ HID = 7 bit

CSE A = 60
CSE B = 30
CSE C = 30
$120 \le 2^8 - 2$ (Yes)



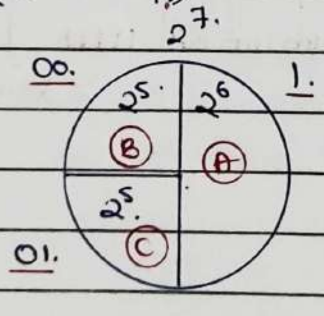
CSE A : SID : 100.100.100.0/26
DBA : 100.100.100.63/26

CSE B : SID : 100.100.100.64/27
DBA : 100.100.100.95/27

CSE C = SID : 100.100.100.96/27
DBA : 100.100.100.127/27.

* B and C are interchangable (2nd way)

(3rd way)



A : SID : 100.100.100.64/26
DBA : 100.100.100.127/26

B : SID : 100.100.100.0/27
DBA : 100.100.100.31/27

C : SID : 100.100.100.32/27
DBA : 100.100.100.63/27

* B and C are interchangable (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. 200.10.11.10010000 — 200.10.11.100_____

NID = 27, HID = 5 bit — 200.10.11.100 11110

158 (last host)

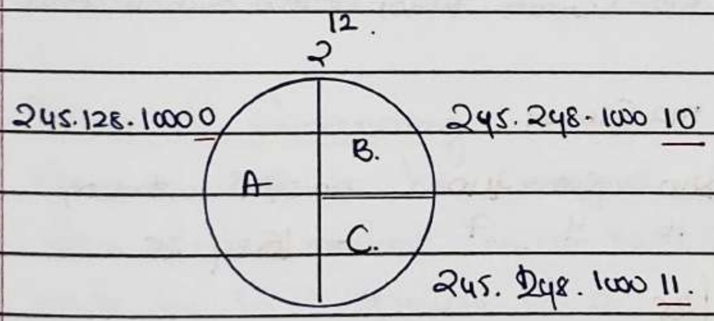
Q2. An internet Service provider has following chunk of CIDR based IP addresses available with it: 245.248.128.0/20. The ISP wants to give half of the chunk of addresses to Organization A, and a quarter to Organization B, while retaining the remaining with itself. Which of the following is a valid allocation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

Ans. 245.248.1000 0_____

NID. SID. HID = 11 bit

no. of IP addresses = $2^{12} = 4096$

no. of hosts = $2^{12} - 2 = 4094$



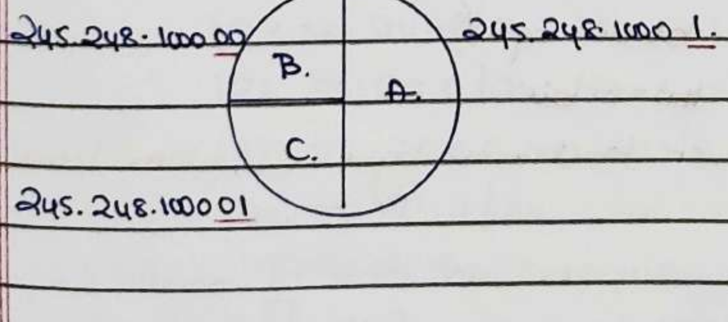
A : 245.248.128.0/21

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.

classmate

Date ____

Page ____

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

NID = 20 bit, HID = 12 bit

203.207.1010

→ 203.207.160.0 NID

2> 203.207.1011

203.207.10110000.00000000.

= 203.207.176.0

3> 203.207.1101|0000.00000000

= 203.207.208.0

Q4. An organisation is granted the block 150.36.0.0/16. 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
16	9	7

no of 1s in the SM = 16+9 = 25

= 255.255.255.128/25

Q5. Block contains 64 IP address which of the following can be first addresses 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 the 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?

classmate
Date 29/3/23
Page

Ans 199.16.16.0
199.16.16.160

Qs. Which of the following would support best point to point link?

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

Advantages of Supernetting:

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

eg::1. 128.56.24.0/24 NID = 24bit, HID = 2^8 IP
128.56.25.0/24 NID = 24bit, HID = 8bit, 2^8 IP
128.56.26.0/24 NID = 24bit, HID = 8bit
128.56.27.0/24, NID = 24bit, HID = 8bit.

1. Network ID must be contiguous
N1: 128.56.24.0000000 → 128.56.24.0
128.56.24.00000001 → 128.56.24.1

classmate
Date
Page

128.56.24.00000010 → 128.56.24.2
⋮ ⋮ ⋮
128.56.24.11111111 → 128.56.24.255
+1
128.56.25.0

N2: 128.56.25.0
128.56.25.00000000 → 128.56.25.00000000
128.56.25.00000001 → 128.56.25.1
| ⋮ ⋮
128.56.25.11111111 → 128.56.25.255
+1
128.56.~~25~~.~~288~~ +1
128.56.26.0

N3: 128.56.26.0
128.56.26.255 +1
= 128.56.27.0.

N4: 128.56.27.0
128.56.27.255 +1
= 128.56.28.0.

∴ Network IDs are contigous

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

: Same 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 = $2^8+2^8+2^8+28 = 2^{10}$.

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

eg: 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 = 255.255.252.0

11111111. 11111111. 11111100. 00000000.

AD rule:	AD rule for Subnet mask
Supernet id: First IP address Always	Total Size of Supernet = $2^8 \times 4$
Supernet id = 128.56.24.0	$= 2^{10}$
	HID = 10 bit
	NID = 32-10 = 22.

Supernet mask = 255.255.252.0.

Problem Solving on Supernetting:

Q1. Perform CIDR 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 → HID = 11 bit of an IP address
→ Network id is contigous
→ no of networks = $4 = 2^2$
→ First NID must be divisible by the Size of Supernet.
$2^{11} \times 4 = 2^{13}$.
57.6.011<u>00000.00000000</u>/2^{13}.

Supernet mask = <u>57.6.96.0/19</u>

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 contigous
2. Same size of networks, networks must be power of 2.

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

194.24.0.0
194.24.0000<u>0000.00000000</u>/2^{12}. (True)
Rem/HID.

= 194.24.0.0/20 }
194.24.16.0/20 }
1. Contigous (True)
2. Same Size = 12 bit, no of n/works = 2^1.
3. Total Size of Supernet = $2^{12} + 2^{12} = 2^{13}$

194.24.0.0
194.24.000<u>00000.00000000</u>/2^{13} (True)

Supernet id = 194.24.0.0, total size = 13 bit
Ans = <u>194.24.0.0/19</u>

Supernetting in Classfu Addressing:

eg1. 200.96.86.0 — 1. Contigous (True)
200.96.87.0 — 2. Same size, 2^8, no of n/ws $= 4 = 2^2$
200.96.88.0 — 3. Size of Supernet $= 2^8 \times 4$
200.96.89.0 — $= 2^{10}$.

200.96.86.0
$200.96.010101\underbrace{10.00000000}_{\text{Rem.}}$

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. Contigous (True)
128.57.0.0 — 2. Same Size $= 2^{16}$. no of n/w's $= 4 = 2^2$.
128.58.0.0 — 3. Total Size of Supernet $= 4 \times 2^{16} = 2^{18}$.
128.59.0.0

128.56.0.0
$= 128.001110\underbrace{00.00000000.00000000}_{\text{Rem / Hid}} / 2^{18}$ (True)

Total size of Supernet $= 2^{18}$
HID = 18 bit, NID = 14 bit.
Supernet mask: 255.252.0.0

	Subnet Mask	Supernet Mask
1.	No. of 1's in the Subnet mask 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.	Supernet mask is applicable for two or more network or Supernetting is applicable for two or more n/ws.
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 prefixes 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)

(i) $\underbrace{12.20.101001}_{NID}$ | $\underbrace{00.00000000}_{HID}$

Range of (i)

12.20.164.0

↓

12.20.167.255

(ii) 12.20.1010101|0.00000000 Range: 12.20.170.0
NID | HID ↓
12.20.171.255

(iii) 12.20.168.0
= 12.20.1010100|0.00000000 Range: 12.20.168.0
NID HID ↓
12.20.169.255

(iv) 12.20.166.0
= 12.20.1010011|0.00000000 Range: 12.20.166.0
NID HID ↓
12.20.167.255

* Network 4 is the part of network I. 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 n/ws = 2 = 2^1
3. Total size of Supernet = $2^9 \times 2 = 2^{10}$
12.20.101010|00.00000000/2^{10}
Rem/Hid part.

Supernet id = 12.20.168.0

12.20.164.0/22 }
12.20.168.0/22 }
1. Contiguous (true)
2. Same size = 2^{10}, no. of n/ws = 2
3. Total size of Supernet = $2^{10} + 2^{10} = 2^{11}$.
12.20.10100100.00000000/2^{11}
Rem or Hid part.

Answers:
12.20.164.0/22
12.20.168.0/22

Date
Page

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, 198.44.33.0, 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

$= 198.47.001000|00.00000000 / 2^{10}$ ← Rem. →

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 n/ws $= 4 = 2^2$

3. Total Size of Supernet $= 2^{10}$.

199.202.000000|00.00000000 $/2^{10}$ ← Rem or Hid →

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 = 255.255.111$\overline{00000}$000.00000000

(Supernet id = 5 bit

• No of n/ws must be combined $= 2^5 = 32$

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

Ans Supernet mask : $\underbrace{11111111.11111111.111111}_{NID}\underbrace{00}_{ID}.00000000$ HID.

No. of n/ws 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 = 255.255.111111$\underbrace{00}$.0

Supernet bits

$= 2^2 = 4$

N1 = 00	N3 = 10
N2 = 01	N4 = 11

201.99.010110 $\underbrace{\_\ \_}_{\text{Supernet bits}}$. _ _ _ _ _ _ _ _

N1 = 201.99.010110.00.0 → 201.99.88.0
↓
201.99.010110 00.255 → 201.99.88.255

N2 = 201.99.01011001.0 → 201.99.89.0
↓
201.99.89.255

N3 = 201.99.01011010.0 → 201.99.90.0
↓
201.99.90.255

N4 = 201.99.01011011.0 → 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 it's supernet mask.

Ans. S_m = 11111111. 11111111. 11111111. 00000000
NID.

Supernet mask : 11111111. 11111111. 11110000. 00000000
Supernet id = 4 bit

Supernet mask = 255.255.240.0

(a) $255.255.(2^{8-m}-1)\times 2^m = (2^{8-4}-1)\times 2^4$
$= (240)$ ✓

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

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

Q8. An organization requires a range of IP addresses to assign one to each of its 1500 computers. The organized 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 space are potential candidates from which the ISP can allot any one to the organisation?

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, NID = 17 bit, HID = 32-17 = 15 bit
202.61.00000000.00000000
.
202.61.01111111.11111111
} Range

(III) 202.61.64.0/21, NID = 21 bit, HID = 11 bit
202.61. 01000000.00000000 / 2^{11} (true)

(IV) 202.61.104.0/21, NID = 21 bit, HID = 11 bit
202.61. 01101000.00000000 / 2^{11} (true)

Ans = II and III

Q9. An Internet Service Provider (ISP) is granted a block of addresses 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.

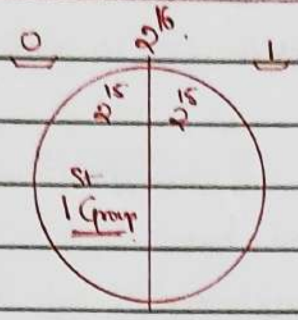
Ans 162.72.0.0/16 NID = 16 bit, HID = 16 bit
No. of IP addresses available in the block = 2^{16} = 65,536

I. First Group = 128 customers each need 256 Addresses
$128 \times 256 = 2^7 \times 2^8 = 2^{15}$ Addresses

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

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

IP addresses available $= 2^{16} - (2^{15} + 2^{13} + 2^{13})$
$= 2^{16} - (2^{15} + 2^{14})$
$= 2^{16} - 2^{14}(2^1 + 1) = 2^{16} - 3 \times 2^{14}$
$= 2^2 \times 2^{14} - 3 \times 2^{14}$
$= 4 \times 2^{14} - 3 \times 2^{14} = \underline{2^{14}}$



162.172.0 0000000.00000000
SID

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

NID-16, HID-16

First Group: $\underbrace{1}_{SID}$ $\underbrace{15}_{HID}$

162.72.0.0/17

NID HID
17 15.

128 customers or Subnet.

17 7 8
NID SID HID

162.72.0 $\underbrace{-------}_{SID}$. $\underbrace{--------}_{HID}$

1st group = 1st customer

162.72.0.$\underbrace{0000000}_{SID}$. 00000000 – 162.72.0.0/24

162.72.0 0000000.1111111 – 162.72.0.255/24

1st Group → 2nd Customer

162.72.00000001.00000000 – 162.72.1.0

162.72.00000001.1111111 – 162.72.1.255

1st Group → 3rd Customer

162.72.00000010.00000000 – 162.72.2.0

162.72.00000010.~~0~~1111111 – 162.72.2.255

1st group : 128th customer

162.72.127.0/24 → 162.72.127.255/24

2nd Group

162.72. 100 ________

NID SID HID

162. 72. 100 00000. 00000000 — 162.72.128.0/19

162. 72. 100 11111. 11111111 — 162.72.159.255/19

NID HID
19 12. 128 customer or 128 customer

→ 19 7 6
NID SID. HID.

2nd Group — 1st customer

162.72.100 _ _ _ _ _ . _ _ _ _ _ _ _ _
SID SID HID

162. 72. 100 00000. 00 000000 → 162.72.128.0

162. 72. 100 00000. 00 111111 → 162.72.128.63/26

HW

Continue the calculation

ERROR CONTROL

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

Types 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.

eg::

Burst length = 4

Sent : 01001010

Recieved : 01101110

eg::1 Data rate = 1kbps = 10^3 bits/sec

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

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

eg::2 Data rate = 1mbps = 10^6 bits/sec

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

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

Error Control

→ Error Detection

→ Error Correction.

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
= Data rate × Noise duration.

Redundancy:
1) The central concept of dectecting 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 recieved by the reciever.

Error dectection: In error dectection we are only looking to see if any error has occured. 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 dectection and error correction points:

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

classmate
Date
Page

Error Control

Error Detection | Error Correction

Error Detection	Error Correction
1. Simple parity	1. Hamming code
2. 2D parity	
3. Check Sum	* Capability of correcting error
4. CRC	* Does not require retransmission
5. Data + Data.	* Hamming code can correct Single bit error.
* 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 = 00|01|10|11 $K = 2$

dataword.

Let $K = 2$ bit and $r = 1$ bit So dataword is of 2 bit and code word is of 3 bit ie. $n = K + r$.

Dataword = K bit
2^k combinations

Codeword = n bit
2^n combinations

$(n > k)$ $2^n - 2^k$ = Codewords that are not used → invalid code words.

Dataword	Valid codeword
00	→ 000
01	→ 011
10	→ 101
11	→ 110

Codeword = 3 bit

000 ✓
001 ✗
010 ✗
011 ✓
100 ✗
101 ✓
110 ✓
111 ✗

Invalid code words

$2^n - 2^k$ → Invalid codewords
$2^3 - 2^2 = 4$

Codeword

Valid Codeword (2^k) — Invalid Codeword $(2^n - 2^k)$

* 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 correspondance 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 reciever can detect a change in the original codeword.
1. The reciever has a list of original codeword
2. The original codeword has changed to invalid one

classmate

Date

Page

- Each codeword sent to the reciever may change during transmission:

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

Hamming Distance:

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

- $d(000, 011) = 2$ (Hamming distance)
- $d(10101, 11110) = 3$ (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 smallest Hamming distance between all possible pairs of code words

eg:: Valid code words.

010 (a)
101 (b)
110 (c)
001 (d)

$$\left.\begin{array}{l} d(a,b) = 3 \\ d(a,c) = 1 \\ d(a,d) = 2 \\ d(b,c) = 2 \\ d(b,d) = 1 \\ d(c,d) = 3 \end{array}\right\}$$ Minimum hamming distance = 1

Minimum Hamming distance for error detection:

1. Sent: 010 → received: 110 (1 bit error)

Valid code word. Reciever can detect one bit error.

2. 010 → 011 (1 bit error)

Invalid code word. Can detect one bit error.

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

eg:: 2

Valid code word

000 (a)
011 (b)
101 (c)
110 (d)

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

Minimum hamming distance = 2.

1. 000 → 100 (1 bit error)

Invalid code word: Can detect one bit error.

(a) $000 \xrightarrow{\text{1 bit error}}$ 100, 010, 001 } Invalid code words

(b) $011 \xrightarrow{\text{1 bit error}}$ 111, 001, 010 } Invalid code word

(c) 101 → 111, 001, 010 } Invalid code word

(d) 110 → 010, 100, 111 } Invalid code word

Note: all one bit error can be detected.

(2)

000 —— 2 bit error —— 110

Valid code word
Can't detect 2 bit error.

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

Min HD.

Valid code word $\xrightarrow{\text{1 bit error}}$ Invalid code word $\xrightarrow{\text{1 bit error}}$ Valid code word

Reciever can detect all one bit error.

eg :: 3.

Valid code word	
00000 (a)	d(a,b) = 3
01011 (b)	d(a,c) = 3
10101 (c)	d(a,d) = 4
11110 (d)	d(b,c) = 4
	d(b,d) = 3
	d(c,d) = 3.

Minimum hamming distance = 3.

00000 —— 1 bit error —— 10000

Invalid code word
Can detect one bit error.

(a) 00000 $\xrightarrow{\text{1 bit error}}$ 10000, 01000, 00100, 00010, 00001 } Invalid code word

Note: all one bit error can be detected.

00000 —— 11000

Invalid code word
Can detect 2 bit error

$00000 \xrightarrow{\text{2 bit error}}$ 11000, 01100, 00110, ⋮ } Invalid code word

Note: All 2 bit error detected.

| 00000 | 3 bit error | 11100 | Invalid code word — can detect 3 bit error

| 00000 | 3 bit error | 01011 | Valid code word — Can't detect 3 bit error

Note : * All 3 bit error can't be detected.
* If minimum hamming distance = 3

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

Min H.D = 3. | Valid Codeword | $\xrightarrow{\text{1 bit error}}$ | Invalid Code word | $\xrightarrow{\text{1 bit error}}$ | Invalid Code word | $\xrightarrow{\text{1 bit error}}$ | Valid Codeword |

Can't detect all 3 bit error.

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

non zero valid code words:

(b) 011

(c) 101

(d) 110

XOR (a,b) = 011

XOR (a,c) = 101

XOR (a,d) = 110

XOR (b,c) = 110

XOR (b,d) = 101

XOR (c,d) = 011

} All valid code 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 ×

non zero code words:

001

011

100

110

Min. no. of 1's = 1.

Minimum hamming distance = 1.

Minimum Hamming Distance for Error Correction:

Min HD = 2: Valid codeword $\xrightarrow{\text{1 bit error}}$ Invalid Codeword $\xrightarrow{\text{1 bit error}}$ Valid code word — Can detect all one bit error

classmate

Date ______
Page ______

Ex:

Valid code word

1001 } Minimum
1010 } hamming dist. = 2.

	Sent	Recieved	
①	1001	1011	Invalid code word - Can detect one bit error, not corr.
	1 bit error.		
②	1010	1011	Invalid code word It can detect one bit error but Cannot correct 1 bit error.
	1 bit error.		

Ex: 2

Valid code word

0000 } Min. Hamming
0011 } distance = 2

Sent	Recieved	
0000	0010	Invalid code word It can detect one bit error but Cannot correct 1 bit error.
1 bit error.		
0011	0010	Invalid code word It can detect one bit, but Can't correct one bit error
1 bit error.		

Ex: 4.

Valid Code word

0000 } Min Hamming
1111 } distance = 4

Sent	Recieved	
0000	0001	Invalid code word It can detect and correct all one bit error.
1 bit error.		
0000	0011	Invalid code word It can detect two bit error but cannot correct 2 bit error.

Note:

1. To correct minimum one bit error minimum hamming distance required = 3 = 2×1+1
2. To correct two bit error minimum hamming distance = 5 = 2×2+1
3. To correct 'd' bit error minimum hamming distance required = $2 \times d + 1$

classmate
Date
Page

Problem Solving on Hamming Code

1. Consider a binary code that consists of only four valid code words 00000, 010111, 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 d bit error = 2d+1
$2d+1 = 3$
$2d = \cancel{2},\ 2d = 2$
$\therefore\ d = \frac{2}{\cancel{2}} = \underline{\underline{1}}$

2. What is the distance of the following code?
000000, 010101, 000111, 011001, 111111

Ans Hamming distance = 2 (minimum)

3. An error correcting code has the following codeword: 0000000, 0000111, 01010101, 11110000 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 = $d+1 = 10+1 = \underline{\underline{11}}$

Error Control

Error direction	Error Correction
1. Simple parity	1. Hamming code.
2. 2-D parity	
3. CRC	
4. Check Sum.	

Simple parity:

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

Simple parity.

Even parity	Odd 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 pattern with four or more error 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
1st row	2nd row	3rd row	4th row	5th row.

By using even parity.

						Row 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

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	
0	1	0	0	0	0	1	
	↑						

* One bit error detected as well as Corrected
* One bit will affect 2 parity.

Two Error:

0	1	0	0	1	0	0	
0	1	1	0	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	
	↑		↑				

* It can detect two bit error but Can't correct two bit error.
* 2 bit error will affect max 4 bit.
* 2 bit error will affect minimum 2 bit.

Three Error:

0	1	0	0	0	0	0	←
0	0	0	1	0	1	1	←
1	0	0	1	0	1	1	
1	1	0	0	1	1	1	←
0	0	1	0	0	1	0	
0	1	0	0	0	0		
↑	↑		↑				

* 3 bit error detected but not corrected
* 3 bit error will effect maximum 6 Parity bits, and minimum 2 parity bit.

Four Error.

0	1	0	0	1	0	0
0	0	0	0	0	1	1
1	0	0	1	0	1	1
1	0	1	0	1	1	1
0	0	1	0	0	1	0
0	1	0	0	0	0	1

4 bit error can't be detected

0	0	0	0	1	0	0
0	1	1	1	0	1	1
1	0	0	0	0	1	1
1	1	1	0	0	1	1
0	0	1	0	0	1	0
0	1	0	0	0	0	1

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 1s in a non-zero valid code word with the smallest number of 1s.

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

Divisor or CRC generator = 1101

```
1101 ) 1001001000
       1101
       ----
        100001000
        1101
        ----
          10101000
          1101
          ----
           0111000
            1101
            ----
             01000
              1101
              ----
         ~~0001~~ 0111 → CRC Remainder
```

Codeword = 1001001111
(Transmitted data)

Codeword = Dataword + CRC
= 1001001000
+ 111
= 1001001111

If reciever recieved uncorrupted data:

```
1101 ) 100100 1111
       1101
       ----------
       10000 1111
        1101
       ----------
         1010 1111
         1101
       ----------
          1111111
          1101
       ----------
            10111
            1101
       ----------
             1101
             1101
       ----------
              000   Syndrome = 0
```

* If syndrome ≠ 0 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 'r' of $g(x)$ (higher power)
2. Determine $x^r d(x)$
3. Determine the remainder by dividing $x^r d(x)$ by $g(x)$
4. Codeword = $x^r d(x)$ + remainder.

eg:: Dataword $d(x)$ = 1001001

$$\begin{array}{ccccccc} 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ x^6 & x^5 & x^4 & x^3 & x^2 & x^1 & x^0 \end{array} = x^6+x^3+1.$$

Divisor

$$\begin{array}{cccc} 1 & 1 & 0 & 1 \\ x^3 & x^2 & x^1 & x^0 \end{array} = x^3+x^2+1. \text{ (higher power : } x^3) \quad r=3$$

$$x^r dx = x^3(x^6+x^3+1)$$
$$= x^9+x^6+x^3.$$

$x^3+x^2+1 \,\big)\, x^9+x^6+x^3 \,\big(\, x^6+x^5+x^4+x^3+x+1$

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

$\cancel{x^9}\quad x^8+x^3$

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

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

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

$\cancel{x^6}+\cancel{x^5}+x^4+\cancel{x^3}$

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

$\cancel{x^4}$

$\cancel{x^4}+x^3+x$

$\cancel{x^3}+x$

$\cancel{x^3}+x^2+\cancel{x}\,1$

x^2+x+1 — Remainder or CRC

Codeword = $x^r d(x)$ + Remainder

$= x^9+x^6+x^3+x^2+x+1$

Codeword = 1001001111

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 $C_2C_1C_0$ are appended at the end of the message by transmitter. The transmitted bit string is denoted by $m_4m_3m_2m_1m_0C_2C_1C_0$. The value of sequence $C_2C_1C_0$ is

Generator $= x^3+x+1$

$= 1011$

message = 11000

$$
\begin{array}{r}
1011 \,\big)\, 11000000 \\
\underline{1011} \\
1110000 \\
\underline{1011} \\
101000 \\
\underline{1011} \\
100
\end{array}
$$

100 — CRC

Ans = 100

classmate

Date
Page

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

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

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

Calculate the transmission function $T(x)$

$$
\begin{array}{r}
x^4+x+1 \;\big)\; x^{11}+x^{10}+x^8+x^6+x^5 \;\big(\; x^7+x^6+x \\
x^{11}+x^8+x^7 \\
\hline
x^{10}+x^7+x^6+x^5 \\
x^{10}+x^7+x^6 \\
\hline
x^5 \\
x^5+x^2+x \\
\hline
(x^2+x) \rightarrow \text{Remainder}
\end{array}
$$

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

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 with 8 bits as info bits and uses x^3+x+1 as generator. In this network the message 01011011 is transmitted as

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

$= 1011$

$$
\begin{array}{r}
1011 \;\big)\; 01011011000 \;\big(\\
1011 \\
\hline
011000 \\
1011 \\
\hline
1110 \\
1011 \\
\hline
0101
\end{array}
$$

Transmitted data = 01011011101

classmate

Date 8/4/23
Page

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 decoder fails to detect them.

Recieved code word = Sent codeword + error

Recieved codeword = $c(x) + e(x)$

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

   Recieved codeword = $c(x)$

$$\frac{c(x)}{g(x)} = 0$$

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

   recieved codeword = $c(x) + e(x)$

Recieved codeword = $c(x) + e(x)$

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

$\frac{c(x)}{g(x)} = 0$ According to the defination of CRC. 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] CRC 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

Recieved codeword = 1101000100

2 bit error.

```
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.

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

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 gives 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-efficient of x^0 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-efficient of x^0 is 1, all single bit error can be detected.

eg: Data: 1011

CRC generator = 1 (Generator is not valid) eg:: Data = 1011

CRC Generator = $x = 1.x^1 + 0.x^0 = 10$

```
10 | 10110
     10
     ---
      110
      10
     ---
       10
       10
      ---
       00 → CRC or Remainder.
```

Transmitted codew. 10110 — Recieved codeword 10010

```
10 | 10010
     10
     ---
      010
       10
      ---
       00 → Syndrom = 0
```

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

Note: Generator should not contain 'x'

eg:: data = 1011

CRC generator = $x + 1 = 1.x^1 + 1.x^0 = 11$

```
11 | 10110
     11
     ----
     1110
     11
     ----
     0010
       11
     ----
       01 → Remainder
```

Sent codeword 10111 — Recieved codeword 10101

```
11 | 10101
     11
     ----
     1101
     11
     ----
       01 → Syndrom = 1
```

One bit error detected

Sent codeword 10111 — Recieved codeword 10100

```
11 | 10100
     11
     ----
     1100
     11
     ----
     0000
```

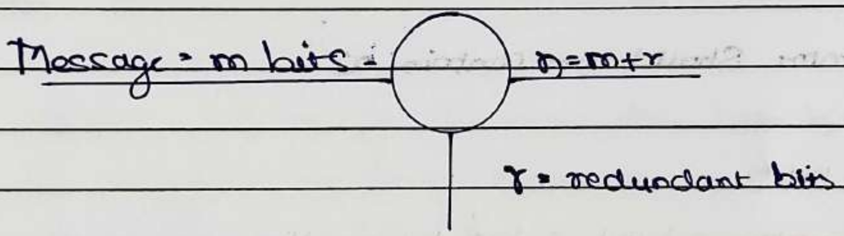
Syndrome = 0, two bit error not detected.

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~~ is used for error correction.



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

eg:: data = 1010111, m = 7

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

$r=1 \rightarrow 7+1+1 \le 2^1$ ×

$r=2 \rightarrow 7+2+1 \le 2^2$ ×

$r=3 \rightarrow 7+3+1 \le 2^3$ ×

$\cancel{r}=4 \rightarrow 7+4+1 \le 2^4 = 12 \le 16$ (yes)

$r=5 \rightarrow 7+5+1 \le 2^5 = 13 \le 32$ (yes)

Choose the minimum value of r that satisfies the condition.

$n = m+r$

$= 7+4$

$= 11$

Redundant bit or Parity bits or Check bits. position $= 2^i$ (where $i \geq 0$)

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

1 2 4 . . .

P_1	P_2	3	P_4	5	6	7	P_8	9	10	11
1	0	1	1	0	1	0	1	1	1	1

P_1

1	3	5	7	9	11
1	1	0	0	1	1

P_2

2	3	6	7	10	11
0	1	1	0	1	1

P_4

4	5	6	7
1	0	1	0

P_8

8	9	10	11
1	1	1	1

eg::

Transmitted data = 10110101111

If reciever recieved uncorrupted data

Recieved data = 10110101111.

P_1.

1	3	5	7	9	11	
1	1	0	0	1	1	— even $P_1=0$.

P_4

4	5	6	7	
1	0	1	0	→ even $P_4=0$

P_2

2	3	6	7	10	11	
0	1	1	0	1	1	— even $P_2=0$.

P_8

8	9	10	11	
1	1	1	1	→ even ($P_8=0$)

P_8	P_4	P_2	P_1
0	0	0	0

→ no error (if non zero then error)

★ If reciever recieved corrupted bit.

Recieved data = 1011010101 1 (9th 10th 11th)

P_1 1 3 5 7 9 11 1 1 0 0 0 1 → odd (P_1=1)	P_4 4 5 6 7 1 0 1 0 → even (P_4=0)
P_2 2 3 6 7 10 11 0 1 1 0 1 1 → even (P_2=0)	P_8 8 9 10 11 1 0 1 1 → odd (P_8=1)

$P_8 P_4 P_2 P_1$

1 0 0 1 → non zero means error

↳ decimal value = 9

so 9th bit got corrupted

★ If reciever recieved corrupted data: (2 bit error)

Recieved data = 10111101011

P_1 1 3 5 7 9 11 1 1 1 0 0 1 → even (P_1=0)	P_4 4 5 6 7 1 1 1 0 → odd (P_4=1)
P_2 2 3 6 7 10 11 0 1 1 0 1 1 → even (P_2=0)	P_8 8 9 10 11 1 0 1 1 → odd (P_8=1)

$P_8 P_4 P_2 P_1$

1 1 0 0 → decimal value = 12

(non zero means error

Two bit error detected.

classmate
Date
Page

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

Ans

P_1 P_2 3 P_4 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)	P_4 P_2 P_1 1 1 1 → non zero means error decimal value = 7, so 7^{th} bit got corrupted.

Q2 Assume that a 12-bit hamming codeword consisting of 8 bit data and 4 check bits is $d_8d_7d_6d_5C_8\ d_4d_3d_2C_4d_1C_2C_1$ where data bits and check bits are:

Data bits: 1 1 0 x 0 1 0 1 (d_8 d_7 d_6 d_5 d_4 d_3 d_2 d_1)

Check bits: y 0 1 0 (C_8 C_4 C_2 C_1)

Correct value of x and y are?

Ans:

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

C_1 1 3 5 7 9 11 0 1 0 0 x 1 (for even parity) → x=0.	C_4 4 5 6 7 12 0 0 1 0 1 → even	∴ The value of x and y are 0 and 0 respectively.
C_2. 2 3 6 7 10 11 1 1 1 0 0 1 — even.	C_8. 8 9 10 11 12 x y 0 1 1. 0. 0 (for even parity)	

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

Ans
$m = 60$

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

$r = 7, \quad 60 + 7 + 1 \le 2^7$ (yes)

Q4. For single bit error correcting hamming code, the code length for 12 data bit is ______

Ans
$m = 12$

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

$r = 4 \longrightarrow 12 + 4 + 1 \le 2^4$ ×

$r = 5 \longrightarrow 12 + 5 + 1 \le 2^5$ ✓

Code Length $= 12 + 5$
$= \underline{17}$

HW

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

Ans
$m = 7, \quad r = 4, \quad n = m + r$
$= 7 + 4 = 11$ bit

$r = 4 \longrightarrow 7 + 4 + 1 \le 2^4 \quad 12 \le 16$ (yes)

P_1	P_2	3	P_4	5	6	7	P_8	9	10	11
		1		0	1	0		1	1	1

P_1	P_4
1 3 5 7 9 11	4 5 6 7
P_2	P_8
2 3 6 7 10 11	8 9 10 11

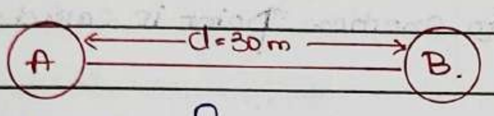
Note: Odd parity is preferable over even parity.

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, distance covered in one second.



100 bits transfer from A to B.

B = 1 bps = 1 bits/sec
v = 10 m/sec

Total time = 100 sec + 3 sec
= 103 sec

Delay:

1. Transmission delay (Td)
2. Propogogation delay (Pd)
3. Queuing delay (Qd)
4. Processing delay (Prd)

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

eg:: 1
Packet size = 1000 bits
Bandwidth = 2bps = 2 bits/sec

$$Td = \frac{1000 \text{ bits}}{2 \text{ bits/sec}}$$
= 500 sec

$$\boxed{Td = \frac{L}{B}}$$

eg:: 2
Packet Size = 100 bits
Bandwidth = 10 bps = 10 bits/sec

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

classmate
Date 10/4/23
Page

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, of distance covered in one second.

$A \xleftrightarrow{d = 30m} B.$

100 bit transfer from A to B.

$B = 1\ bps = 1\ bits/sec$

$v = 10m/sec$

Total time $= 100\ sec + 3\ sec$

$= \underline{103\ sec}$

Delay:

1. Transmission delay (Td)
2. Propogogation delay (Pd)
3. Queuing delay (Qd)
4. Processing delay (Prd)

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

eg:: 1.

Packet size = 1000 bits

Bandwidth = 2bps = 2 bits/sec

$Td = \frac{1000\ bits}{2\ bits/sec}$

$= \underline{500\ sec}$

$$\boxed{Td = \frac{L}{B}}$$

eg:: 2

Packet Size = 100 bits

Bandwidth = 10bps = 10 bits/sec

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

$= \underline{10\ sec}$

	Data	Bandwidth
K	1024 (2^{10})	10^3
M	1024x1024 (2^{20})	10^6
G	1024x1024x 1024 (2^{30})	10^9

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

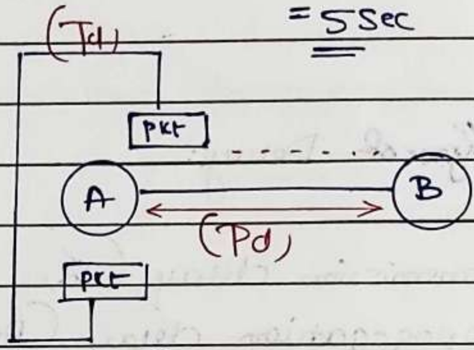
eg:- (A) $\xleftrightarrow{d = 50m}$ (B)

$v = 10m/sec.$

Propogation delay $= \frac{50m}{10m}$ ^5^

$= \underline{\underline{5 sec}}$

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



Total time taken to send a packet from A to B = $\underline{Td + Pd}$

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

* DLL → Node to Node or Hop to Hop

* NL → source host to destination host.

* TL → Process to Process or end to end

Date 17/4/23

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 recieve a packet from it's input port, remove the header, perform an error direction procedure. and deliver the pkt to the out 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 Packet Size = 1KB = 1024 Byte = 1024 * 8 bits
= 8192 bits

Bandwidth (B) = 10^9 bits/sec

$T_d = \frac{L}{B} = \frac{8192}{10^9 \text{ bits/sec}} = 8.192 \times 10^{-6}$ sec
$= 8\mu s$

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 propogation delay along the link is 2×10^8 m/sec. Host x send a file of 50,000 byte as one large message to host ~~x~~ y continously. Let the transmission and propogation delay be p milliseconds and q (ms), the value of p and q are:

Ans $B = 10^6$ bits/sec, $d = 10,000$ km

$v = 2\times10^8$ m/sec packet size (L) = 50,000 bytes ×8

= 4,00,000 bits

$Td = \frac{L}{B} = \frac{4,00,000}{10^6 \text{ bits/sec}} = 400\times10^{-3}$ sec

$= 400$ msec

$Pd = \frac{d}{v} = \frac{10,000}{2\times10^5 \text{ km/sec}}$ ∴ p = 400 msec and q = 50 msec.

$= 50\times10^{-3}$ sec

$q = 50$ msec

Q3. Consider two computers x and y connected via a single bandwidth 512 Gbps. Suppose that both hosts are seperated by distance m meters, and propogation delay along with the link is 2×10^9 meter/sec. Computer x has to send a packet of size 1 KByte to computer y. What will be the distance m such that the delay in propogation is equal to the delay in transmission?

Ans. $B = 512\times10^9$ bits/sec, distance = 'm' bits

$v = 2\times10^9$ m/sec, L = 1KB = 1024 Bytes = 8×1024 bits

$Pd = Td$

$\frac{d}{v} = \frac{L}{B}$ $\frac{m}{2\times10^9 \text{ m/sec}} = \frac{8\times1024 \text{ bits}}{512\times10^9 \text{ bits/sec}}$

$m = \frac{8\times1024\times2\times10^9}{512\times10^9}$ mtr

m = 32 mtr

Q4 Consider a 100 Mbps link between an earth station (sender) and a satellite (reciever) at an altitude of 2100 Km. The signal propogates at a speed of 3×10^8 m/s. The time taken (in ms) for the reciever to completely recieve a packet of 1000 byte transmitted by the sender is ________

Ans

$d = 2100$ km, $u = 10^8$ m/sec, $u = 10^5$ Km/sec.

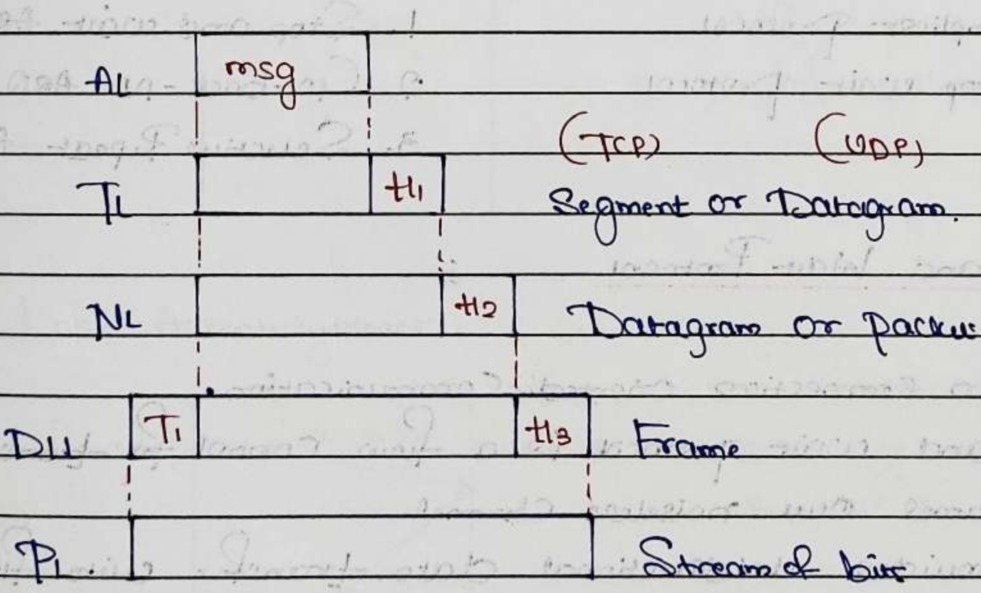
Pkt size = 1000 byte = 8000 bit

$B = 100$ Mbps $= 100\times10^6$ bits/sec
$= ~~100~~\ \underline{\underline{10^8 \text{ bit/sec}}}$

$Pd = \frac{d}{v} = \frac{\cancel{2100}\overset{7}{} \text{ Km}}{3\times10^5 \text{ Km/sec}}$
$= 7\times10^{-3}$ sec
$= 7$ m.Sec

$Td = \frac{L}{B} = \frac{8000 \text{ bit}}{10^8 \text{ bit/sec}} = 8\times10^{-5}$ sec
$= 0.8\times10^{-3}$
$= 0.8$ mSec

$\therefore Td + pd$
$= 7 + 0.8$
$= 7.08$ m.Sec



Flow Control

1. Flow control co-ordinate the amount of data can be sent before recieving 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 reciever.

3. Reciever has a limited speed at which it can process incoming data and limited amount of memory in which to store incoming data.
4. Reciever must inform the sender before limit are 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, reciever has a block of memory (buffer) storing incoming data until they are processed.

Flow Control Protocols

- Noiseless Channel
  1. Simpliest protocol
  2. Stop wait protocol.
- Noisy Channel
  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 acknoledgement before transmitting the next frame.

Sender Side.

Rule 1: Send one data packet at a time

Rule 2: Send the next packet only after recieving the Ack for the previous packet.

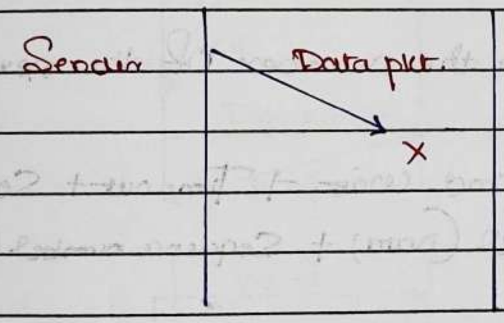
Reciever Side:

Rule 1: Recieve and consume the data packet.

Rule 2: After consuming packet, acknowledgement needs to be sent.

Problems of Stop and wait Protocol.

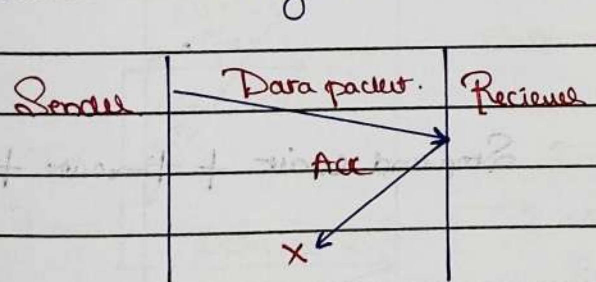
1. Lost data packet



Note: * Sender wait for ack for an infinite amount of time.

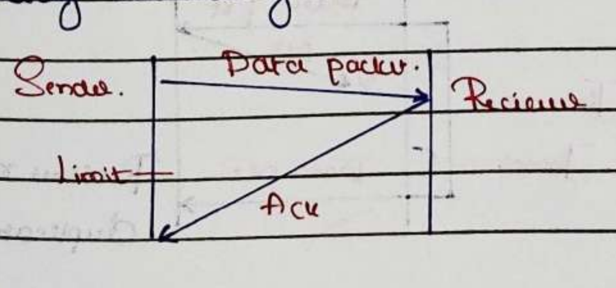
* Reciever wait for data an infinite amount of time.

2. Lost Acknowledgement.



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

3. Delay acknowledgment.



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

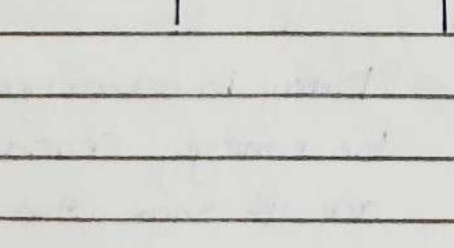
- The above 3 problems are resolved by using Stop and wait ARQ (Automatic Repeat Request)

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 the copy of sent frame until it recieves an acknowledgement.
3. Sender Start a timer when it Sends a frame. If ACK is not found / recieved within the allocated time period, the Sender assume that the frame was lost or damage and resends it.
4. Reciever send an acknoledgment to Sender if it recieves a frame Correctly.
5. ACK number always define the number of the next expected frame.
6. Stop and wait ARQ = Stop and wait + Time out + Sequence number (Data) + Sequence number (ACK).

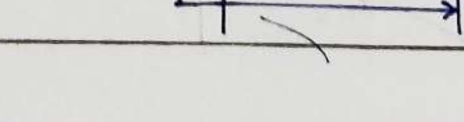
Solutions:

① Lost data packet.

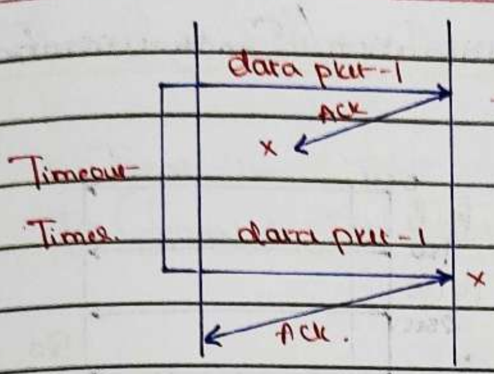


→ Stop and wait + timeout time.

② Lost acknoledgment.



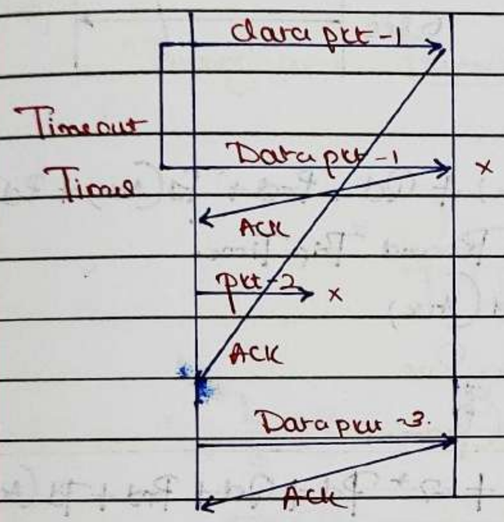
Reciever recieved duplicate data.



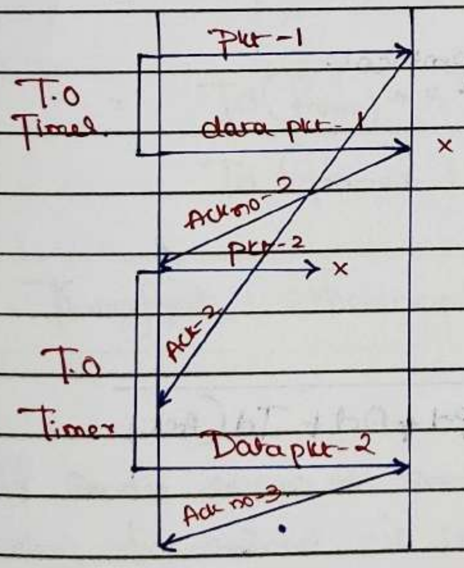
→ Stop and wait + Timeout timer + Sequence number (data pkt)

Duplicate packet discarded by the reciever.

③ Delay Acknowledgement.



Duplicate packet discarded by the reciever.



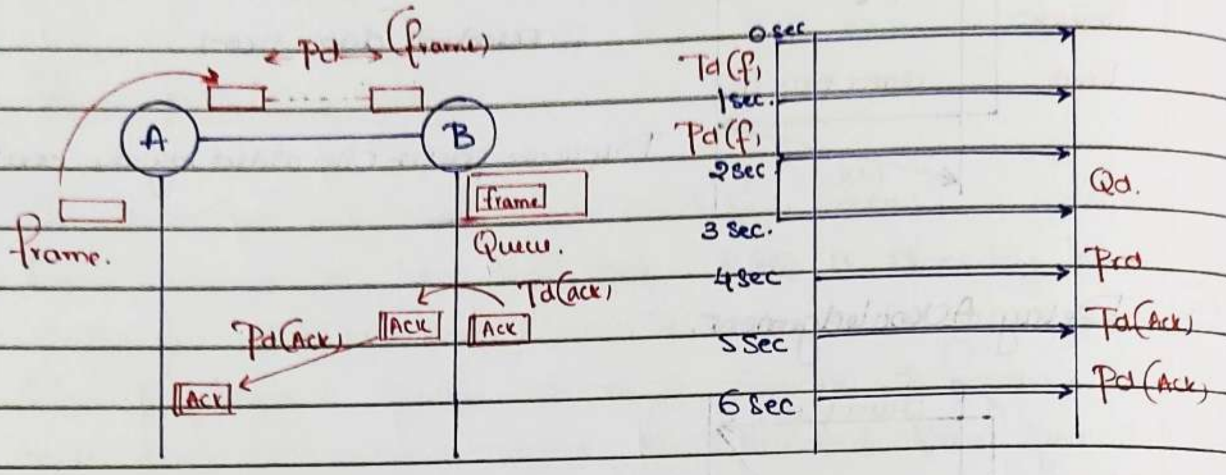
Duplicate packet discarded by the reciever.

→ Stop and wait + T.O timer + Seq no. (data pkt) + Seq no (ack)

↓

Stop and Wait ARQ.

Efficiency / Line utilization / Link utilization / Sender utilization:



$\underline{\text{Total time}} = Td(\text{frame}) + Pd(\text{frame}) + Qd + Prd + Td(Ack) + Pd(Ack)$

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

$RTT = Td(\text{frame}) + 2(Pd) + Td(Ack)$

Ack Size < Frame Size

$Td(Ack) < Td(\text{frame})$

$$\boxed{RTT/\text{Total Time} = Td(\text{Frame}) + 2 * Pd + Qd + Prd + Td(Ack)}$$

Efficiency of stop and wait protocol:

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

$$\text{efficiency} = \frac{Td(\text{frame})}{Td(\text{frame}) + 2 * Pd + Qd + Td(Ack)}$$

* If $Qd \cdot Prd = Td(Ack) = 0$

then $\text{Total time} = Td(\text{frame}) + 2 * Pd + Qd + Prd + Td(Ack)$

$\text{Total time} = Td(\text{frame}) + 2 * Pd$

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

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

Total time $\longrightarrow$ 1 Frame

$\underbrace{Td(frame) + 2^* Pd + Qd + Prd + Td(Ack)}_{10\ Sec} \longrightarrow \underbrace{1\ Frame}_{1000\ bits}$.

10 Sec $\longrightarrow$ 1000 bit

1 Sec $\longrightarrow \frac{1000}{10} = 100$ bit/sec

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

$$= \frac{L}{Td(frame) + 2^* pd + Qd + Prd + Td(Ack)}$$

$$= \frac{\frac{L}{B} \times B}{Td(frame) + 2^* Pd + Qd + Prd + Td(Ack)}$$

$$= \frac{Td(frame) * B}{Td(frame) + 2^* Pd + Qd + Prd + Td(Ack)}$$

$$\boxed{\text{Throughput} = \text{efficiency} * \text{bandwidth}} \qquad \boxed{\text{Efficiency} = \frac{\text{Throughput}}{\text{Bandwidth}}}$$

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

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

Total transmissions = 13

No. of retransmissions = 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. $n = 500$, $p = 0.2$

$$\underset{500}{n} + \underset{500(0.2)}{np} + \underset{100(0.2)}{np.p} + \underset{20(0.2)}{np.p^2}$$

$$500 + 100 + 20 + 4 \ldots$$

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

Total transmission required $= \dfrac{n}{1-p}$

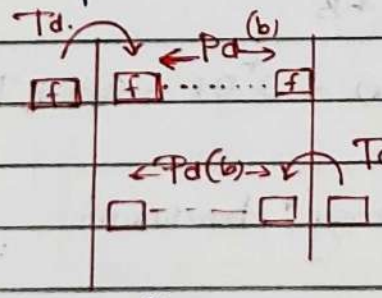
$$= \frac{500}{1-0.2} = \frac{500}{0.8} = 625$$

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

$a+b+a+b$

$= 2a+2b$



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

Ans. Frame size = 1000 bits $\qquad d = 100$ Km

Bandwidth = 20 mbps

$= 20 \times 10^6$ bits/sec.

$$Td(frame) = \frac{L}{B}$$

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

classmate
Date
Page

$v = 2\times10^5$ km/sec. $\quad Pd = \frac{d}{v} = \frac{100 km}{2\times10^5 km/sec} = 0.5$ m sec.

$$\text{efficiency} = \frac{Td(\text{frame})}{Td(\text{frame}) + 2^* pd + \cancel{Qd} + \cancel{Prd} + Td(\cancel{Ack})}$$

$$= \frac{0.05 \text{ m sec}}{0.05 \text{ m sec} + 2^* 0.5 \text{ m sec.}} = \frac{0.05}{1.05} = \frac{5}{105} = 0.04761$$

$$\eta = \underline{\underline{4.761\%}}$$

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

Ans $B = 1.5$ mbps $= 1.5\times10^6$ bits/sec $\quad$ RTT = 45 m sec

$$Td(\text{frame}) = \frac{8192 \text{ bits}}{1.5\times10^6 \text{ bits/sec}} = 5461.33\times10^{-6} \text{ sec} = \underline{\underline{5.461 \text{ m sec}}}$$

$$\eta = \frac{Td(\text{frame})}{RTT} = \frac{5.461 \text{ m sec}}{45 \text{ m sec}} = 0.1213$$

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

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 acknoledgement is 100 bytes and the transmission rate at the reciever is 8 kbps. The one way propogation delay is 100 miliseconds. Assuming no frame is lost, the senders throughput is 2500 bytes/sec.

Ans Frame size = 1000 bytes = 8000 bits. $\quad$ Ack size = 100 Byte = 800 bits. $\quad$ $B = 8$ kbps $= 8\times10^3$ bits/sec (Reciever)

$B = 80$ kbps $= 80\times10^3$ bits/sec

$Pd = 100$ m sec. $= 100\times10^{-3}$ sec $= \frac{1}{10}$ sec.

classmate

Date
Page

Td(frame)

$= \frac{8000 \text{ bits}}{80\times10^3 \text{ bits/sec}}$

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

Td(Ack) $= \frac{800 \text{ bits}}{8\times10^3 \text{ bits/sec}}$

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

$$\text{Throughput} = \frac{\text{Frame Size}}{Td(\text{frame}) + 2^* Pd + QD + Prd + Td(\text{Ack})}$$

$$= \frac{8000 \text{ bits}}{\frac{1}{10}\text{ sec} + 2^*\frac{1}{10}\text{ Sec} + \frac{1}{10}\text{ sec}} = \frac{8000}{0.4 \text{ sec}} = 20{,}000 \text{ bits/sec} = \frac{20000}{8}$$

$= \underline{2500 \text{ byte/sec}}$

Q7.. The value 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 errors. Then the transmission efficiency of Stop and wait ARQ for the above parameters is ____

Ans. B = 1 Mbps = 10^6 bits/sec

Pd = 0.75 msec

Prd = 0.25 msec

Frame Size = data + Header

$= 1980 + 20 = 2000$ Byte

$= 16{,}000$ bits.

Ack = 20 bytes = 160 bits

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

$= \frac{160}{10^6 \text{ bits/sec}} = 0.16\times10^{-3}$ Sec

$= \underline{0.16 \text{ m sec}}$

$Pd(\text{frame}) = \frac{\text{Frame Size}}{\text{Bandwidth}} =$

$= \frac{16{,}000}{10^6} = 16\times10^{-3} = \underline{16 \text{ msec}}$

$$\eta = \frac{Td(\text{frame})}{Td(\text{frame}) + 2^* Pd + Qd + Prd + Td(Ack)}$$

$$= \frac{16}{16 + 2^* 0.75 + 0.25 + 0.16} = \frac{16}{17.91} = 0.8933$$

$\eta = 89.33\%$

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 as 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 P. delay in m. sec is?

Ans $B = 10^6$ bit/sec $\qquad \eta = 25\% = \frac{1}{4}$

data pkt size = 1000 Byte
= 8000 bits

$$Td(\text{frame}) = \frac{8000 \text{ bits}}{10^6 \text{ bits/sec}}$$

$= 8 \times 10^{-3}$ sec = 8 m sec

$$\text{efficiency} = \frac{1}{4} = \frac{Td(\text{frame})}{Td(\text{frame}) + 2^* Pd + \cancel{Qd} + \cancel{Prd} + \cancel{Td(Ack)}}$$

$$\Rightarrow \frac{1}{4} = \frac{8}{8 + 2^* Pd} = 8 + 2^* Pd = 32$$

$2^* Pd = 32 - 8$

$2^* Pd = 24$ m sec.

$Pd = \frac{24}{2}$ m sec. $\qquad$ $Pd = 12$ m. sec

Q9. Suppose that the stop and wait ARQ is used on a link with a bit rate of 64 kb/sec and 20 ms prop. delay. Assume that the transmission time for the acknowledgement and the processing time at nodes are negligible. Then the min frame size in bytes to achieve a link utilization of atleast 50% is ____

Ans $B = 64 \times 10^3$ bits/sec, $\quad Pd = 20$ m sec, $\quad$ Frame Size $(L) = ?$

classmate
Date
Page

efficiency $\geq 50\% \left(\frac{1}{2}\right)$ efficiency $= \frac{\text{usefultime}}{\text{total time}} = \frac{1}{2}$

$$\frac{Td(\text{frame})}{Td(\text{frame}) + Pd*2 + Qd + Prd + Td(\text{Ack})} \geq \frac{1}{2}$$

$$\frac{Td}{Td + 2*pd} \geq \frac{1}{2} \Rightarrow 2*Td \geq Td + 2*pd$$

$$Td \geq 2*pd$$

$$\frac{L}{B} \geq 2*pd$$

$L \geq 2*pd*B$

$L \geq 2*20 \times 10^{-3}\,\text{sec} * 64\times10^{3}$ bits/sec

$L \geq 40 \times 64$ bits

$L \geq \frac{40\times 64}{8}$ byte $\boxed{L \geq 320 \text{ Byte}}$

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 transmiss-ion time of the acknowledgement frame is negligible. To get a channel efficiency of atleast 50% the min frame size should be?

Ans $B = 4\times10^{3}$ bits/sec $L \geq 2*pd*B$

$Pd = 20$ m.sec $L \geq 2*20*10^{-3}\,\text{sec} \times 4*10^{3}$ bits/sec.

$\underline{L \geq 160 \text{ bits}}$

Q11. On a wireless link, the probability of packet is 0.2. A stop and wait ~~ARQ~~ 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 $P = 0.2$ Total transmission $= \frac{?}{1-P} = \frac{100}{1-0.2} = \frac{1000}{8} = \underline{\underline{125}}$

classmate

Date ______
Page ______

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 ~~80%~~ 75%, the min frame size?

Ans $B = 4\times10^{3}$ bits/sec. $Pd = 10$ m.sec $= 10\times10^{-3}$ m.sec.

efficiency $\geq 75\%$ $\left(\frac{3}{4}\right)$

efficiency $\geq \frac{3}{4}$

$$\frac{Td(\text{frame})}{Td(\text{frame}) + 2^{*}pd + \cancel{Qd} + \cancel{Prd} + \cancel{Td(Ack)}} \geq \frac{3}{4}$$

$$\frac{Td(\text{frame})}{Td(\text{frame}) + 2^{*}pd} \geq \frac{3}{4}$$

$4 \times Td(\text{frame}) \geq 3\ Td(\text{frame})$

$Td(\text{frame}) \geq 6\ pd$

$$\frac{L}{B} \geq 6^{*}pd$$

$L \geq 6^{*}pd \times \text{Bandwidth}$

$L \geq 6^{*}10\times10^{-3}\text{sec} \times 4\times10^{+3}$ bits/sec

$\underline{L \geq 240 \text{ bits (frame size)}}$

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 x packet is 500. The value x is ___

Ans Avg no. of transmission for 'n' pkt $= \frac{n}{1-p}$

Avg no. of transmission for 'x' pkts $= \frac{x}{1-p}$

$$500 = \frac{x}{1-0.6}$$

$$\frac{500}{1} = \frac{x}{0.4}$$

$x = 500^{*}0.4$

$\underline{\underline{x = 200}}$

Q14. Consider stop and wait ARQ for flow control, data transfer rate of channel is 32 kbps, one way end to end propagation

classmate

Date ______
Page ______

delay is 16 ms and frame size is 32 byte then efficiency in percentage is ____

Ans $B = 32$ Kbps $\qquad$ $P_d = 16$ m sec

$= 32 \times 10^3$ bit/sec $\qquad$ Frame size $= 32$ byte

$= 32 * 8$ bit

$= 256$ bit

T_d (frame) $= \dfrac{\text{frame size}}{\text{bandwidth}}$

$= \dfrac{\cancel{32} * 8 \text{ bit}}{\cancel{32} \times 10^3 \text{ bit/sec}} = 8 \times 10^{-3}$ sec $= 8$ msec

efficiency $= \dfrac{T_d(\text{frame})}{T_d(\text{frame}) + 2 * pd + \underbrace{\cancel{Qd}}_{0} + \underbrace{\cancel{Prd}}_{0} + \underbrace{\cancel{T_d(\text{ACK})}}_{0}}$ $= \dfrac{8}{8 + 2 * 16}$

$= \dfrac{8}{40} = \dfrac{1}{5}$

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. Packet size $= 1000$ Bytes, $\quad d = 2000$ km

$= 8000$ bit $\qquad v = 2 \times 10^8$ m/sec

$v = 2 \times 10^5$ km/sec

$B = 1$ mbps $= 10^6$ bit/sec

~~efficiency~~ T_d (frame) $= \dfrac{\text{Frame size}}{\text{Bandwidth}} = \dfrac{8000}{10^6 \text{ bit/sec}} = 8 \times 10^{-3}$ sec $= 8$ m sec

$P_d = \dfrac{d}{v} = \dfrac{2000 \text{ km}}{2 * 10^5 \text{ km/sec}} = 10 \times 10^{-3}$ sec $= 10$ m sec

efficiency $= \dfrac{T_d(\text{frame})}{T_d(\text{frame}) + 2 * pd}$

$= \dfrac{8}{8 + 2 * 10} = \dfrac{8}{28}$

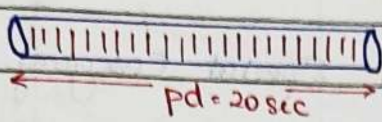
Throughput $=$ efficiency $\times B$

$= \dfrac{8}{28} \times 1$ mbps

$= 0.285$ mbps

Date 18/4/23

Capacity of Link/wire/Channel.



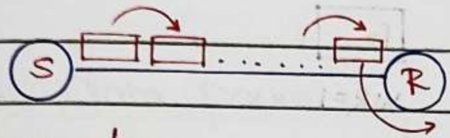
B = 1 bps = 1 bit/sec

Capacity of Link = 1 bit/~~sec~~ * 20 ~~sec~~

Capacity of Link = 20 sec bits

Capacity of the Link = $\underline{B^* pd}$

eg::



B = 1 bit/sec

Pd = 10 sec   Capacity of the Link = 1 bit/sec * 10 sec
= 10 bits.

Capacity of Link = $\underline{B^* pd}$

Q1. Bandwidth = 1Mbps and pd = 1 sec and packet size = 1000 bits, then how many packets can be transit at a time?

Ans Capacity of Link = $B^* pd$

$= 10^6$ bits/sec * 1 sec

$= 10^6$.

no. of packets $= \frac{10^6}{10^3} = \underline{10^3}$ packets can be in transit

Q2. If bandwidth = 1Mbps and Propagation delay is 1 msec and packet size is 100 bits/sec. Find the no. of packets needed to maximally pack the link.?

Ans (Capacity of the link)

Capacity of link $= B^* pd$

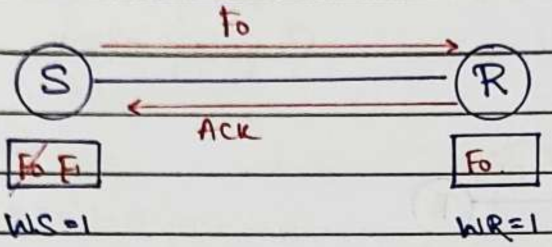
$= 10^6$ bits/sec * 10^{-3} sec

$= 10^3$ bits = 1000 bits.

No of packets
$= \frac{1000}{100}$
$= \underline{10 \text{ packets}}$

Important points about Stop and wait Protocol

1. Stop and wait protocol is a special category of protocols where window size = 1 Always.



2. Stop and wait protocol uses two sequence number i.e 0 and 1 irrespective of number of packet sender is having

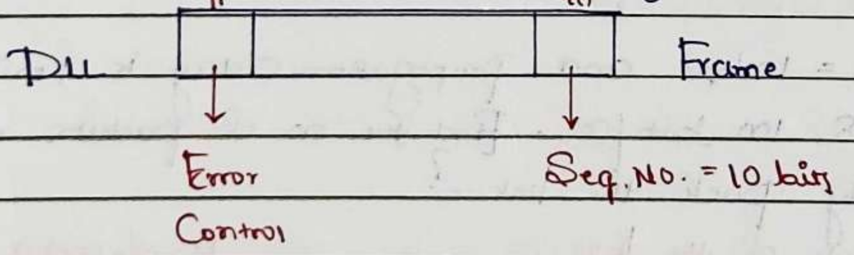
Sender wants to send 1000 frames to reciever

F_0 F_1 F_2 F_3 . . . . . . F999

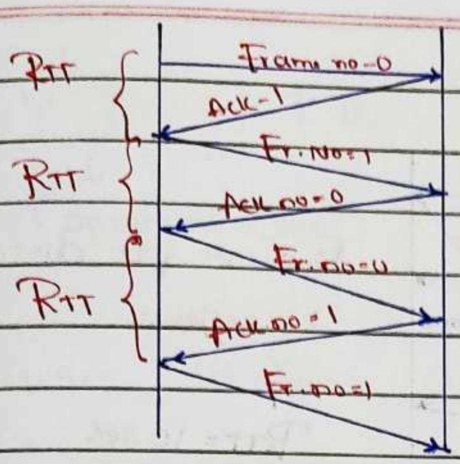
0 1 2 3 999

Total Sequence number required = 1000

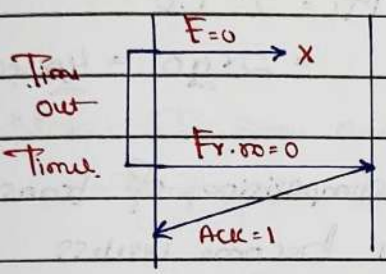
No. of bits required = $\lceil \log_2 1000 \rceil$ = 10 bits.



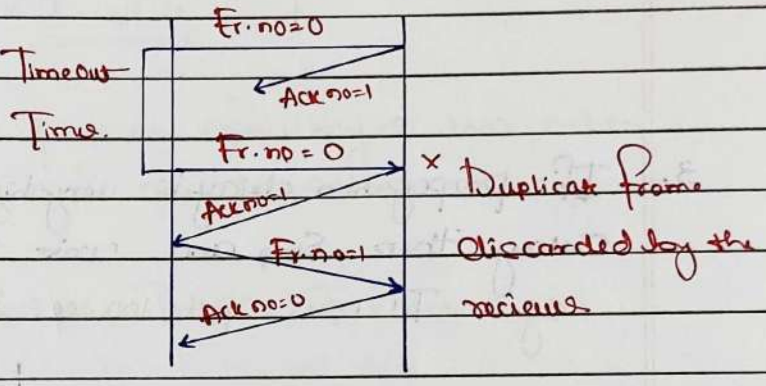
10 bits overhead for one byte. To send 1000 frames total overhead = 10*1000 = 10,000 bits.



Lost data packet.

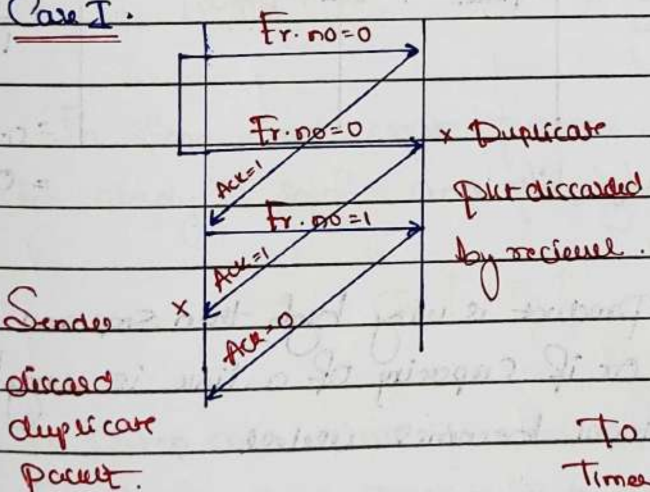


Lost Acknowledgement.

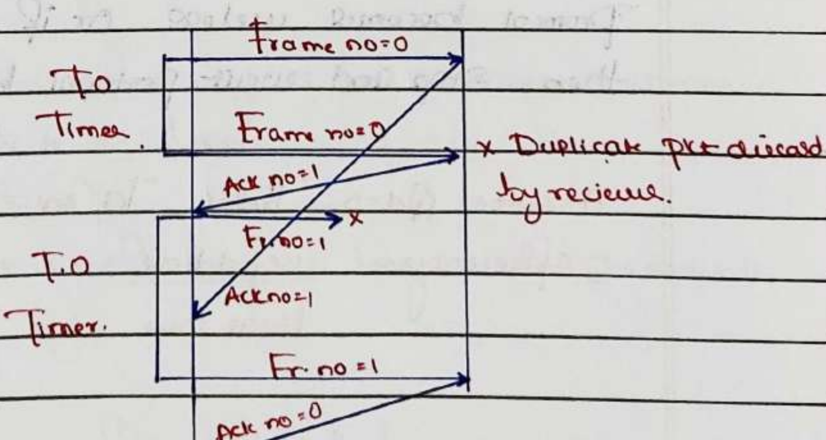


Delay in Acknowledgement.

Case I.



Case II

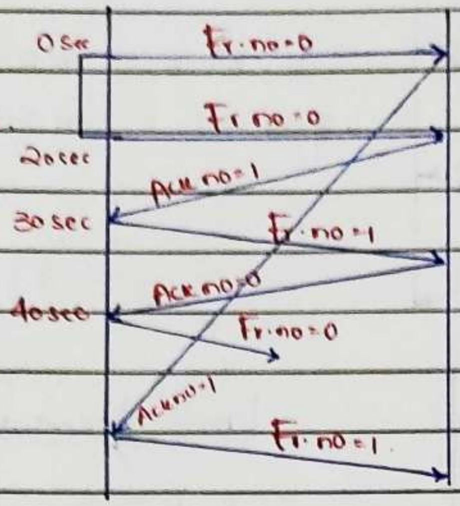


Case III

T.O Timer

$T.O = 2^* RTT$

$TTL = 2^* T.O$



× Duplicate pkt discarded by reciever

$RTT = 10\ sec$

$T.O = 2^* RTT$

$= 2^* 10 sec = \underline{20\ sec}$

$TTL = 2^* T.O$

$= 2^* 20 = \underline{40\ sec}$

3. If propogation delay is very high in comparision of transmission delay then Stop and wait protocol become useless.

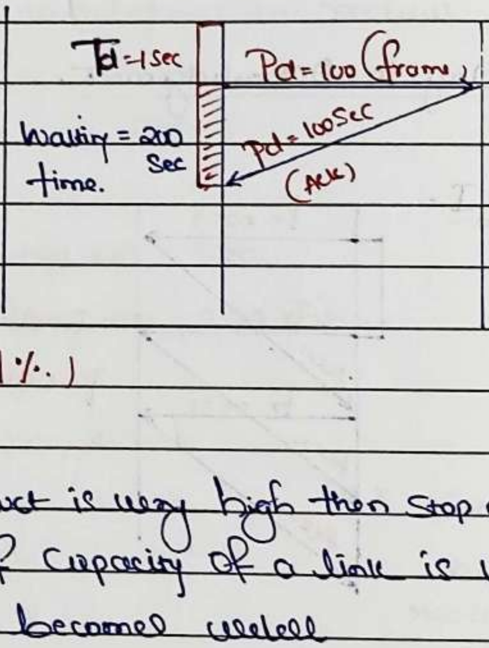
eg: Td = 1 sec, pd = 100 sec, Qd = 0, Prd = 0, Td (Ack)

$$\text{efficiency} = \frac{Td\ (\text{frame})}{Td\ (\text{frame}) + 2^* pd}$$

$$= \frac{1}{1 + 2^* 100}$$

$$= \frac{1}{201} = 0.0049$$

$$= \underline{0.49\% \ (< 1\%)}$$



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

$$= \frac{1}{1+200} = \frac{1}{201}$$

$$= 0.0049$$

$$= \underline{0.49\%}$$

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 Qd = 0, Prd = 0, Td (Ack) = 0

$$\text{efficiency} = \frac{\text{useful time}}{\text{total time}} = \frac{Td}{Td + 2^* pd} = \frac{Td}{Td\left[1 + 2^* \frac{Pd}{Td}\right]}$$

classmate

Date
Page

$\eta = \frac{1}{1+2*\left[Pd * \frac{B}{L}\right]}$ — ↑ then $\eta \downarrow$.

Capacity of a link

4. Td = 1 sec, Pd = 100 sec, Qd = 0, Prd = 0, Td (Ack) = 0

$$\eta = \frac{Td}{Td + 2*Pd + Qd + Prd + Td(Ack)} \qquad \eta = \frac{Td}{Td + 2*pd}$$

$$\eta = \frac{1}{1+2*100} = \frac{1}{201} = 0.0049$$

$$= \underline{\underline{0.49\%}}$$

Note: In Stop and wait protocol efficiency is low when propogation delay is high and transmission delay is low.

5. Td = 100 sec, Pd = 1 sec, Qd = 0, Prd = 0, Td (Ack) = 0

$$\eta = \frac{Td}{Td + 2*pd}$$

$$= \frac{100}{100+2*1} = \frac{100}{102} = 0.9830$$

$$= \underline{\underline{98.30\%}}$$

In Stop and wait protocol efficiency is high when transmission delay is high and propogation delay is low.

Pd ↓ Td ↑ η ↑

6. In stop and wait protocol efficiency is low when distance is high and packet size is less.

7. In stop and wait protocol efficiency is low when distance is high and bandwidth is high.

8. In stop and wait protocol efficiency is high when packet size

is high and distance is low.

a. $\eta = \frac{Td}{Td + 2 * pd} = \frac{Td}{Td\left[1 + 2 * \frac{pd}{Td}\right]}$

$\eta = \frac{1}{1 + 2 * \frac{d}{v} * \frac{B}{L}}$ $v \longrightarrow$ fixed, B — fixed

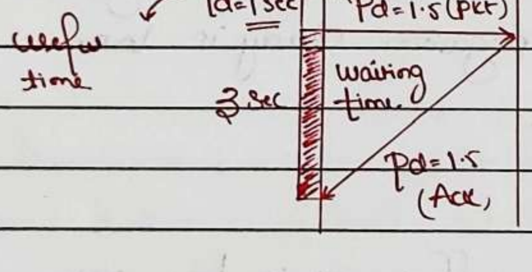
$d \uparrow$ $\eta \downarrow$: It is good for LAN
$L \uparrow$ $\eta \uparrow$: It is good for Large packet.

Q1. 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.

eg:: $Td = 1\,sec$, $Pd = 1.5\,sec$; $\eta = ?$

$\eta = \frac{Td}{Td + 2 * pd} = \frac{1}{1 + 2 * 1.5} = \frac{1}{4} = 25\%$

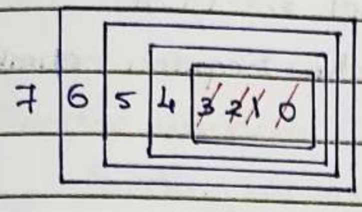


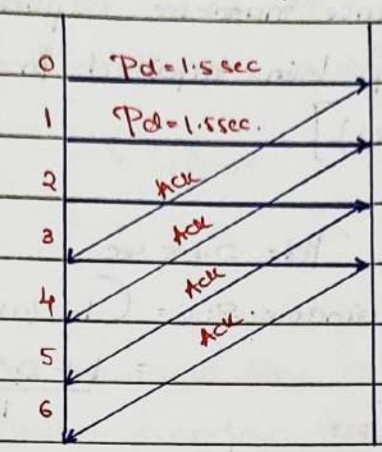
$\eta = \frac{\text{useful time}}{\text{Total time}} = \frac{1}{4} = 25\%$

eg:: $Td = 1\,sec$, $Pd = 1.5\,sec$

Maximum window size $= (1 + 2a)$ pkt
$= 1 + 2 * \frac{1.5}{1}$
$= 4$ pkt

Sliding Window





11 10 9 8 — Next to be transmitted

[7 6 5 4] — Transmitted & not acknoledged

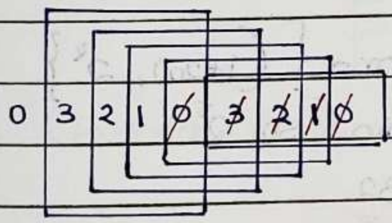
3 2 1 0 — Transmitted & Acknoledged

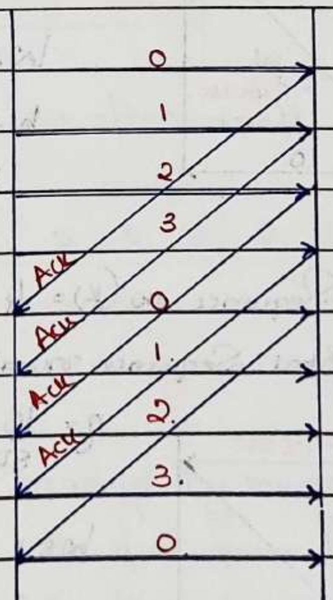
eg::

$Td = 1\ sec,\ Pd = 1.5\ sec$

max window size $= (1+2a)$ pkt

$= 1+2 * \frac{1.5}{1} = \underline{4}$ pkt





Minimum Sequence number required = 4

Min no. of bit required in the sequence no. field = 2 bit

$\{00, 01, 10, 11\}$

$= \lceil \log_2 (1+2a) \rceil$

$= \lceil \log_2 [4] \rceil$

$= \lceil \log_2 2^2 \rceil = 2 \lceil \log_2 \rceil = \underline{2 \text{ bit}}$

Maximum window size = $(1+2a)$ pkt.

Minimum Sequence number required = $(1+2a)$

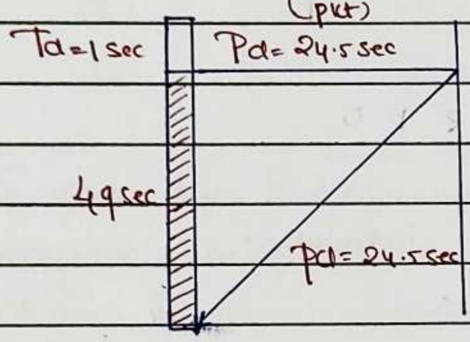
Minimum no. of bits required in the Sequence number field

$= \lceil \log_2(1+2a) \rceil$

eg:: $T_d = 1$ Sec, $P_d = 24.5$ sec

Max. window Size = $(1+2a)$ pkt

$= \frac{1 + 2 * 24.5}{1} = 50$ pkt.



Min Sequence no. required = $(1+2a) = 50$

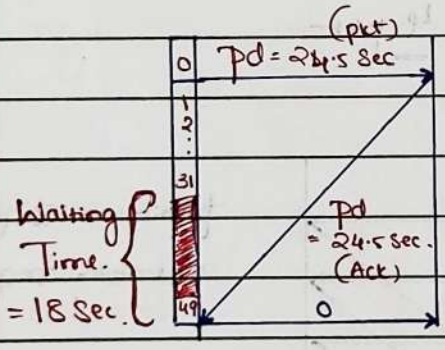
Min. no. of bits required in the Sequence number of field = $\lceil \log_2(1+2a) \rceil$

$= \lceil \log_2 50 \rceil$

$= \lceil 5.8 \rceil = 6$ bits.

Case I : Sequence no. (k) = 5 bit

Total Sequence No. $= 2^5 = 32$ (0 – 31)



efficiency $= \frac{32}{50} = 0.64 = 64\%$

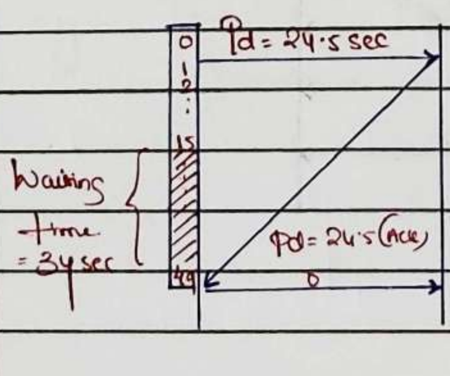
$W_S = \min\{(1+2a), 2^k\}$

$W_S = \min(50, 2^5)$

$W = 32$

Case II : Sequence no (k) = 4 bit

Total Sequence number $= 2^4 = 16$ (0 – 15)



$\eta = \frac{16}{50} = 0.32 = 32\%$

$W_S = \min((1+2a), 2^k)$

$= \min(50, 2^4)$

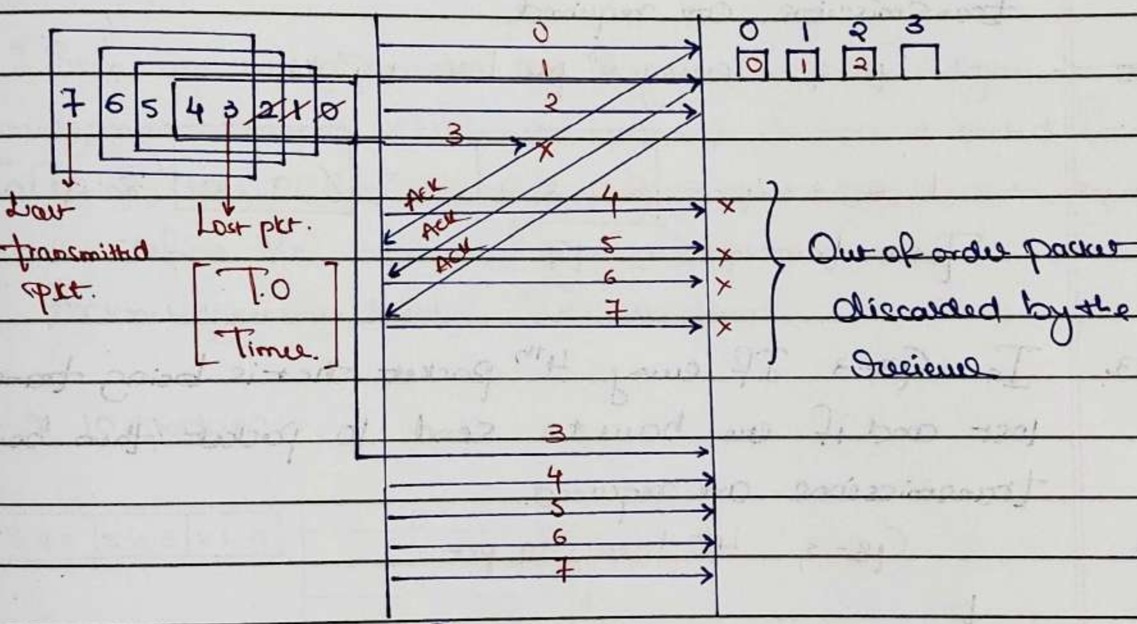
$= 16$

Sliding Window: In the Sliding window concept instead of sending one packet and wait for the acknowledgement, we send 'w' packet and wait for the acknowledgement, where 'w' is the Sender window Size.

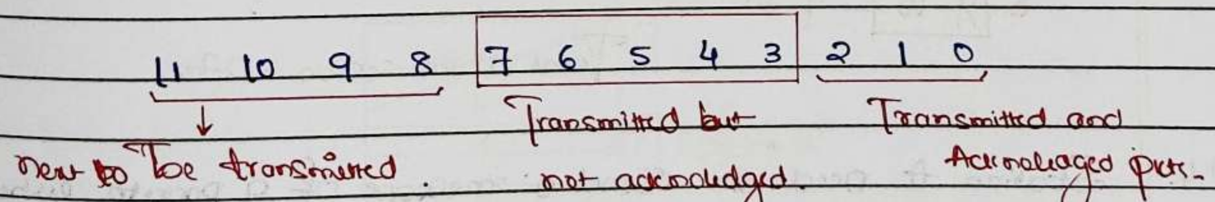
Sliding Window → GB-N
Sliding Window → S-R

GB-N (N>1)

1. In the GB-N the Sender window Size is N itself.
2. In the GB-N the reciever 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 recieved by the reciever.
* Timer is maintained only for the first frame (right most) in the window because if timer expires then sender assume that rest of the frames are not recieved by the reciever (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 packet, then how many transmission are required.

Ans. GB-3, 5th lost. 10 pkt.

1 2 3 4 | ~~5~~ 6 7 | 5 6 | ~~7~~ 8 9 | 7 8 | ~~9~~ 10 | 9 10

Total transmissions = 18.

Q2. In GB-4, if every 6th packet that is being transmitted is lost and if we have to send 10 packet then how many total transmissions are required

Ans GB-4, every 6th pkt lost, 10 pkt

1 2 3 4 5 | ~~6~~ 7 8 9 | 6 7 | ~~8~~ 9 10 | 8 9 10

Total transmissions = 17

Q3. In GB-3 If every 4th packet that is being transmitted is lost and if we have to send 10 packet then how many transmissions are required.

Ans. GB-3, 4th lost, 10 pkt.

1 2 3 | ~~4~~ 5 6 | 4 | ~~5~~ 6 7 | 5 | ~~6~~ 7 8 | 6 | ~~7~~ 8 9 | 7 | ~~8~~ 9 10 |
8 | ~~9~~ 10 | 9 10

Total transmission = 27.

Q4. Station A needs to send a message of 9 packets where Sender window = 3. All packets are ready and immediately available for transmission. By using GBN strategy, if 5th packet gets lost, what will be the total transmission?

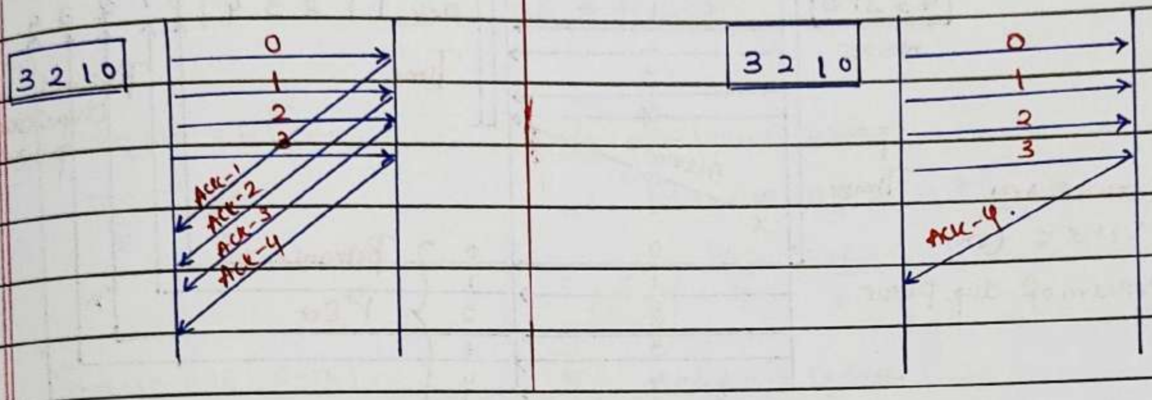
Ans Ws = 3, 5th lost, 9 packet

1 2 3 4 | 5 6 7 | 5 6 | 7 8 9 | 7 8 | 9 | 9.

Total transmission = 16

ACK

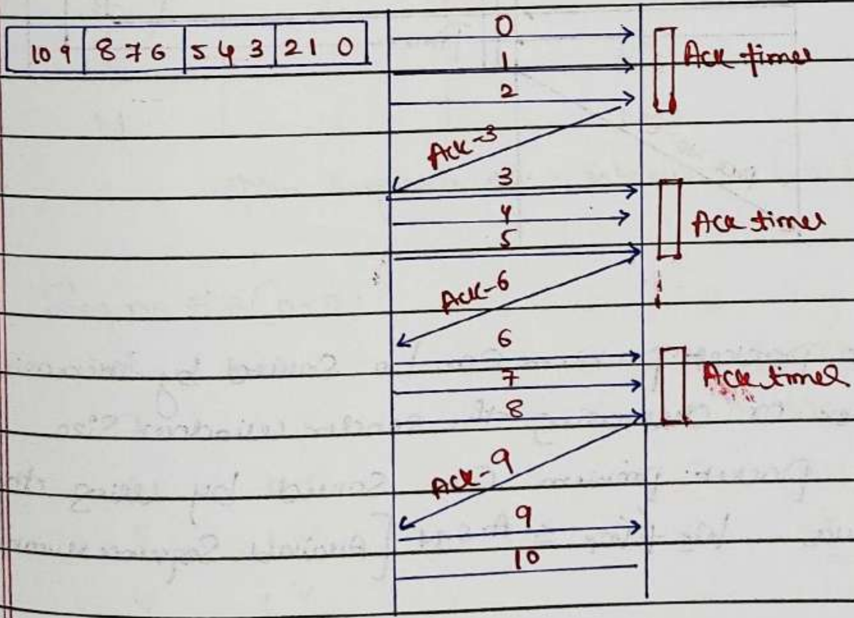
Independent | Cumulative



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 define the number of next expected frame.
* Acknowledgement time < Time out time.

→ GB-3, 10 packets.



classmate
Date 29/4/23
Page

$$\text{efficiency} = \frac{10 \times 5}{5 + 2 * 25 + 2 + 0.5}$$

$$= \frac{50}{57.5} = 0.8695$$

$$\therefore \eta = 86.95\%$$
$$\cong \underline{87\%}$$

Q4 Assume a sender send 6 packet (0-5). The sender recieves an acknoledgement with Ack no = 3. What is the interpretation if the system is using GB-N

Ans It means packet 0, 1, 2 have recieved uncorrupted and reciever expected packet 3.

Q5. In a sliding window ARQ scheme, the transmitter's window size is N and the reciever's window size is M. The min no of distinct sequence numbers required to ensure correct operation of the ARQ scheme is.

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 2 ms/km is used, the efficiency in % if N is set to 7 in GB-N

Ans pkt size = 1000 bits $\qquad B = 1\text{ Mbps} = 10^6$ bit/sec.

d = 5 km. $\qquad$ Propogation time = 5 × 2 ms.
= 10 ms

Speed ~~V~~ = 2 ms/km.

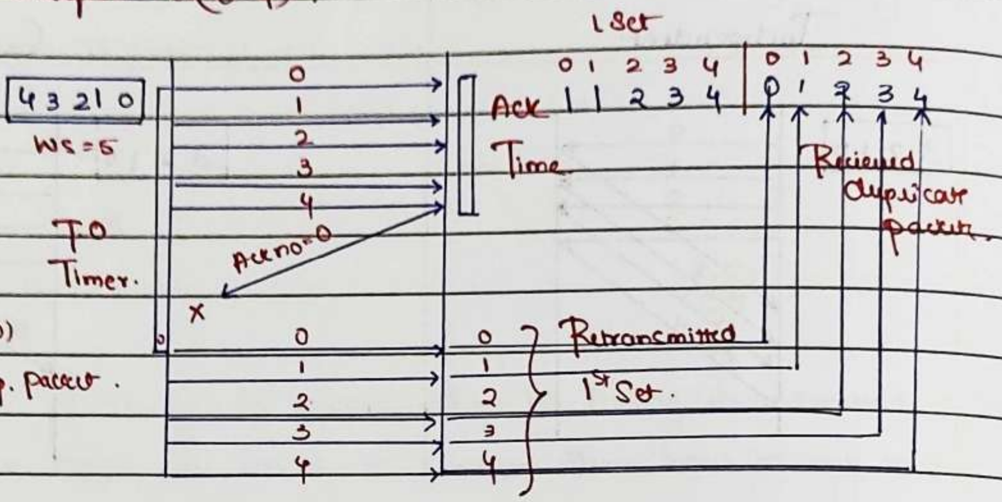
$$\eta = \frac{N \times Td(\text{frame})}{Td(\text{frame}) + 2^* pd + Qd + Td(\text{Ack})} \qquad Td(\text{frame}) = \frac{1000\text{ bits}}{10^6} = 10^{-3} = \underline{\underline{1 ms}}$$

$$= \frac{7 \times 1}{1 + 2 \times 10} = \frac{\cancel{7}}{\cancel{21}_{3}} = \frac{1}{3} = \underline{\underline{33.33\%}}$$

Q7 In GB-N protocol the packet size is 1000 bytes transmission time for one packet is 1 ms, If distance between hosts is 10 km

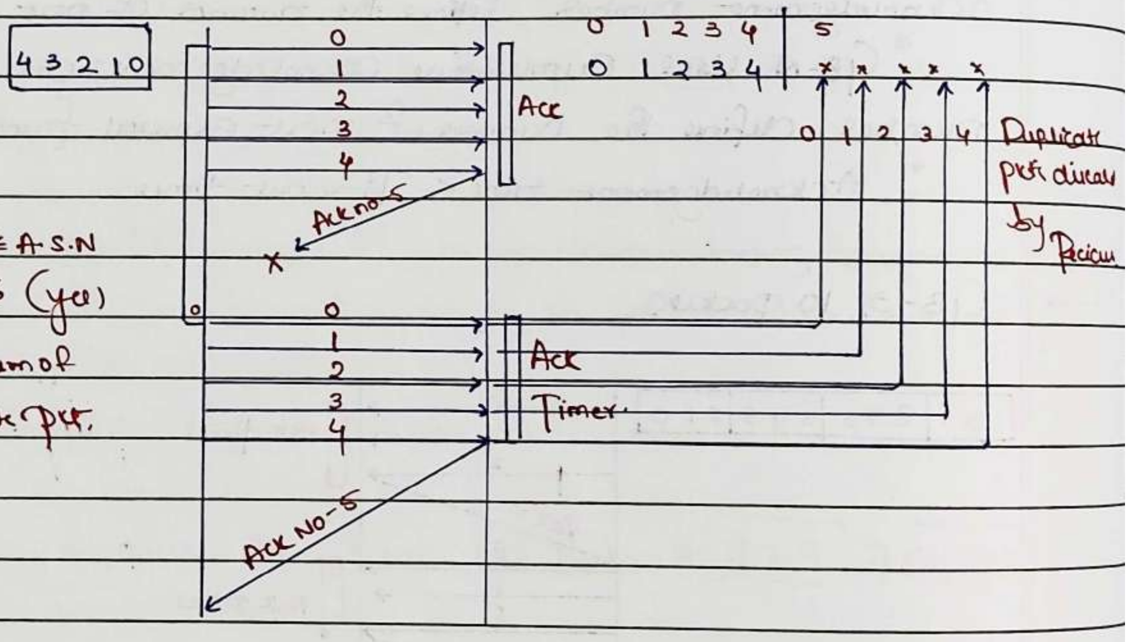
Relationship between window size and sequence number

GB-5, Seq no = 5 (0-4).



WS+WR ≤ ASN
5+1 ≤ 5 (no)
Problem of dup. packet.

GB-5, Sequence No = 6 (0-5)



WS+WR ≤ A.S.N
5+1 ≤ 6 (yes)
no. problem of duplicate pkt.

Note:

* Duplicate packet problem can be solved by increasing the sequence Number or decreasing the sender window size.
* Duplicate packet problem can solved by using the following formula $W_S + W_R \leq$ A.S.N [Available Sequence Number]

WR size = In GB-N the window reciever size is equal to one always irrespective of window sender size ($W_r = 1$)

and Signal speed is 5ms per km (5ms/km) and frame sequence number are 6 bit long in frame format then throughput in Mbps is ______.

Ans pkt size = 1000 Byte = 8000 bits   Prop. time for 1 km = 5ms

T_d = 1msec = 10^{-3} sec   " " 10 km = 50 ms

d = 10 km   Seq no = 6 bit.

GB-N

Seq no = k bit   B = ?   efficiency = $\frac{63 \times 1}{1+2^{*}50}$

Ws Wr $T_d = \frac{L}{B}$ $= \frac{63}{101}$

$2^k - 1$ 1.

$\therefore 2^6 - 1$ 1 $\frac{10^{-3}\text{sec}}{1} = \frac{8000 \text{ bits}}{B}$

$= 63$.   1.   Throughput = $\eta \times B$

$B = \frac{8000}{10^{-3}} = 8 \times 10^6$ $= \frac{63}{101} \times 8$ mbps

$= \underline{8 \text{ Mbps}}$

$= 4.99$ mbps

$\simeq \underline{5 \text{ Mbps}}$

Q8 Host A is sending data to host B over a full duplex link. A and B are using S.W protocol. The Ws = Wr = 5 packets each. Data packets (sent only from A to B) are all 1000 byte long and transmission time for such a packet is 50 μ sec. Acknowledgement packets (sent from B to A) are very small and negligible. The propogation delay over the link is 200 μ sec. What is max achievable throughput?

Ans. Ws = 5, Wr = 5   Throughput = $\frac{5 \times 1000 \text{ Byte}}{T_d(\text{frame}) + 2^{*}pd + Qd + Pcd + T_d(\text{ack})}$

Packet size = 1000 byte $= \frac{5000 \text{ byte}}{50 \mu\text{sec} + 2^{*} 200 \mu\text{sec}}$

T_d (frame) = 50 μsec

Pd = 200 μsec. $= \frac{5000 \text{ byte}}{450 \mu s \times 10^{-6} \text{sec}}$

$= \underline{11.11 \times 10^{+6} \text{ byte/sec}}$

Q9. Consider GB-N ARQ is used for flow control, frame size is 4000 bits, data transfer rate of channel is 1mbps and one way propogation delay is 18ms, then what should be the min value 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 = 1Mbps = 10^6 bits/sec

$Pd = 18$ msec.

$$Td(frame) = \frac{L}{B} = \frac{4000}{10^6} = 4\,msec$$

$$\eta = \frac{N * Td(frame)}{Td(frame) + 2*Pd + Qd + Prd + Td(Ack)} \qquad = \frac{1}{1} = \frac{N*4}{4+2*18}$$

$$N = \frac{40}{4} = 10.$$

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 x 10 bits/sec. The propogation speed of the media is 4×10^6 meter/sec. It is needed to design a GB-N 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 km. B = 500×10^6 bits/sec

v = 4×10^6 m/sec pkt size = 10^7 bits.

$$Td(frame) = \frac{L}{B} = \frac{10^7}{500 \times 10^6} = 0.02\,sec$$

$$Pd = \frac{d}{v} = \frac{8000}{4 \times 10^3\ km/sec} = 2\,sec$$

$$\eta = \frac{N * Td(frame)}{Td(frame) + 2*pd + Qd + Prd + Td(Ack)} \qquad \frac{1}{1} = \frac{N*0.02}{0.02 + 2*2}$$

$$N = \frac{4.02}{0.02} \quad N = \frac{402}{2} = 201$$

Minimum Sequence no. required = 201+1
= 202

$2^k = 202$ ∴ K = 8 bit

Q11. Consider a 512×10^3 bits/second Satellite Communication link with one way Propagation delay of 150 m.sec GB-N 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 5ms. Then what should be min window size —

Ans $B = 512 \times 10^3$ bits/sec   Ack size = 64 byte   Pcd = 5 msec
P_d = 150 msec.   = 8×64 bit
Frame size = 1 kbyte   = 512 bit.
= 1024 × 8
= 8192 bit

$T_d(\text{frame}) = \frac{L}{B} = \frac{8 \times 1024}{512 \times 10^3} = 16 \times 10^{-3} = 16$ msec

$P_d = \frac{d}{v} = 150$ msec $T_d(\text{Ack}) = \frac{\text{Ack size}}{B} = \frac{512}{512 \times 10^3} = 1$ msec

$$\text{efficiency} = \frac{N * T_d \text{frame}}{T_d(\text{frame}) + 2^* P_d + Q_d + P_{cd} + T_d(\text{ACK})}$$

$$1 = \frac{N \times 16}{16 + 2^* 150 + 5 + 1} \Rightarrow 1 = \frac{N * 16}{322} = \frac{322}{16}$$

N = 20.125
N = ⌈20.125⌉ = 21

Q12. The distance between two stations M and N is L km. All frames are K bits long. The propagation delay/km is 't' seconds. Let R 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 M —— d = L km —— N   Propagation delay for 1 km = t sec
Frame size = K bits, B = R bits/sec.   - for 'L' km = tL sec.

$T_d(\text{frame}) = \frac{L}{B} = \frac{K}{R}$ sec.

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

$$= \frac{W_s * \frac{K}{R}}{\frac{K}{R} + 2 * Lt} = 1 \Rightarrow W_s \times \frac{K}{R} \times \frac{R}{K + 2LtR}$$

$$W_s = \frac{K + 2LtR}{K}$$

min seq. no. required $= \frac{K + 2LtR}{K}$

min no of bit required in the seq no field $\left\lceil \log \frac{K + 2LtR}{K} \right\rceil$

Q13. Consider two hosts are connected with direct link having data transfer rate 10 Mbps and signal speed 3 msec/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 $B = 10$ Mbps $= 10 \times 10^6$ bit/sec   Pkt size = 5000 byte

propagation time for 6km = 18 msec $= 8 * 5{,}000$

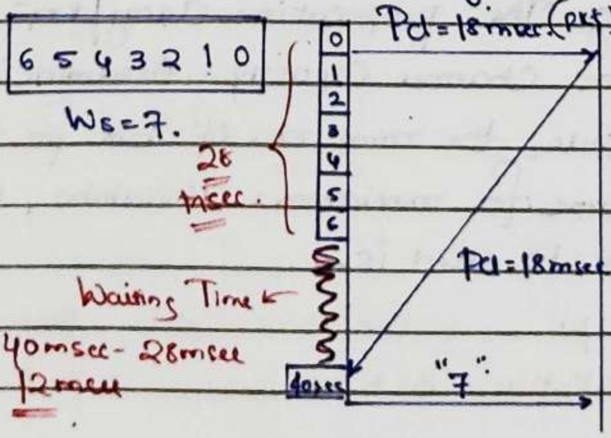
Seq. no = 3 bit $= 40{,}000$ bit

Seq no = k bit,

W_s	W_R	W_s	W_R
$2^k - 1$	1.	$2^3 - 1$	1.

$N = 7$ (Sender window size in GB-N)

$$T_d(\text{frame}) = \frac{F.S}{\text{Bandwidth}} = \frac{40{,}000 \text{ bits}}{10^7 \text{ bit/sec}} = 4 \times 10^{-3} \text{ sec.} = 4 \text{ msec}$$



Waiting Time
$= 40$ msec $- 28$ msec
$= \underline{12 \text{ msec}}$

Max amount of time the sender remain idle = Total time − useful time

= Total time − N * Td

= 40 msec − 7 * 4 msec

= 40 msec − 28 msec

= $\underline{12}$ msec

Total time = Td(frame) + 2 * pd + Qd + Pcd + Td(ACK)

= 4 msec + 2 * 18 msec

RTT = $\underline{40}$ msec

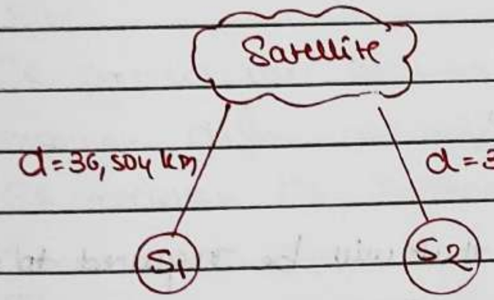
Q14 A 1 Mbps satellite link connects two ground stations. The altitude of the satellite is 36,504 km and speed of the signal is 3×10^8 m/sec. What should be the packet size for a channel utilization of 25% for satellite link usage go-back-127 sliding window. Assume that the acknowledgement packets are negligible in size and there are no errors during communication.

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

$v = 3 \times 10^8$ m/sec $= 3 \times 10^5$ km/sec

distance = 2 * 36,504

= 73,008 km



Packet size = ?

$\eta = 25\% = \frac{1}{4}$, GBN-127

N = 127

$P_d = \frac{d}{v} = \frac{73,008 \text{ km}}{3 \times 10^5 \text{ km/sec}} = 24336 \times 10^{-5}$ sec.

$= .24336$ sec.

$$\frac{1}{4} = \frac{N * Td(\text{frame})}{Td(\text{frame}) + 2 * pd + Qd + Pcd + Td(\text{ACK})}$$

$$= \frac{1}{4} = \frac{127 * Td}{Td + 2 * pd}$$

$\Rightarrow 127 * 4 * Td = Td + 2 * pd$

$508\ Td = Td + 2 * pd$

$507\ Td = 2 * pd$

$Td = \frac{2 * pd}{507}$

$$Td = \frac{2 \times .24336 \text{ sec}}{507}$$

$$\frac{L}{B} = \frac{2 \times .24336 \text{ sec}}{507} \qquad L = \frac{2 \times .24336 \text{ sec} * 10^6 \text{ bits/sec}}{507}$$

$L = 960$ bits $= \frac{960}{8}$ $\quad \underline{L = 120 \text{ Byte}}$

Q15. Frames of 1000 bits are sent over a 10^6 bps duplex link b/w two hosts. The propagation time is 25ms. Frames 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
Frame size = 1000 bit
$B = 10^6$ bits/sec
propagation time = 25 ms.

Capacity of Link = $B * pd$
$= 10^6$ bits/sec $\times 25 * 10^{-3}$ sec
$= 10^3 \times 25$ bits
$= 25{,}000$ bits.

Capacity of Link (in frames)
$= \frac{(\text{Capacity of Link})\ \text{bits}}{(\text{Frame Size})\ \text{bits}} = \frac{25{,}000\ \text{bits}}{1000\ \text{bits}}$

No of frames = 25
$2^k = 25$
$K = 5$ bit
$I = k$

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 frames.
Suppose that SW protocol is used with the sender window size of 2^I, wher I is the no. of bits earlier and acknowledgements are piggy backed. After sending 2^I frames, what will be the min time sender will have to wait before starting transmission of the next frame?

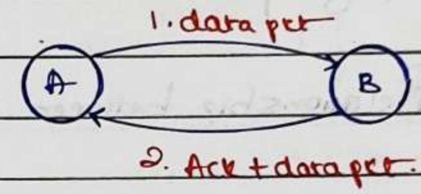
Ans
Sender window size $= 2^I = 2^5 = 32$.
min time sender have to wait before starting transmission of next frame = Total time - useful time
= Total time - $N * Td$(frame)
= 52 msec - $32 * 1$ msec
= 20 msec

$Td(\text{frame}) = \frac{1000}{10^6} = 10^{-3}$ sec = 1 msec

Total time = Td(frame) + 2* pd + Qd + Pod + Td(Ack)

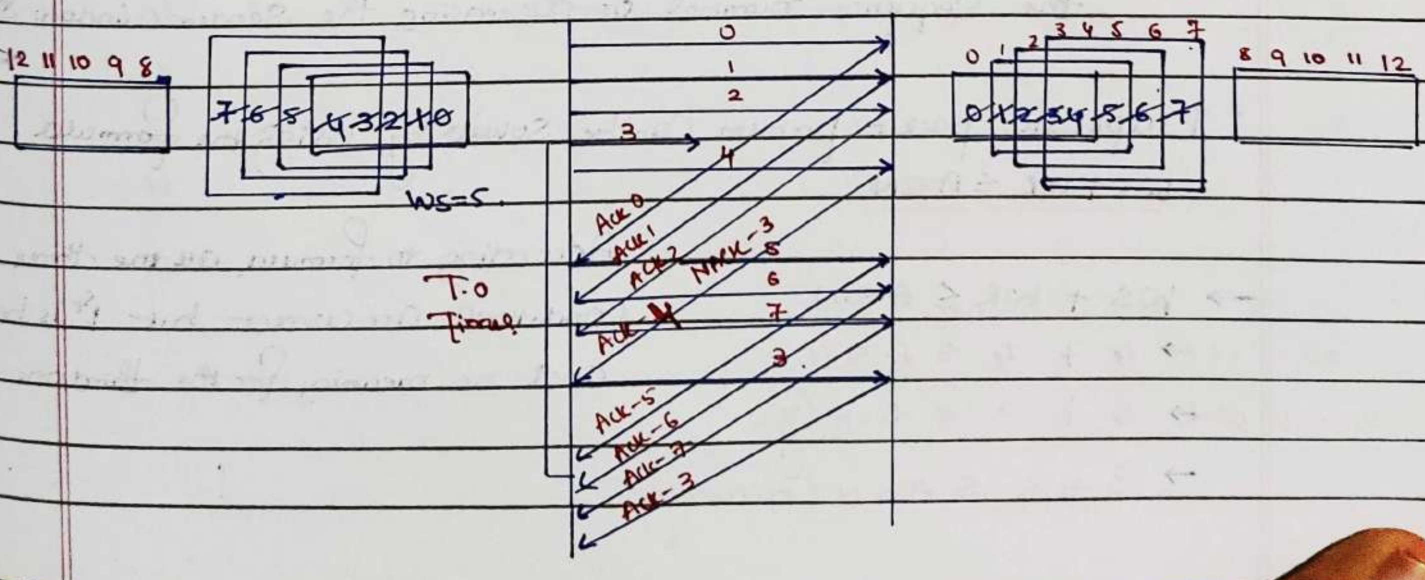
= 1msec + 2* 25 + 1

= 52msec.

General Approach	Piggy Backed
	

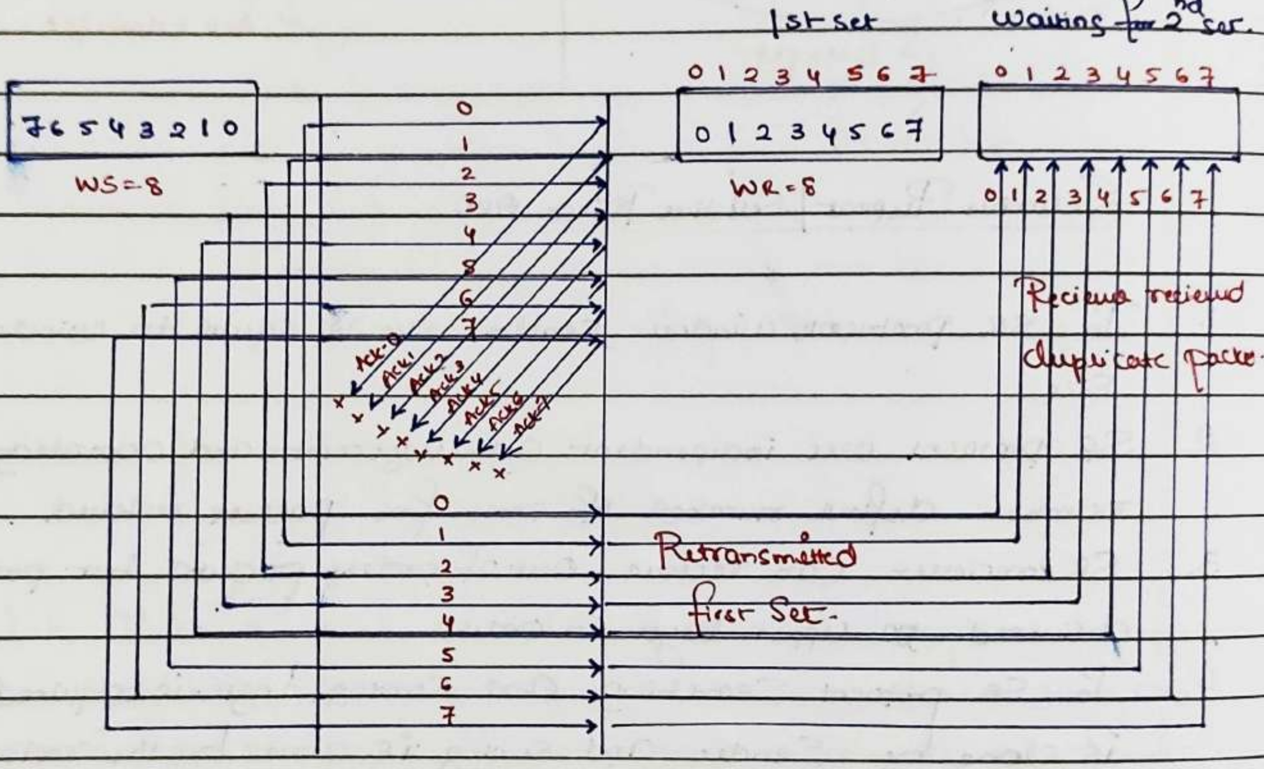
Selective Repeat / Selective Reject ARQ.

1. In SR protocol window sender size is equal to window reciever size
2. SR protocol uses independent acknoledgement and acknoledgement number define number of error free packets recieved.
3. SR reciever can recieve 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 reciever
5. Timer is maintained for each and every frame in the window at sender side.



1. For 1st out of order delivery or if packet recieved is Corrupted then NAK for respective packet is sent by reciever to Sender.
2. When Sender recieve NAK-3 then it will search in the window for packet 3 and immediately packet 3 is retransmitted even though it's timer is not expired.

<u>Relationship between window size and Sequence no.</u>

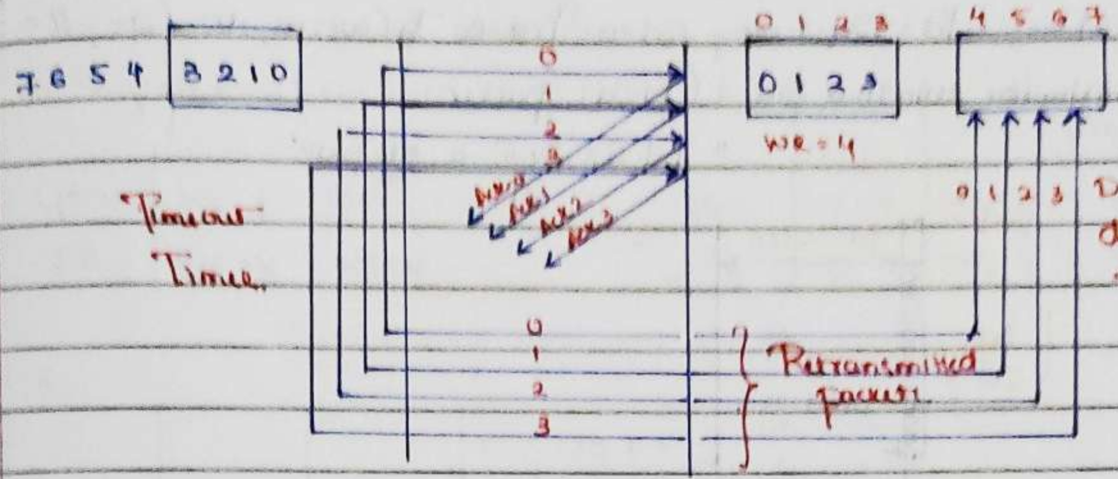


<u>Note:</u> * Duplicate packet Problem Can be Solved by increasing the sequence number or decreasing the sender window size.

* Duplicate packet Problem Can be Solved by using the formula <u>$WS + WR \le ASN$</u>.

→ $WS + WR \le A.S.N$
→ $4 + 4 \le A.S.N$
→ $5 + 3 \le ASN$ (yes)
→ $3 + 5 \le A.S.N$ (no meaning)

According to formula, all the three Conditions are correct but 1st is best and no meaning for the third one.



Duplicate packet discarded by the receiver.

$WS + WR \leq ASN$

$4 + 4 \leq 8$ (yes)

no problem of any pkt.

1. Sequence no = 8 (0-7)

WS	WR
4	4.

2. Sequence No = 16 (0-15)

WS	WR
8	8

3. Seq No = N (0-N-1)

WS	WR
N/2	N/2.

4. Seq no = 3 bit

Total seq no = $2^3 = 8$ (0-7)

WS	WR
~~8~~4	4

5. Seq No = 4 bit

Total sequence no = $2^4 = 16$ (0-15)

WS	WR
8 $[2^{4-1}]$	8 (2^{4-1})

6. Seq no = k bit

WS	WR
2^{k-1}	2^{k-1}.

7.

WS	WR.	Min. Sequence no required.
4	4	8
8	8	16
N	N	2N

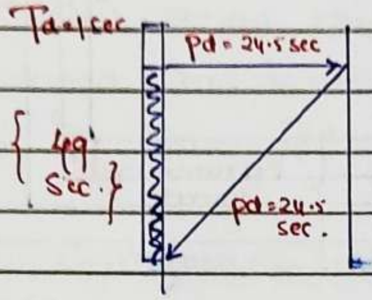
Seq no = 8 (0-7)

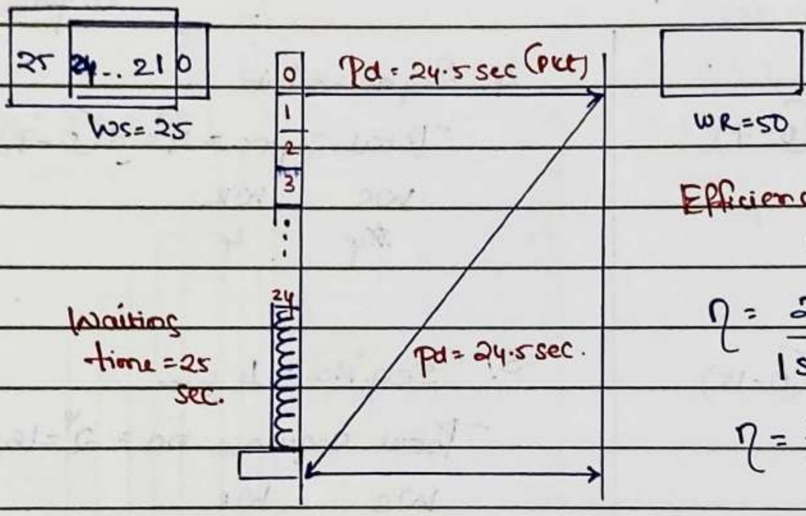
WS	WR	
4	4 ✓	
5	3 ✓	
1	2 ✗	WS > 1 in SR
1	1 ✗	Stop & wait

Q. $T_d = 1$ sec, $P_d = 24.5$ sec, $Q_d = 0$, $Pr_d = 0$, $T_d(ACK) = 0$, $W_S = 25$, $\eta = ?$

Maximum window size $= (1 + 2a)$ packet.

$= 1 + 2 \times \frac{24.5}{1} = \underline{50}$ pkt





Efficiency $= \frac{25}{50} = \frac{1}{2} = \underline{50\%}$

$\eta = \frac{25 \times 1}{1\,sec + 2 * 24.5\,sec + 0 + 0 + 0}$

$\eta = \frac{1}{2} = \underline{50\%}$

$$\boxed{\text{Efficiency} = \frac{W_S * T_d(\text{frame})}{T_d(\text{frame}) + 2 * P_d + Q_d + Pr_d + T_d(\text{Ack})}}$$

Q. $\eta = \frac{1}{2}$, Bandwidth = 40 mbps, Throughput = ?

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

OR

$$\boxed{\text{Throughput} = \frac{W_S \times \text{Frame Size}}{\text{Total time}}}$$

Throughput $= \frac{1}{2} \times \overset{20}{40}$

$= \underline{20}$ mbps

1. SR protocol required more sequence number in comparision of GBN

(i) Seq no = 8 (0-7)

GB-N	WS = 7	WR = 1
SR	WS = 4	WR = 4

(ii)

			Min. seq. no required
GBN	WS = 7	WR = 1	8
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 comparision of GB-N.

	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 acknoledgement.

	Stop and wait	GBN	SR
Efficiency.	$\eta = \frac{Td}{\text{Total time}}$	$\eta = \frac{N * Td}{\text{Total time}}$	$\eta = \frac{Ws \times Td}{\text{Total time}}$
Throughput.	$\eta * B$	$\eta * B$	$\eta * B$
Buffer	1+1	N+1	N+N
Seq-No	2 (0 & 1)	N+1 (0-N)	2N (0-2N-1)
Seq.no = k bit	-	Ws: 2^k-1, WR: 1.	Ws: 2^{k-1}, WR: 2^{k-1}.
Total time.	Same for all	Same for all	Same for all

classmate
Date
Page

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 75. What will be the sequence no. required in GBN and SR protocol?

Ans. Sender window size = N.

min seq. no in GBN = N+1 (0-N)

" " " " SR = N+N = 2N (0-2N-1)

$\therefore$ GBN = 76 (0-75)

SR = 150 (0-149)

Q3. If 'N' is the maximum sequence number then window size in GB and SR is.

Ans. Seq. no = 8 (0, 1, 2, 3, 4, 5, 6, 7) ← N

GB-N

WS	WR
7	1.
N-1.	1.

SR.

WS.	WR
4	4
$\frac{N+1}{2}$	$\frac{N+1}{2}$

$\therefore$ Ans = N, $\frac{N+1}{2}$

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.

η sliding window = N * η stop & wait

$\eta_{S\&W}$ = $\frac{1}{N}$ x sliding window

$\therefore \eta_{\text{stop \& wait}} = \frac{1}{5} \times 1 = 20\%$

Q5. Consider minimum number of bit required for sequence number field in SR. ARQ for maximum utilization are 4, then efficiency of Stop & wait ARQ is ______

Ans η sliding window = N^* η stop & wait   N – Sender window size.

η stop & wait = $\frac{1}{N} * \eta$ sliding window   Seq no = 4 bit

Ws. Wr.

$= \frac{1}{8} \times 1 = 0.125$ 2^{4-1} 2^{4-1}

$= \underline{12.5\%}$ = 8 8.

Q6. Assume we need to design SR protocol for a network in which B is 1 Mbps and average distance btw. Sender & reciever is 5000 Km. Assume that avg pkt size is 5000 bit. Propagation speed in the media is 2×10^8 m/sec. If window sender size is 8 and process delay is 0.5 msec and qd = 2msec. η = ?

Ans. $B = 10^6$ bit/sec, d = 5000 km $v = 2 \times 10^8$ m/sec.

Pkt size = 5000 bit. $v = 2 \times 10^5$ Km/sec.

$Pd = \frac{d}{v} = \frac{5000 \text{ Km}}{2 \times 10^5 \text{ Km/sec}}$ $Td(\text{Frame}) = \frac{L}{B} = \frac{5000 \text{ bit}}{10^6 \text{ bit/sec}}$

$= 25 \times 10^{-3}$ sec $= \underline{25 \text{ msec}}$. $= 5 \times 10^{-3}$ sec $= \underline{5 \text{ m sec}}$

Ws = 8, Qd = 2 m sec, Prd = 0.5 m sec.

$\eta = \frac{Ws \times Td(\text{frame})}{Td(\text{frame}) + 2^* pd + Qd + Prd + Td(\text{Ack})} = \frac{8 \times 5}{5 + 2^* 25 + 2 + 0.5}$

$= \frac{40}{57.5} = 0.6956$

$= 69.56\%$

$\cong \underline{70\%}$.

H.W

Q7. In selective repeat ARQ, packet size is 2000 byte transmission time for one packet is 1 ms. If distance btw hosts is 10 km & signal speeds is 4 ms/km. and frame seq no. are 6 bit long in frame format then throughput (in Mbps) = $\underline{6.32 \text{ Mbps}}$.

classmate
Date
Page

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 carries 1KB of data, the min no. of bits you need for the sequence number.
(i) for RWS = 1 (GBN) and
(ii) for SWS = RWS (SR) is.

$B = 10^6$ bits/sec

Pd = 1.25 sec.

Frame size = 1KB

$= 1024 \times 8 = 8196$ bits.

$$Td(\text{frame}) = \frac{8192 \text{ bits}}{10^6 \text{ bits/sec}}$$

$= 0.008192$ sec.

$$\text{efficiency} = \frac{N * Td(\text{frame})}{Td(\text{frame}) + 2^* pd + Qd + Prod + Td(ack)}$$

$$1 = \frac{N \times 0.008192}{0.008192 + 2^* 1.25}$$

$$N = \frac{0.008192 + 2 \times 1.25}{0.008192}$$

$N = 306.17$

$N = \lceil 306.17 \rceil = \underline{\underline{307}}$

Sliding Window	GB-N	SR
Minimum sequence no. required = 307 $2^k = 307$ $K = 9$ bit.	Min SeqNo required in GB-N $= 307 + 1 = 308$ $2^k = 308$ $k = 9$ bit	Min. seq no. required in SR is. $= 2N + 1$ $= 614 + 1$ $= 615$ $\cdot\ 2^k = 615$ $k = 10$ bit

$\therefore$ Ans = 9, 10

HW

Q9. Consider a 128×10^3 bits/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. $B = 128 \times 10^3$ bits/sec

$Pd = 150$ m sec

Frame size $= 1KB$

$= 1024 \times 8$

$= 8192$ bits

$$Td = \frac{L}{B} = \frac{8 \times 1024}{128 \times 10^3} \; (2^3)$$

$= 64 \times 10^{-3}$ Sec.

$= 64$ m sec.

$$\eta = \frac{W_s * Td(frame)}{Td(frame) + 2^* pd + Qd + Prd + Td(ack)}$$

$$1 = \frac{W_s \times 64}{64 + 2 * 150} \qquad W_s = \frac{364}{64}$$

$W_s = 5.68$

$W_s = \lceil 5.68 \rceil$

Min. sequence no. $= 6 + 6 = 12$

$2^k = 12$

$k = 4$ bits

Q10. A 3000 Km long trunk operating at 1.536 Mbps is used to transmit 64 byte frame and use SWP. If propogation speed is 6 μsec/km then the number of bits should the sequence number is.

Ans. $d = 3000$ Km, $B = 1.536 \times 10^6$ bits/sec.

Frame size $= 64$ Byte

$= 64 \times 8$

$= 512$ bits.

Prop. time for 1 Km $= 6$ μsec

propogation time for 3000 km

$= 3000 \times 6$ μsec $= 18000$ μsec.

$$Td(frame) = \frac{L}{B} = \frac{512 \text{ bits}}{1.536 \times 10^6 \text{ bits/sec}}$$

$= 333.33 \times 10^{-6}$

$= 333.33$ μsec.

$$\eta = \frac{N * Td(frame)}{Td(frame) + 2^* pd + Qd + Prd + Td(Ack)}$$

$$= \frac{N \times 333.33 \,\mu sec}{333.33 \,\mu sec + 2^* 18000 \,\mu sec}$$

$$N = \frac{36,333.33 \,\mu sec}{333.33 \,\mu sec}$$

$N = 109.00108$

$N = \lceil 109.00108 \rceil = 110$

Min sequence no is

$2^k = 110$

$k = 7$ bits

classmate

Date
Page

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 ms then minimum no. of bits required for sequence number field for maximum utilization is

Ans $L = 4000$ bits

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

$Pd = 18$ ms.

$Td(\text{frame}) = \frac{4000}{10^6} = \underline{4 \text{ msec}}$

$$\eta = \frac{Ws \times Td(\text{frame})}{Td(\text{frame}) + 2^* pd + Qd + Prd + Td(\text{ack})} = \frac{Ws \times 4\text{msec}}{4\text{msec} + 2\times 18 \text{ msec}}$$

$= Ws = \frac{40}{4} = 10$

Min sequence no $= Ws + WR$

$= 10 + 10$

$= 20.$

$2^k = 20$

$2^5 = 20 \quad \therefore \underline{\underline{k = 5 \text{ bit}}}$

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 size $= 32B$

$= 32 \times 8 = 256$ bits

RTT $= 80$ msec

$B = 128 \times 10^3$ bits/sec.

$$Td(\text{frame}) = \frac{256}{128 \times 10^3 \text{ bit/sec}}$$

$= 2 \times 10^{-3}$ sec $= \underline{\underline{2 \text{msec}}}$

$$\eta = \frac{Td(\text{frame})}{RTT} = \frac{2 \text{ msec} * Ws}{80 \text{ msec.}}$$

$$Ws = \frac{80 \text{ msec}}{2 \text{ msec}} = \underline{\underline{40}}$$

AD Steps to solve SWP Problem.

1. Calculate RTT
2. Based on given bandwidth and RTT calculate no. of bits we all

able to transfer even in RTT and equate it as window in terms of bits (W_{bits}) = $B * RTT$.

3. W_{pkt} or $W_p = \frac{W_{bit}}{\text{(Packet size)}}$

4. Minimum Sequence no. required = W_p

5. $2^k = W_p$

Where k = no. of bits required in the sequence no field.

Q13 Consider two node A and B round trip delay between these is 80 mS and bottleneck bandwidth of line between A and B is 512 kbps, the optimal window size (in packets) if the packet size is 64 Byte ______.

Ans. $RTT = 80\ msec = 80 \times 10^{-3}$ sec, $B = 512\ KBps = 512 * 10^3 \times 8$ bits/sec

packet size = 64 byte = 64×8 bits.

As Rule:

1. RTT = 80 msec.

2. $W_{bits} = B \times RTT = 512 \times 10^3 \times 8\ \text{bits/sec} \times 80 \times 10^{-3}\ \text{sec} = 512 \times 8 \times 80$ (bits)

3. $W_{pkt} = \frac{W_{bits}}{\text{(pkt size) bits}} = \frac{512 \times 8 \times 80}{64 \times 8} = 640$ pkts

$Td(\text{frame}) = \frac{L}{B} = \frac{64 \times 8}{512 \times 10^3 \times 8}$

$= \frac{1}{8} \times 10^{-3}$

$= \frac{1}{8}$ msec.

$\eta = \frac{W_S \times Td(\text{frame})}{RTT}$

$W_S = \frac{RTT}{Td(\text{frame})} = \frac{80\ \text{msec}}{\frac{1}{8}\ \text{msec}}$

$= 80 \times 8 = 640$ pkts.

IPv4 Header and Fragmentation.

IPV4 Header.

VER 4.	HL 4.	Service 8	Total Length 16	→ 32 bit = 4 Byte
Identification No. 16.	Flags 3	Fragment Offset 13.		→ 32 bit = 4B
Time to Live 8	Protocol 8	Header Checksum, 16		→ 32 bit = 4B
Source IP Address 32				→ 32 bit = 4B
Destination IP Address, 32				→ 32 bit = 4B.
Option. (0-40 Byte)				5 x 4B = 20 Byte

20 Byte fixed

40 B variable

Minimum header size = 20B + 0 B = 20 B.

Maximum header size = 20B + 40B = 60 B.

Header Length =(4 bit)
↳ max. no = 1111 = 15.

Max. Header size = 60 Byte.

$S.f \rightarrow \frac{60}{x} = 15.$

$(SF) \rightarrow \frac{60}{4} = 15$

Header size	HLF
$\frac{20B}{4} = 5$	0101
$\frac{40B}{4} = 10$	1010

Header Size	HLF
$\frac{30B}{4} = 7.5$ ✗	
30B+2B = $\frac{32}{4}$ = 8.	1000

dummy byte, → Option
↓
Padding = 2 byte

HLF	Header Size
1010 = 10	10×4 = 40 Byte
1100 = 12	12×4 = 48 Byte
1000 = 8	8×4 = 32 Byte
1111 = 15	15×4 = 60 Byte
HLF (5-15)	Header size (20-60 B)

Version (4 bit) : It is used to indicate IPv4 or IPv6.
(0100 (0110

Services : In this interpretition the first 3 bits are called precedence bit (priority bit) and next 4 bit are 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 services — not used.

D : minimum delay
T : maximise throughput
R : High reliability
C : minimum cost.

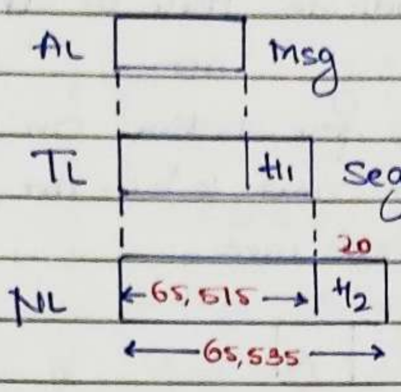
Priority : It is a 3 bit subfield ranging from 0-7 (000 to 111 in binary). Priority field is needed if router is congested need to discard some datagram, those datagram that have the lowest priority are discarded first.

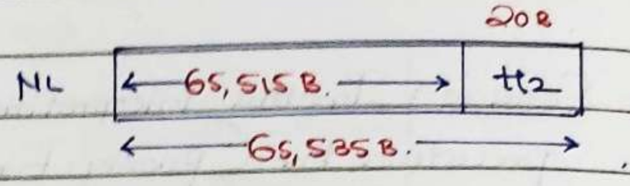
Types of Service : It is a 4 bit subfield. Each bit having a special meaning although a bit can be 0 or 1. One and only one of the bits can have the value 1 in each datagram.

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 → max no. $2^{16}-1$.

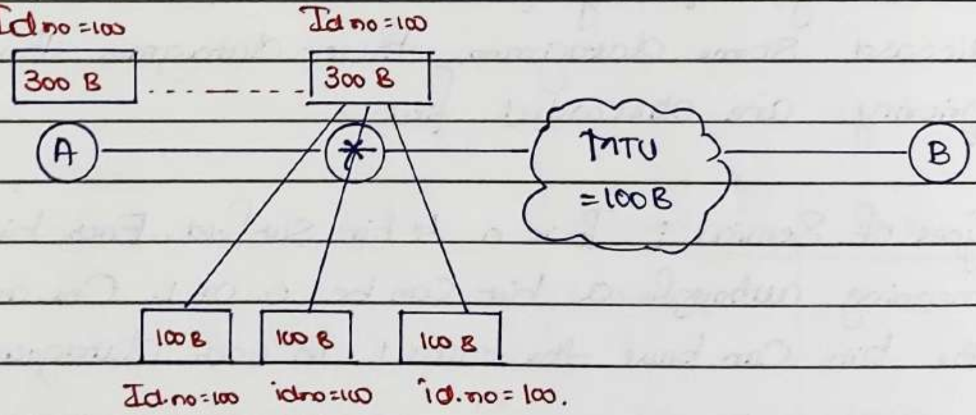




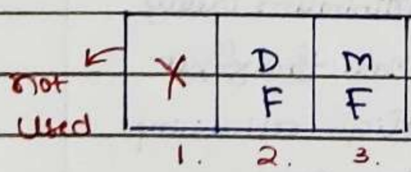
Maximum data size at NL = 65,515 Byte.

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.



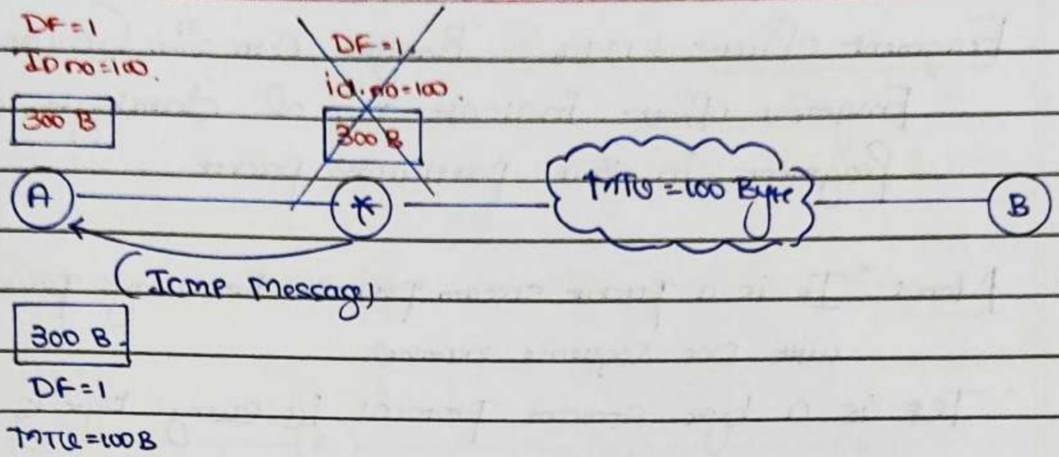
2nd bit is called Don't fragment

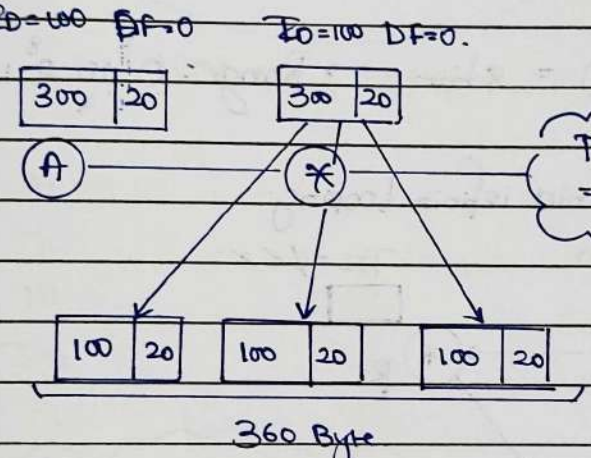
3rd bit is called more fragment.

DF (Don't Fragment)

DF = 1 means datagram can't be fragmented

DF = 0 means datagram can be fragmented





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

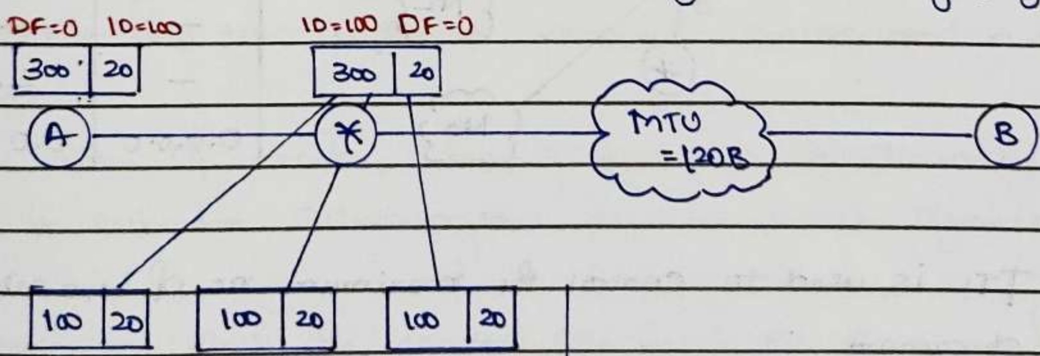
$$= \frac{300}{360} = 0.833$$

$$= \underline{\underline{83.33\%}}$$

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.



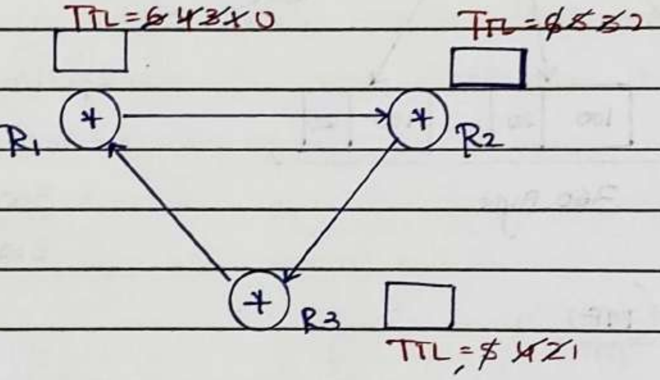
100	100	100	ID.no
0	1	1	MF
200	100	0	Fragment Offset.

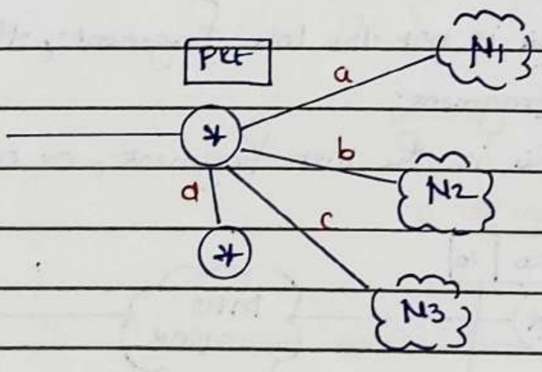
Fragment Offset : (13 bit) Range 0 to $2^{31}-1$ (0 to 8191)
Fragment offset indicate no. of databyte ahead of the fragment in that particular packet.

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 → Range : 0 to 2^8-1 = 0 to 255

1. TTL is used to avoid infinite Looping.





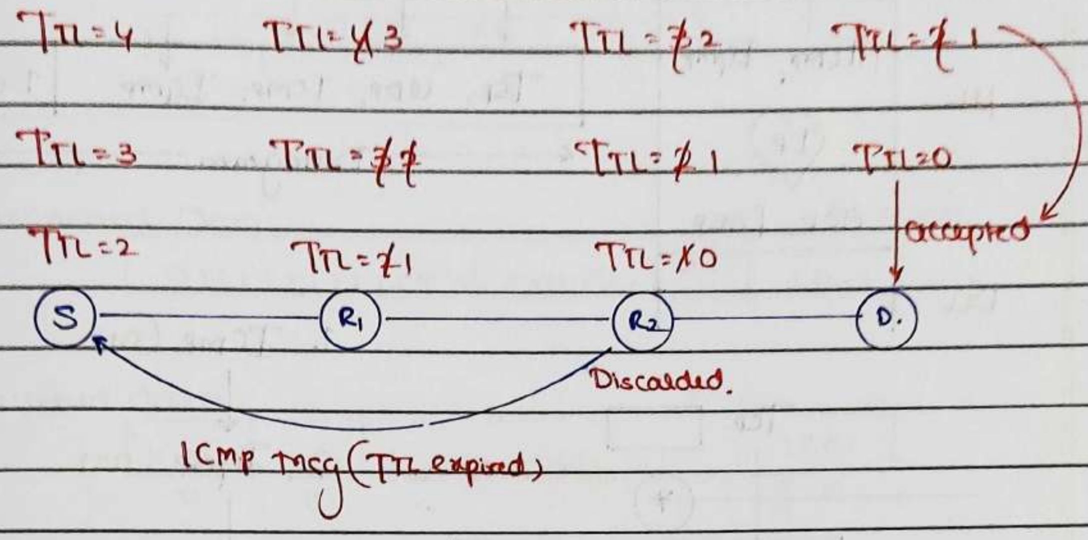
Routing Table

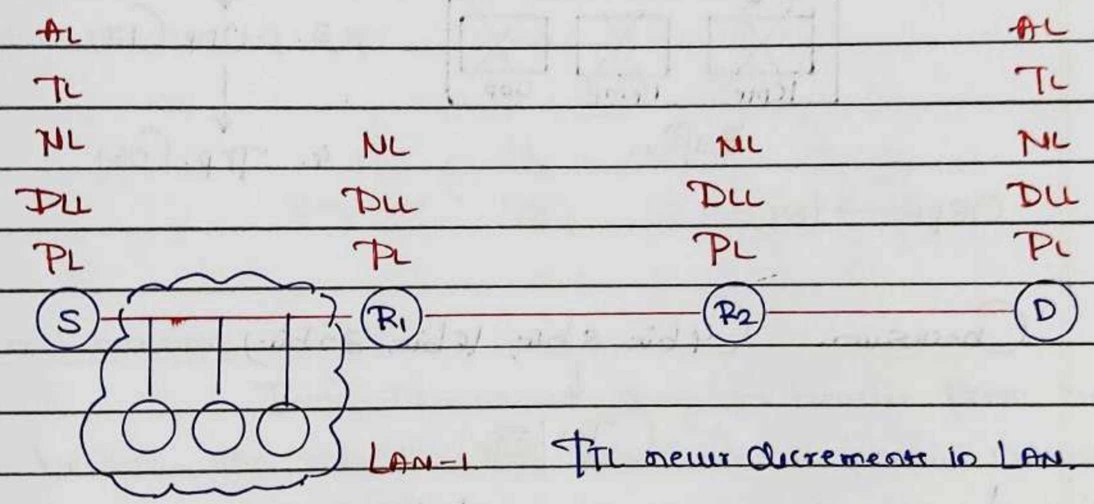
NID	SM	I/F
—	—	a
—	—	b
—	—	c
0.0.0.0	0.0.0.0	d.

default

2. TTL is used to control the maximum no. of hops visited 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 it's destination, then datagram is discarded and

an ICMP message is sent back to sender.



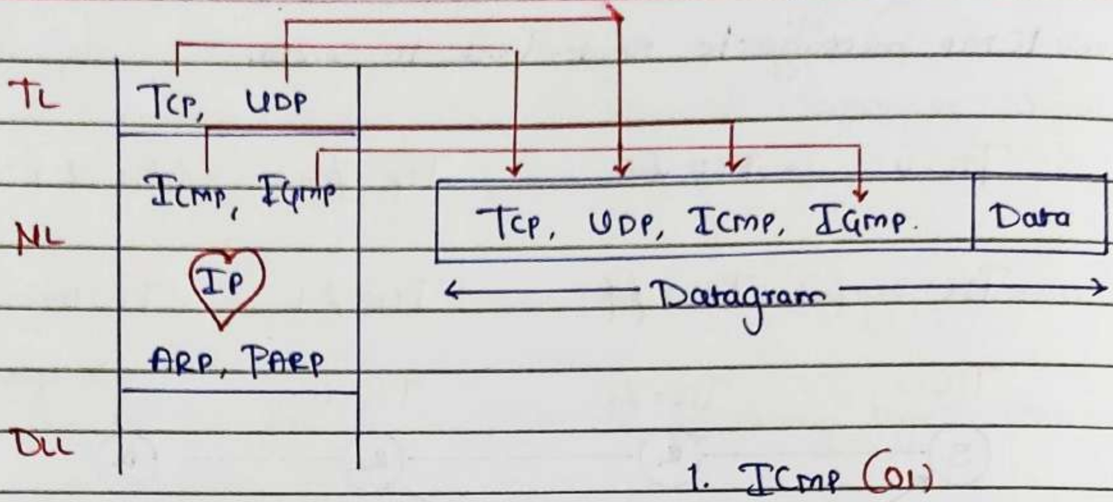


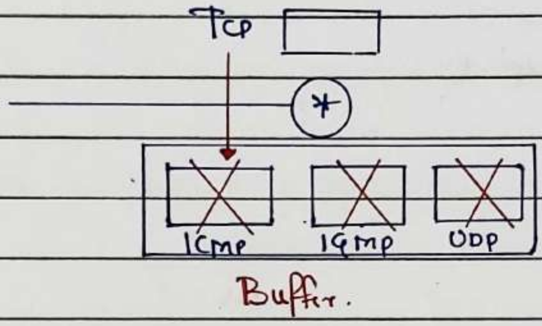
TTL never decrements in LAN.

Protocol (8 bit)

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 it contains.
3. The order in which the router eliminates the datagram from buffer is:

$$\boxed{ICMP > IGMP > UDP > TCP}$$





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.

1.

0111 1011 1100 0000 0110	36

0111 1011 1100 0000 0110	−36

36−36 = 0 (No error)

Checksum = 4 bit $\xrightarrow{\text{Max. no.}}$ 1111 : 15.

Checksum = 36 = $\boxed{10}0100$

$\hookrightarrow + 10$

0110 → 6

1's Compliment → 1001 → 9

Transmitted data. Checksum.

0111 1011 1100 0000 0110	1001

Recieved data.

0111	1011	1100	0000	0110	1001
7	11	12	0	6	9

7+11+12+0+6+9 = 45 : $\boxed{10}1101$

$\hookrightarrow$ 10

1111

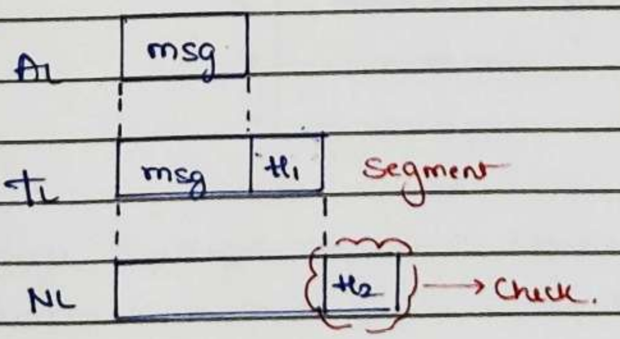
1's Compliment. → 0000 → no error

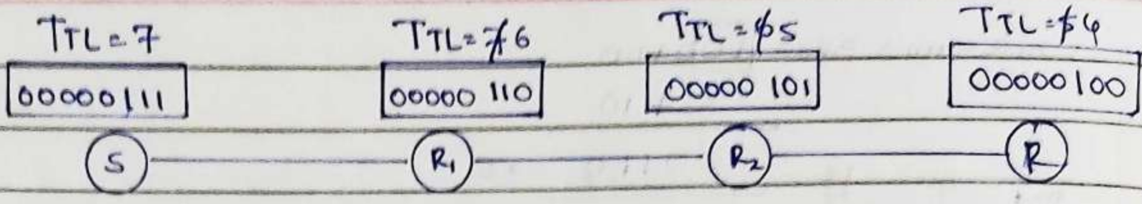
Header Checksum: (16 bit)

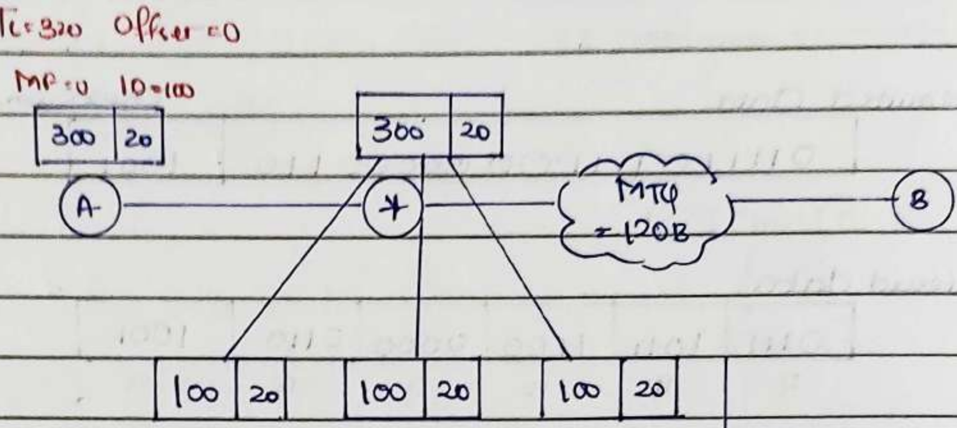
It is calculated only for header part not the data because the rest of the component in packet already covered by TCP checksum.

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 maybe changed at Router.







100	100	100	1000
0	1	1	MF
200	100	0	Offset
120	120	120	TL

VER, HL, Service	Total length	Id.no
0100 0101 10010010	1001101001001000	1000100000110101
16 bit	16 bit	16 bit

Flag and fragment offset	TTL, Protocol
1010 0010 0100 1000	$\underbrace{10010011}_{TTL}\underbrace{10100001}_{Protocol}$

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 IPv4 address of the source. This field remain unchanged during the time IPv4 datagram travel from source to destination.

Destination Address: This 32 bit defines the address of the destination. This field remains unchanged during the time IPv4 datagram travel from source to destination.

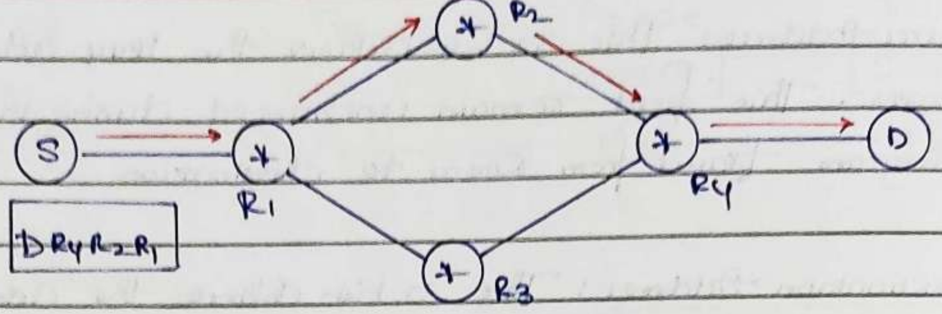
Not Changed	Maybe Changed	Definitely Changed
1. VER	Total Length	TTL
~~2. HL~~	MF	Header Checksum.
3. Services	Fragment offset.	
4. Identification no.	HL (if option fixed)	
5. DF	Option.	
6. Protocol		
7. SIP		
8. DIP.		

Option: The header of IPv4 datagram is made of two part a fixed part and a variable part. The fixed part is 20 Byte long and variable part can be maximum of 40 Byte.

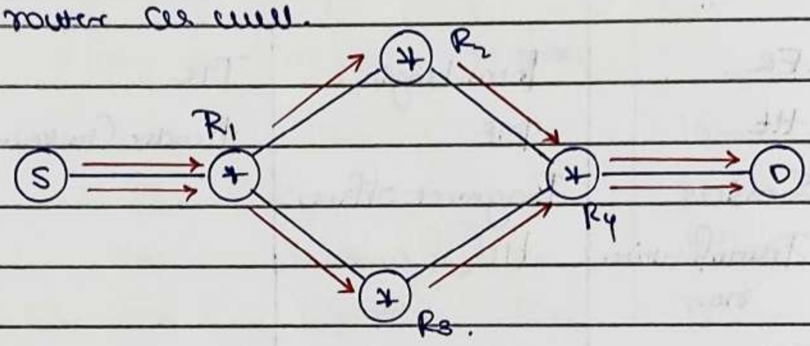
There are 5 options:

1. Strict source routing } Source will decide the root
2. Loose source routing }
3. Record routing { router will decide the route
4. Timestamp
5. Padding

1. Strict Source Routing: A strict source routing is used by the source to predetermine a route for datagram to travel through the Internet.

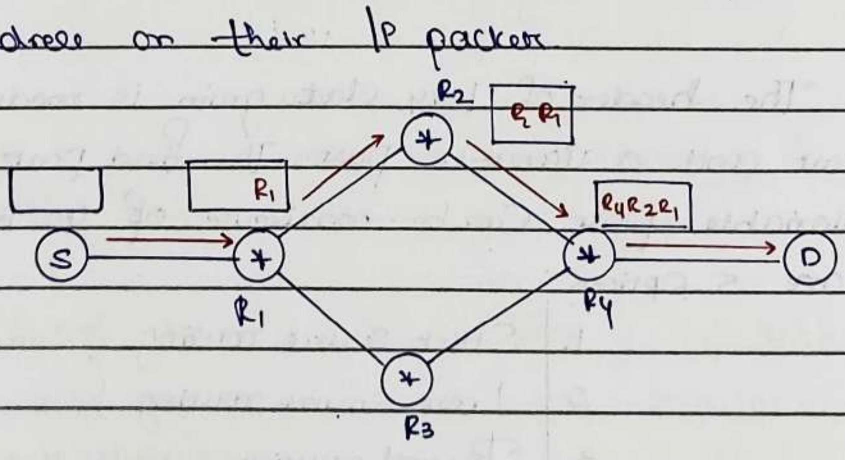


2. <u>Loose Source Routing</u>: A loose source route option is similar to strict source route but it is less rigid. Each router in the list must be visited, but the datagram can visit other routers as well.



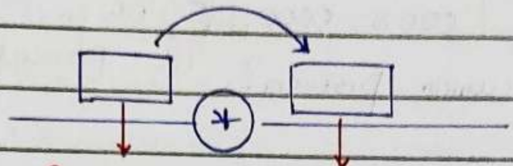
Two route.
$SR_1R_2R_4D$
$SR_1R_3R_4D$.

3. <u>Record Routing</u>: A record route option is used to record the internet routers that handle the datagram. It can list upto 9 router address. All the routers are supposed to record their IP address on their IP packet.



<u>Note</u>: First 16 bit (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 addresses. In 38 byte we can store 9 IPv4 addresses as each IPv4 address is of 4 byte.

4. Time stamp: It is used to find out delays at each router. Every router should record incoming and outgoing time.



9:05 Am   9:10 Am.   Delay = 5 min

Q1. In an IPv4 packet the value of HLEN is $(1100)_2$. How many Byte of options are being carried by this packets?

Ans $HLEN = (1100)_2 = 12$

Header size $= 12 \times 4 = 48$ Byte

-20 Byte (option)

28 Byte

Q2 In an IPv4 packet, the value of HLEN is 5, and the value of total length field is $(0048)_{16}$. How many byte of data are being carried by this packet?

Ans $HLEN = 5$

$TL = (0048)_{16}$

$= 4 * 16 + 8 \times 16^0$

$= 64 + 8 = 72$

$TL = D + Header$

$Data = TL - H$

$= 72 - 20 = 52$

Q3. An IPv4 packet has arrived with first few hexadecimal digit as shown

$(4|5|00|00 \; 5C|000 \; 3|00\,00|59|06 \ldots)_{16}$

(V', HL, Ser., T.L, id.no, F&F, TTL)

How many Hops does this packet take before being dropped?

Ans $TTL = (59)_{16}$

$= 5 \times 16^1 + 9 \times 16^0 = 89$

Hw

Q4. In an IPv4 packet the value of HLEN is $(1000)_2$, How many bytes of options are being carried by this packet?

Q5. An IPv4 packet has the first few hexa decimal digits as shown below

450000 5C | 0003 0000 | 59 06

TTL Protocol.

The above belong to which protocol?

Ans Protocol = $(06)_{16}$

$= 0\times16^1 + 6\times16^0$

$= 06 \quad \therefore$ TCP

Q6. In an IPv4 packet the value of HLEN is 10 and value of total length field is '0084' hexadecimal, how many byte of data are being carried by this packet?

Ans HLEN = 10

header size = 10×4 = 40 Byte

$TL = (0084)_{16}$

$= 8\times16 + 4\times16^0$

$= 132$

$TL = D+H$

$D = \cancel{H}TL - H = 132-20$

$= 92$

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 explains the need of this field?

Ans It can be used to prevent packet looping.

Q9. In the TCP/ICP 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?

classmate
Date
Page

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 occured during the transmission of D. When D reaches B which of the following IP header field(s) 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 in between 20 to 60B
But always multiple of 4. so ans is 20, 60.

Q15 An IPv4 packet has the first few Hexadecimal digits as shown below.

45000 5C000 30000 5905.

What is the size of data packet

Ans. $T_L = (005C)_{16}$

$= 5\times 16^1 + 12\times 16^0 = 92.$

Header Size $= 5\times 4$
$= 20$

$\therefore$ 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

Size of TCP data present in the datagram.

Ans. IPv4 header = 10

TL = 1000B

TCP header length = 15.

TL : $\underbrace{900 + 60}_{960}$ [Segment]

TL : $\underbrace{960 + 40}_{1000}$ [Datagram]

TCP data size = Total length (IP) - IP (H) - TCP (H)

= 1000 - 40 - 60

= 900.

Q17. An IPv4 packet has arrived with the first 16 bits as $[0100001011110000]_2$ the reciever discard this packet. Why?

Ans. VER = $(0100)_2$ = 4

HLEN = $(0010)_2$ = 2. Header size = $2*4$ = 8

Min header size = 20 Byte

Min HLEN field = $\frac{20}{4}$ = 5

∴ Invalid HLEN

Q18. An IPv4 packet has first few hexadecimal digits as shown below

450000 5C | 000 30000 | 59 060000 | 0A0C0E05

1st row | 2nd row | 3rd row | 4th row.

What is the source IP address in the IPv4 packet?

Ans. SIP = (0A.0C.0E.05)

= $10 * 16^0 = 10$ + $12 * 16^0 = 12$ $14 * 16^0 = 14$ $5 \times 16^0 = 16$

= 10.12.14.5.

Q19. Which of the following value is/are not possible of the TTL in a datagram?

Ans. TTL = 8 bit

Range = 0 to $2^8 - 1$

= 0 to 255.

TTL value cannot be zero

∴ TTL value cannot be 0, and 300

Note:

* If their is no option field (in IPv4 header) then the will not change when packet is moving from one packet to another.
* If their is a option field present in IPv4 header then the field maybe changed when packet is moving from one router to another router.

→ Total length = 16 bit.

↓

Max. no = $2^{16}-1 = 65,535$

Total length = Data + Header

NL: | 65,515 | 20(B) |

← 65,535 →

AL: | 65,495 | msg.

← 65,495 →

TL: | 65,495 | 20 | Segment

← 65,515 →

NL: | 65,515 | 20 | Datagram

← 65,535 →

DLL: | T | | H | Frame

→ AL can pass any size of data to transport layer.

← 1GB →

AL: | |

↓

TL: | 65495 | 65,495 | 65495 | 65,495 | . . .

Segmentation

Data.	H.
← 65,515 →	20

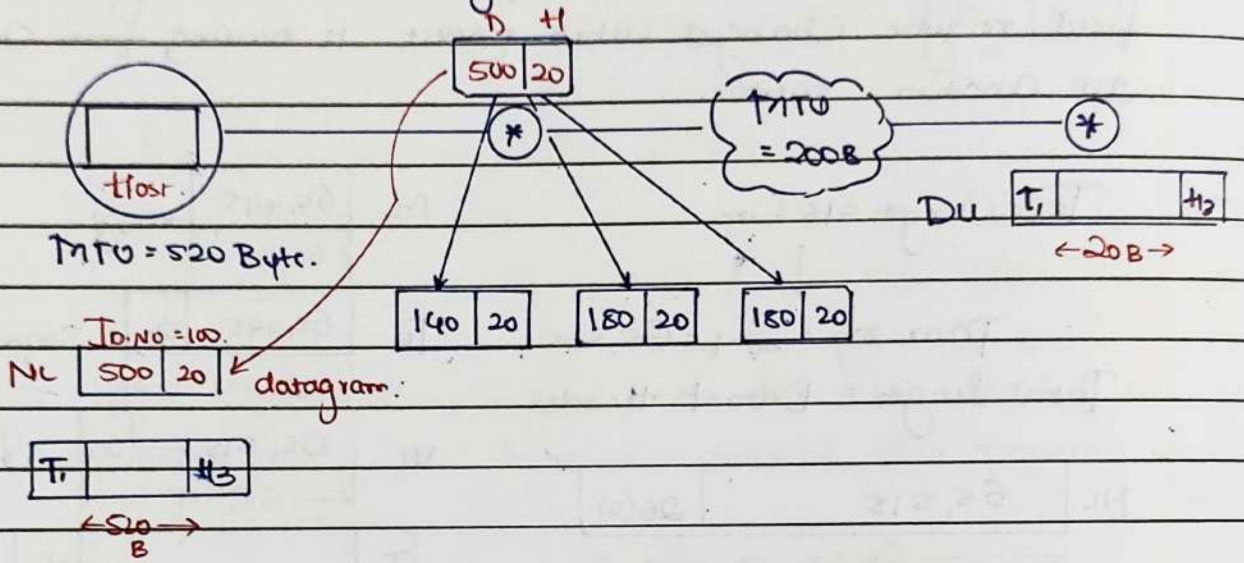
NL

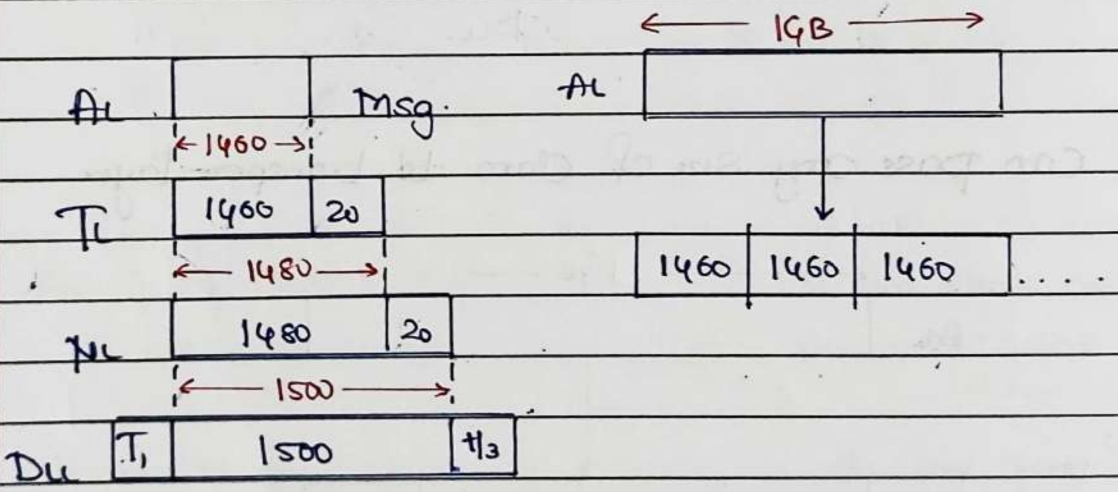
| 1480 | 20 | 1480 | 20 | .... | 1450 | 20 |

Fragmentation

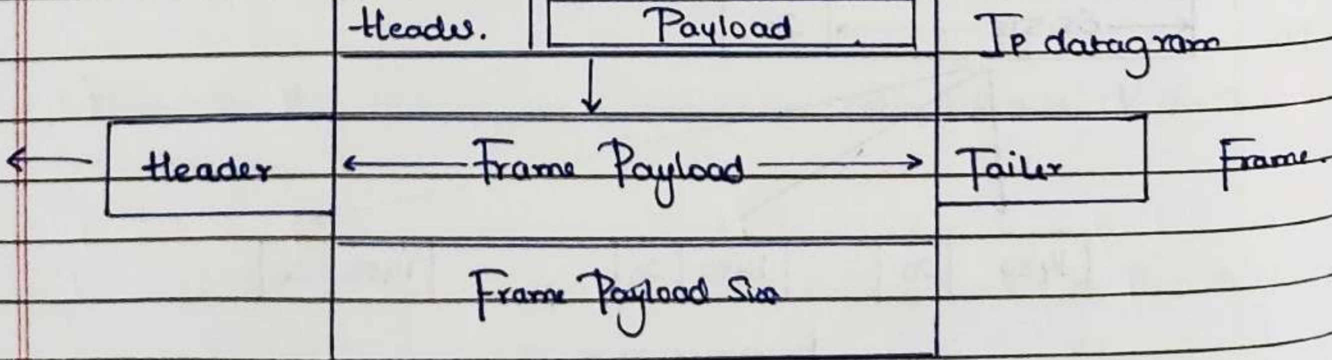
Fragmentation at Router.

MTU : Maximum amount of data that can be Stored in any data link layer.

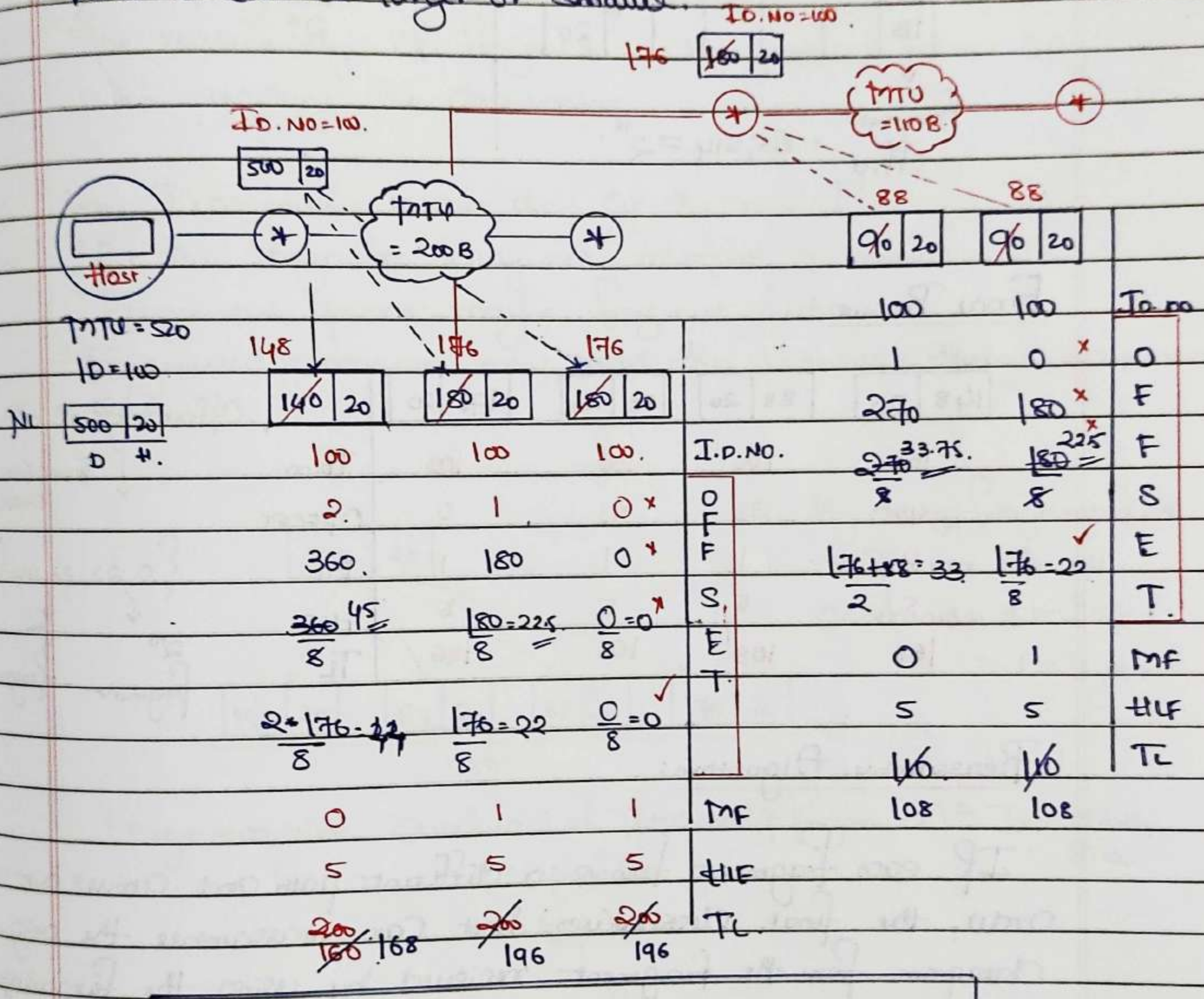


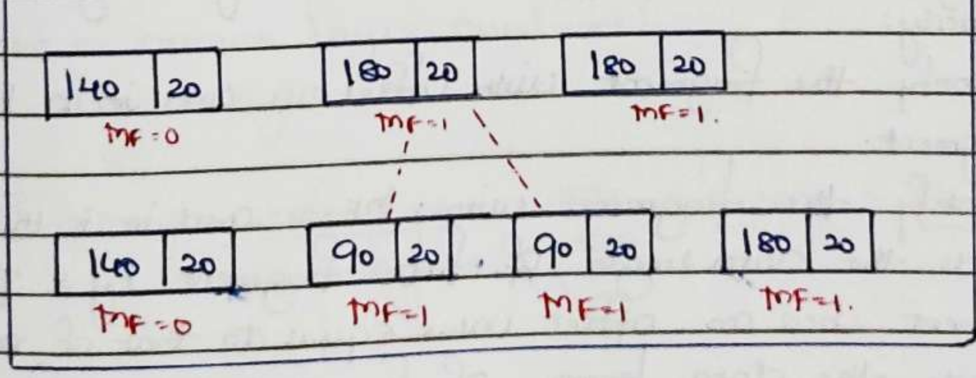


Maximum transfer Unit (MTU)



* When a datagram is encapsulated in a frame, the total size of the datagram must be less than this 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 = $2^{16}-1 = 65,535$.

NL |← 65,515 →| 20 |
|← 65,535 →|

← 65,515 → IP.
| 18 | | | | | 20 |
↓
Fragment offset = 65,514 = 2^{16}.

Fragment Offset = 13 bit.
Maximum no = $2^{13}-1 = 8191$

$\frac{2^{16}}{x} = 2^{13}$.
S.F ← x

$\frac{2^{16}}{2^{3}} = 2^{16-3} = 2^{13}$.

Final Result:

	148 | 20	88 | 20	88 | 20	176 | 20
ID.no	100	100	100	100
OFFSET	44	33	22	0
MF	0	1	1	1
TTL	5	5	5	5
TL	168	108	108	196

Offset = {22, 33, 0, 44}
↓ Increasing Order
{0, 22, 33, 44}
2nd fragment, 4th 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 recieved by using the following strategy:

1. Identify the fragment with offset = 0 and it is the first fragment.
2. Identify the fragment with MF = 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 that of reassm.

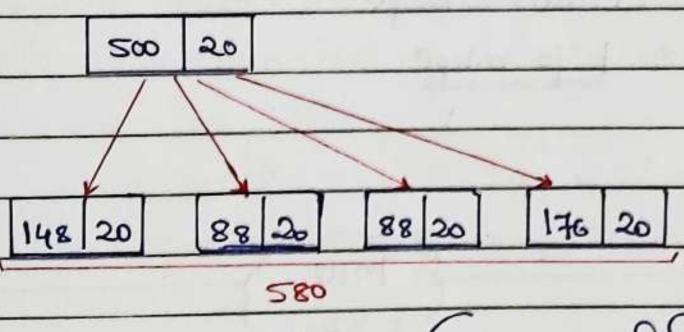
5. Repeat the process as many times as possible to cover all the fragment.

Note:

* Fragmentation is done by intermediary devices such as Router.
* The reassembly of fragmented datagram is done only after reaching the destination.

Q. Why Reassembly is not done at the router?

Ans. * All the fragment may not meet at a router.
* Fragmented packet maybe fragment further.
* Fragmented datagram may reach the destination through independent path.



By doing fragmentation at Router the NL Overhead = 580 - 520
= 60 Byte.

Fragmentation Overhead = (Total no of fragment - 1) * Ipv4 Header Size.
$= (4-1) * 20$
$= \underline{\underline{60}}$

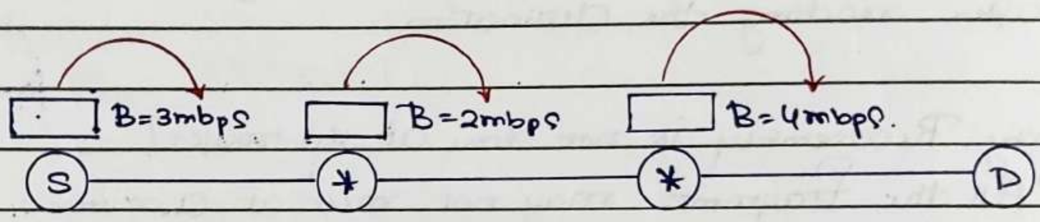
Q2 What is network layer overhead?

Ans 580 - 500 = 80 Byte.

$$\text{Efficiency} = \frac{\text{useful Byte}}{\text{Total Byte}} = \frac{500}{580} = 0.8620 = \underline{86.2\%}$$

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. $\boxed{\text{Total Overhead} = (\text{Total no. of fragments} - 1) * \text{Size of IP header}}$



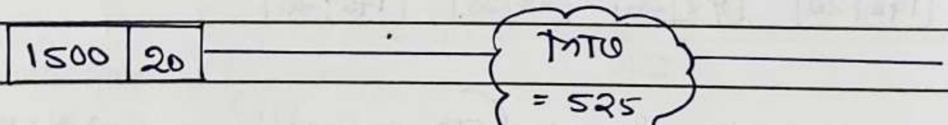
Throughput = $\eta * B$

Throughput = η * min. bandwidth

Throughput = 0.86×2 mbps

= $\underline{\underline{1.72 \text{ mbps}}}$

ex: 1.



	492 | 20	504 | 20	505 | 20
Offset	$\frac{2 \times 504}{8} = 126$	$\frac{504}{8} = 63$	$\frac{0}{8} = 0$
MF	0	1	1
TL	512.	524	524

classmate

Date ____
Page ____

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.

← 1000 B →

$12 \times 80 = 960$

$980 - 960 = 20$ Byte (Remaining)

$\therefore$ 13 part 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 Fragment offset = 100

No. of byte ahead of this fragment $= 8 * 100$

$= 800$

| 100 | H |

| 800 | H |

$\frac{800}{8} = 100$ $\frac{0}{8} = 0$ | Offset

Q3 In IPv4 datagram, offset value is non zero and in MF bit is 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 recieved an IP packet of size 4404 bytes with an IP header of length 20 bytes. The value of the relevant fields in the header of the third IP fragment generated by this router for this packet are:

Ans. $\frac{2 \times 1480}{8} = \underline{\underline{370}}$

Q5. Host A send a UDP datagram containing 8880 bytes of user data to host B over Ethernet LAN. Ethernet frames may carry data upto 1500 bytes (ie. MTU = 1500 bytes). Size of UDP header is 8 bytes and size of IP 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.

AL			msg
TL	8880	8	datagram
NL	8888	20	

| 8868 | 20 | — MTU = 1500 B —

| 8 | 20 | | 1480 | 20 | . . . . . |

7   6

$$\text{Offset} = \frac{6 \times 1480}{8}$$

$$= \frac{8880}{8} = \underline{\underline{1110}}$$

Ans = 7 and 1110.

Q6. In an IPv4 datagram, M bit is 0, the value of HLEN 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. HLEN = 10

Header Size = 10*4 = 40B.

$TL = 400$

$TL = D + H$

$D = TL - H = 400 - 40 = \underline{\underline{360}}$ Byte

Fragment Offset: 300

No. of data type ahead = 8x300 = 2400

2759   2400   2399 . . . ?

| 360 | 40 | | 2400 | H |

D   H

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 byte 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.

2100 Byte — MTU = 1200B — MTU = 400B

900 + H   1200 + H

divided into 3 fragment

Total overheads = 6 × 20
= $\underline{120\text{ B}}$

Q8. Consider an IPv4 packet with a length of 4500 byte that includes a 20-byte IPv4 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 fragment offset value stored in third fragment is $\underline{144}$.

Ans.

NL | 4440 | 40 | 20 |

← 4500 →

MTU = 600 B.

576+20	576+20	576+20
3.	2	1

$$\text{Offset} = \frac{2 \times 576}{8} = \underline{144}$$

Q9. A packet has arrived in which the offset value is 100, the value of HLEN 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 HLEN = 5

No. of databyte ahead = 8 × 100 Header size = 5 × 4 = 20 Byte

TL = 100

D = TL − H = 100 − 20 = 80.

879 . . . 800 | 799 . . . 0

80	20		800	H

Offset = $\frac{800}{8}$ = 100.

Q10. In IPv4 datagram HLEN is 5 and TL = 200, then what is the position of datagram?

Ans. HLEN = 5 TL = 200

Header size = 5 × 4 = 20B. Data = TL − H

= 200 − 20

= 180 → not div by 8

∴ last fragment

Q11. Consider transport layer packet (PDU) size is 1200 Bytes, IPv4 Header size is 20 Bytes and MTU is 300 Bytes then number of IP fragments is ______.

Ans. D H

NL | 1200 | 20 | —— (MTU = 300B) ——

| 80 | 20 | | 280 | 20 | . . . 1.

5 4

No. of fragments = 5.

HW

Q12. An IP router with MTU of 1200 byte has recieved 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 recieve an IP packet containing 300 data type byte has to forword the packet to the network with maximum transmission unit of 80 byte. Assume that IP header is 10 byte long. Find the total fragment, more fragments and offset value.

Q14. Consider PDU size of transport layer packet is 2200 Bytes at source host. MTU for the network is 400 Bytes and IPv4 (header) size is 20 Bytes the no. of fragments for given PDU is <u>6</u>

Ans. NL $\boxed{2260 \mid 20}$

$+12$. $\boxed{380 \mid 20}$ $\boxed{376 \mid 20}$ ...... 1.

6 5

$\therefore$ No. of fragments = 6.

Q15. A packet has arrived with the offset value is 100 what is the number of first byte <u>800</u>

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 <u>No fragmentation</u>

MF = 0 → Last fragment / only fragment

Offset = 0 → 1^{st} fragment.

Q19. In an IPv4 datagram, M bit is one, then fragment is
Ans Both first and middle fragment.

HW

Q20. A packet has arrived with in which the offset value is 100, the value of HLEN 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 a network with below details in incoming packet header and network characteristics. MTU size as 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 packets 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 size of the incoming IP packet.

Q23. An IPv4 datagram is recieved by an IPv4 router, HL 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 800, the HLEN is 8, and the value of total length field is 500 and M bit is 0. What are the numbers of the 1st Byte and the last byte and the position of the datagram.

Date 18/5/23
Page

Header TCP

20 Byte Header fixed

16 bit								16 bit	
Source port (16 bit)								Destination Port (16 bit)	→ 4B
Sequence Number (32 bit)									→ 4B
Acknowledgement number (32 bit)									→ 4B
HL 4 bit	Reserved 6 bit	URG	ACK	PSH	RST	SYN	FIN	Window Size or (Advertisement window) (16 bit)	→ 4B
Check Sum (16 bit)								Urgent Pointer (16 bit)	→ 4B
Options (0-40 Bytes)									20 Byte

40 B. (Variable)

Min Header Size = 20 B + 0 = 20 B

Max Header Size = 20 B + 40 B = 60 B

HL (Header Length) = 4 bit $\xrightarrow{\text{Max no.}}$ 1111 = 15

Maximum Header Size = 60 Byte.

[S.F] = $\frac{60}{2}$ = 15
↓
4

Port no = 16 bit.

Range = $(0 \text{ to } 2^{16}-1)$ = 0 to 65,535

0 → 1023 { Well Known port no. Assigned & controlled by IANA

	Port No.
SMTP	→ 25
HTTP	→ 80
FTP	{ 20, 21
DNS	→ 53

0 → 49,151 { Reserved or Registered Port No. Not assigned and controlled by IANA only registered with IANA.

49,152 → 65,535 { Dynamic Port number. Neither Controlled nor registered with IANA.

<u>Source port address</u>: This is a 16 bit field that defines the port number of the application program in the host that is sending the segment.

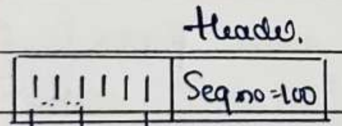
<u>Destination port address</u>: This is a 16 bit field that defines the port number of the application program in the host that is recieving the segment.

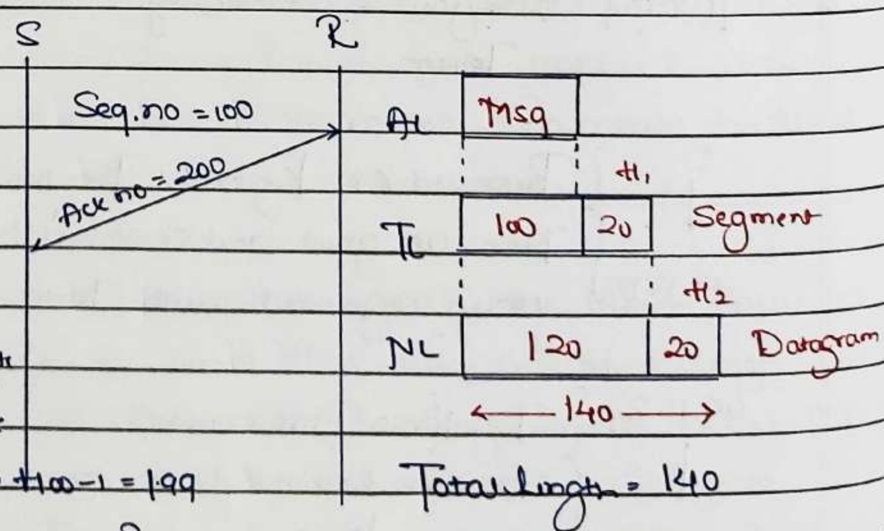
<u>Sequence number</u>: This is 32 bit field that defines the sequence number of the first data byte.

<u>Note</u>: * TCP is a byte stream protocol i.e every byte is associated with one sequence number.

* IP is a packet stream protocol ie every packet is associated with one sequence number.

<u>Acknoledgement Number</u>: This is a 32 bit field defines the sequence number of the next expected byte. If the reciever has recieved successfully the byte number 'x' from other party it returns the acknoledgement number 'x+1' back to the sender.

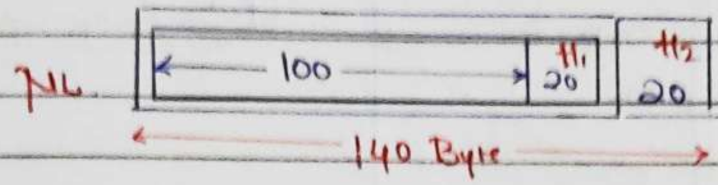




* 1st byte Seq.no = 100
* Total.L at NL = 140 Byte
* D.L at TL = 100 Byte
* Last B. seq no = 100 + 100 − 1 = 199

∴ Acknoledgement no = 200.

OR



→ Data Size at TL
= Total Length (IP) − IP(H)
− TCP(H)

Q1. HL = 10
Total length = 1000 } IP

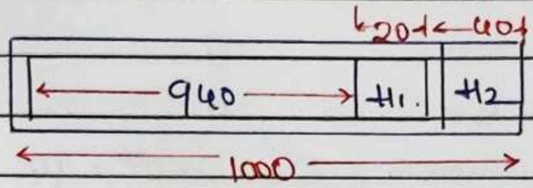
Seq. No.
HL = 5 } TCP

Ack no = ?

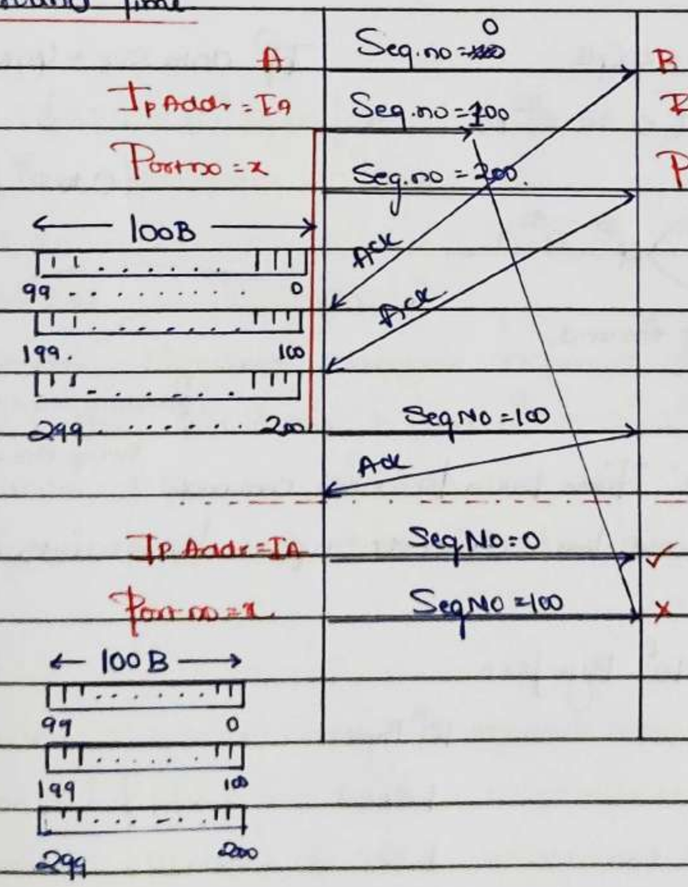
Data Size at TL = 940
1st Byte Seq No = 100
Last byte Sequence no = 100 + 940 − 1
= 1039.

Ack no = 1040.

Sol :

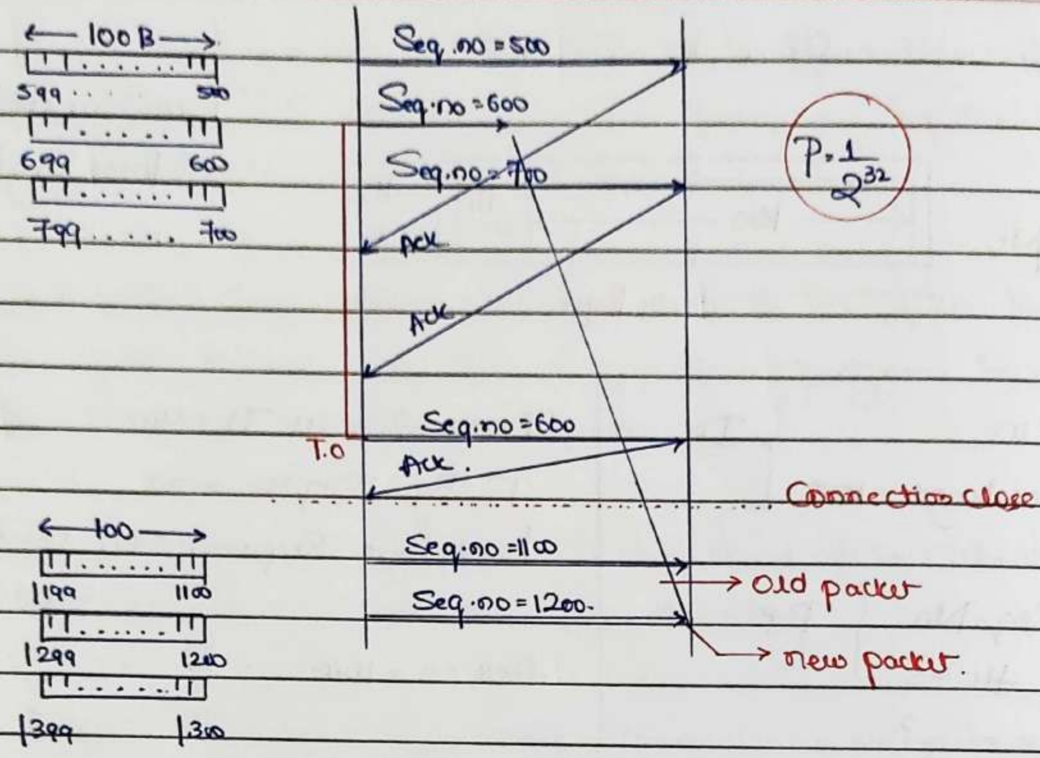


Wrap Around Time



Connection Close

Note: TCP suggest that do not start the Sequence number with 0. Always choose any random Sequence number initially.



$P = \frac{1}{2^{32}}$

Sequence No = 32 bit

Total Sequence number $= 2^{32} = 2^{2} \times 2^{30} = 4G$ Sequence number

data Size = 4GB

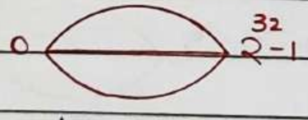
If dataSize > 4GB.

Seq no $= 2^{32}$ (0 to $2^{32}-1$)

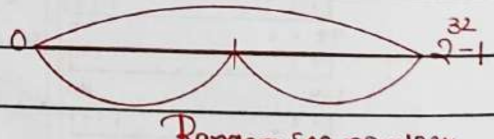
If data Size = 4GB + 4GB

↓ ↓

0 to $2^{32}-1$ 0 to $2^{32}-1$



Wrap Around.



Random Seq.no = 1024

Wrap Around.

Wrap Around time: Time taken to wrap around.

Note: Wrap around time depends upon bandwidth.

① $B = 1$ MBPS $= 10^6$ Byte/sec

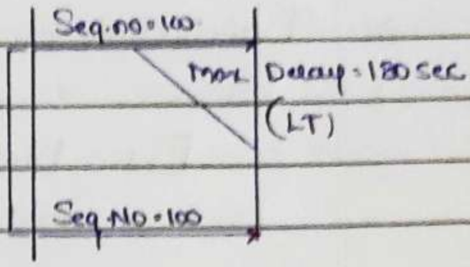
1 sec → 10^6 Byte

10^6 Byte → 1 sec

10^6 Seq.No → 1 sec

1 Seq.No → $\frac{1}{10^6}$ sec

2^{32} Seq. No $\longrightarrow$ $\frac{2^{32}}{10^{6}}$ Sec.



WAT = 4294.96 sec.

WAT > LT No problem.

$$\left[WAT = \frac{\text{total seq. no}}{\text{(Bandwidth) Byte/sec.}} \right]$$

(2) B = 1GBPS = 10^9 Byte/sec

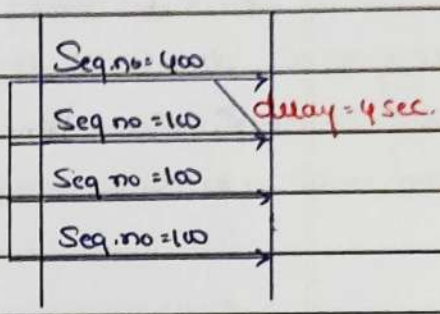
10^9 Byte $\longrightarrow$ 1 Sec.

10^9 Seq No $\longrightarrow$ 1 sec

1 Seq. No. $\longrightarrow$ $\frac{1}{10^9}$ sec

2^{32} Seq. No. $\longrightarrow$ $\frac{2^{32}}{10^9}$ sec

W.A.T = 4.294 sec.



WAT < LT

Problem.

(Lifetime = 180 sec)

\#. B = 1GBPS = 10^9 Bytes/sec, LT = 180 sec.

1 sec $\longrightarrow$ 10^9 Byte

1 sec $\longrightarrow$ 10^9 Seq. no

180 sec $\longrightarrow$ 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 = $\lceil \log_2 180 \times 10^9 \rceil = 38$ bit

$\lceil \log_2 LT \times B \rceil$

Note:

1. Minimum sequence number required to avoid wrap around time within life time = LT × B.
2. Minimum number of bits required in the sequence number field to avoid wrap around time in the life time = $\lceil \log_2 LT \times B \rceil$

3. Bandwidth must be in Byte/sec.

Extra bits = 38 − 32 = 6 bits

$\boxed{\text{Option}}$ → Time Stamp = 6 bits

Range = 0 to $2^6 - 1$

= 0 to 63.

Time Stamp = 6 bits

1^{st} Set time stamp value = 000000 → 0

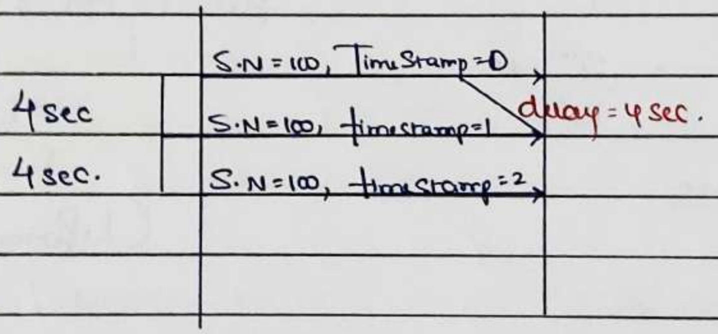
2^{nd} Set time stamp value = 000001 → 1

⋮

64^{th} Set time stamp value = 111111 → 63.

$\frac{2^{\cancel{38}} \text{ seq.no}}{2^{\cancel{32}} \text{ seq.No}} = 2^6 = 64 \text{ sets}$

$2^{32} \times 64 = 2^{32} \times 2^6 = 2^{38}$
↓
Sets.



Q1. Consider 200 Mbps network with a sequence number field 28 bits. The wrap around time of sequence number is.

Ans

$B = 200 \text{ Mbps} = 200 \times 10^6$ bits/sec

$B = \frac{200 \times 10^6}{8}$ Byte/sec $= 25 \times 10^6$ Byte/sec

25×10^6 Byte → 1 sec

25×10^6 Seq.No → 1 sec

1 seq No → $\frac{1}{25 \times 10^6}$ sec

2^{28} Seq No. → $\frac{2^{28}}{25 \times 10^6}$ sec = 10.73

W.A.T = 10.73 sec.

Shortcut:

$\text{WAT} = \frac{\text{total Seq.no}}{[\text{Bandwidth}] \text{ Byte/sec}}$

$\text{WAT} = \frac{2^{28}}{25 \times 10^6}$ sec

WAT = 10.73 sec

classmate
Date
Page

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 $B = 1\text{Gbps} = 10^9 \text{bits/sec}$

$WAT = \dfrac{\text{total seq. no}}{(\text{Bandwidth}) \text{ Byte/sec}} = \dfrac{2^{32}}{\frac{10^9}{8}} = \dfrac{8\times2^{32}}{10^9} = 34.35$

$\therefore$ 34 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 MSL is ______

Ans. $B = 10^9 \text{ bits/sec}$, $L_T = 60 \text{ sec}$

$B = \frac{10^9}{8}$ Byte/sec.

Min. no of bits required to avoid WAT within lifetime

$= \lceil \log_2 L_T \times B \rceil = \lceil \log_2 60 \times \frac{10^9}{8} \rceil = \lceil \log_2 7.5\times10^9 \rceil = \lceil 32.8 \rceil$

$= 33$ bits

Q5. Suppose you are asked to design a new reliable byte-stream transport protocol like TCP. This protocol named myTCP, runs over a 100 Mbps network with RTT of 150 ms 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. $B = 100 \text{ Mbps} = 100\times10^6 \text{ bits/sec}$, $L_T = 2\text{min} = 120 \text{ sec}$

$\frac{100\times10^6}{8}$ Byte/sec $= 12.5\times10^6$ byte/sec

Min seq. no to avoid wrap around time within the lifetime

$= L_T \times B = 120\times12.5\times10^6$

$= 1500\times10^8$

Minimum no. of bits required in the sequence length field $= \lceil \log_2 15\times10^8 \rceil$

$= \lceil 30.32 \rceil = 31$ bits

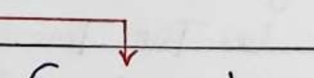
Important Points about TCP:

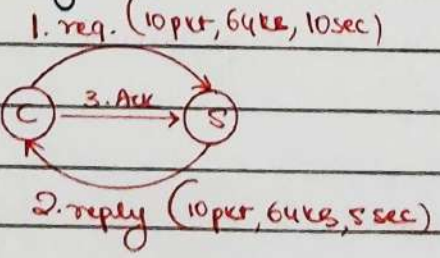
1. TCP is a connection oriented and reliable protocol (TCP has both flow and error control mechanism).
2. It is a virtual connection and not physical i.e segments of TCP may follow different paths, some of them may be lost or duplicated or arrive out of order. Segments are encapsulated in IP datagram
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 direction.
6. TCP uses sliding window protocol for it's flow control (GBN & SR)
7. Each TCP connection have 4 window.

Communication

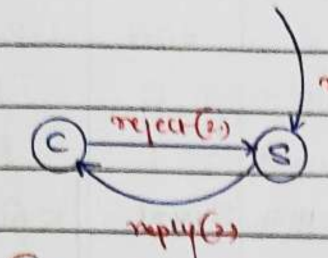
Connection oriented → Connection establishment → 3 way Handshake

Connection less →



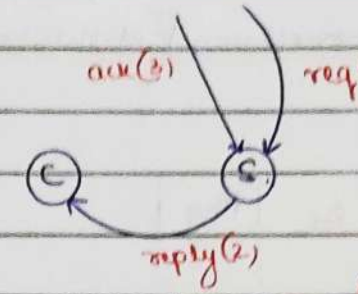


(1.)



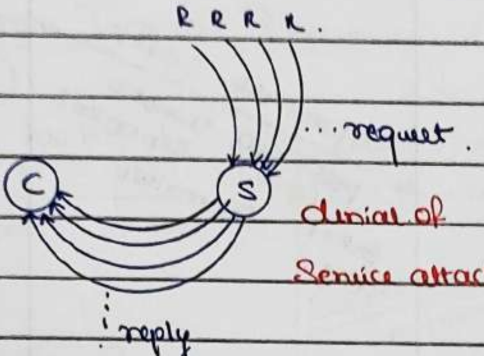
Connection not established.

(2.)

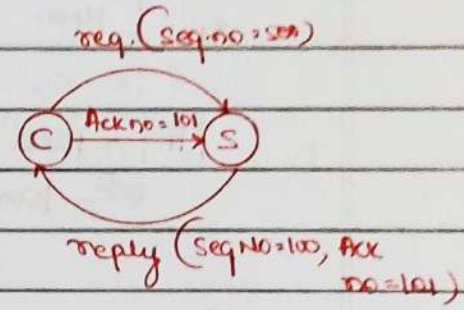


Connection established.

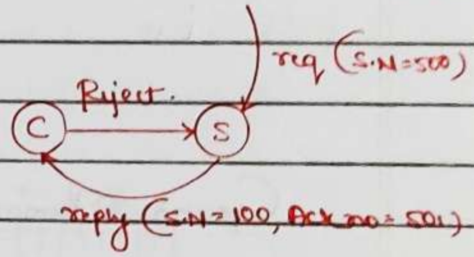
(3.)



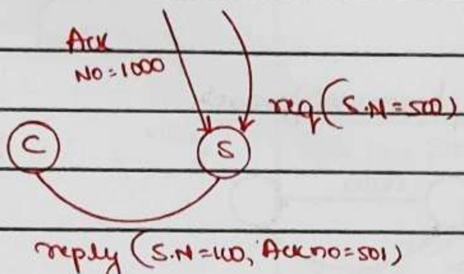
denial of Service attack



1>



2>



Connection not established.

Note: Sequence number and Ack no are also used for authentication purpose.

Flags

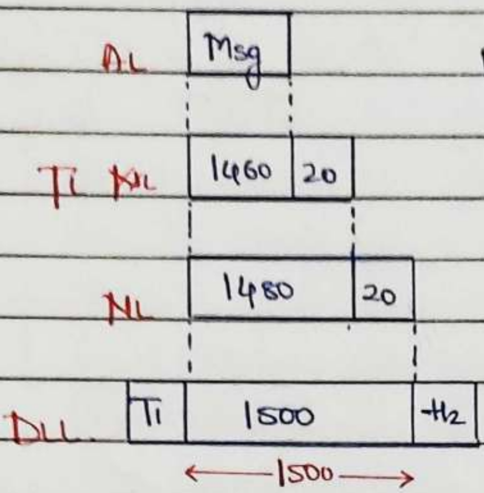
URG → Urgent Flag
ACK → Acknowledgement Flag
PSH → Push flag
RST → Reset Flag
SYN → Synchronization Flag
FIN → Finished Flag.

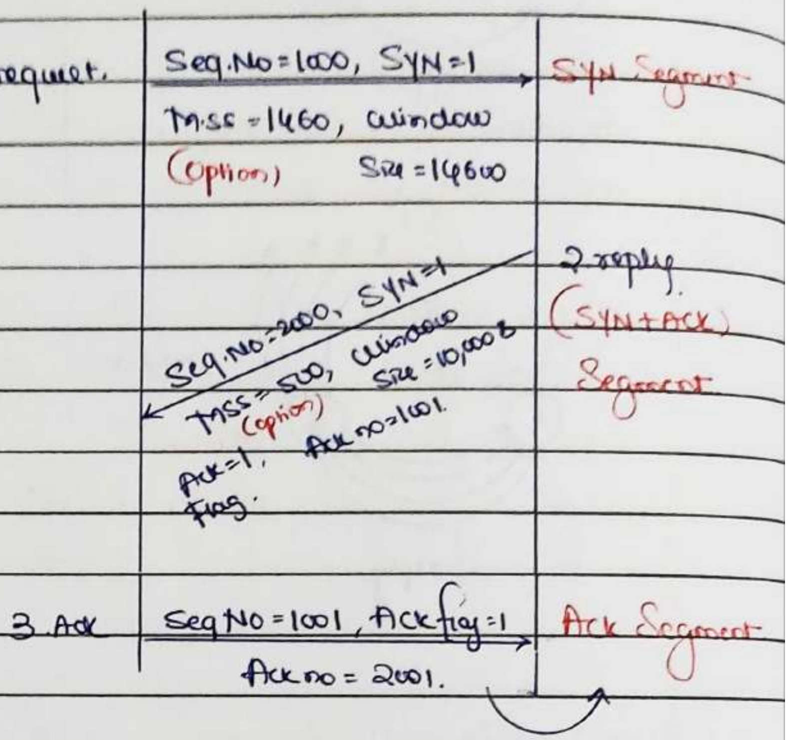
* SYN and ACK are used in Connection est. Phase.

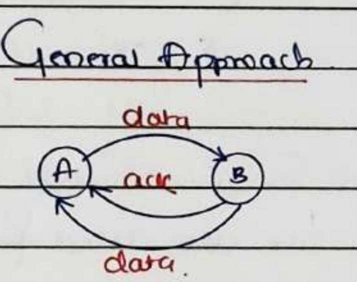
Phases of TCP Connection.

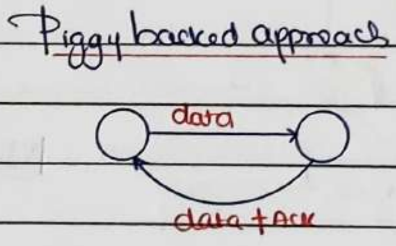
1. Connection establishment phase
2. Data transfer phase
3. Connection termination phase.

Connection Establishment Phase









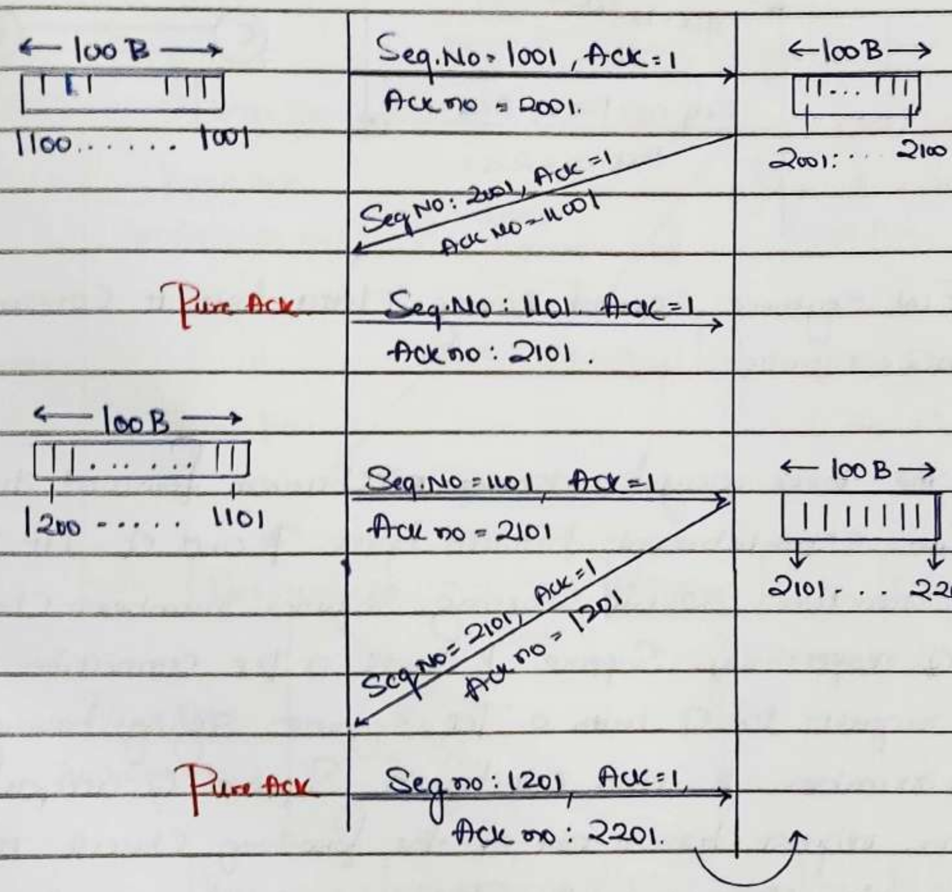
SYN = 1	Consume one Sequence number.
FIN = 1	Consume one Sequence number.
ACK = 1	Consume No sequence number.
1 DataByte	Consume One Sequence number.

Note:

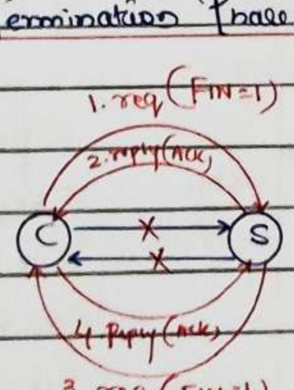
1. A SYN Segment Cannot Carry data, but it consume One Sequence number.
2. A SYN+ACK Segment Cannot Carry data, but it cons. one Sequence number.
3. An Ack Segment if carry no Data then it will not consume Sequence number.

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.

classmate

Date

Page

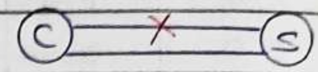
C | Seq.no = 1201, FIN = 1 → | S

req. | ACK = 1, Ack No = 2201

reply (Ack)

← Seq No = 2201, ACK = 1

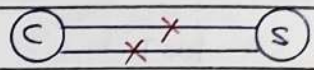
Ack No = 1202.



request.

← Seq.No = 2201, FIN = 1

ACK = 1, Ack no. = 1202



reply (Ack) | Seq.no = 1202, ACK = 1 →

Ack.no = 2202.

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 | | Q

request | Seq.no = x, SYN = 1, ACK = 0 → |

| ← Seq no = Y, SYN = 1, ACK = 1, Ack No = x+1, FIN = 0 | reply.

SYN bit = 1,

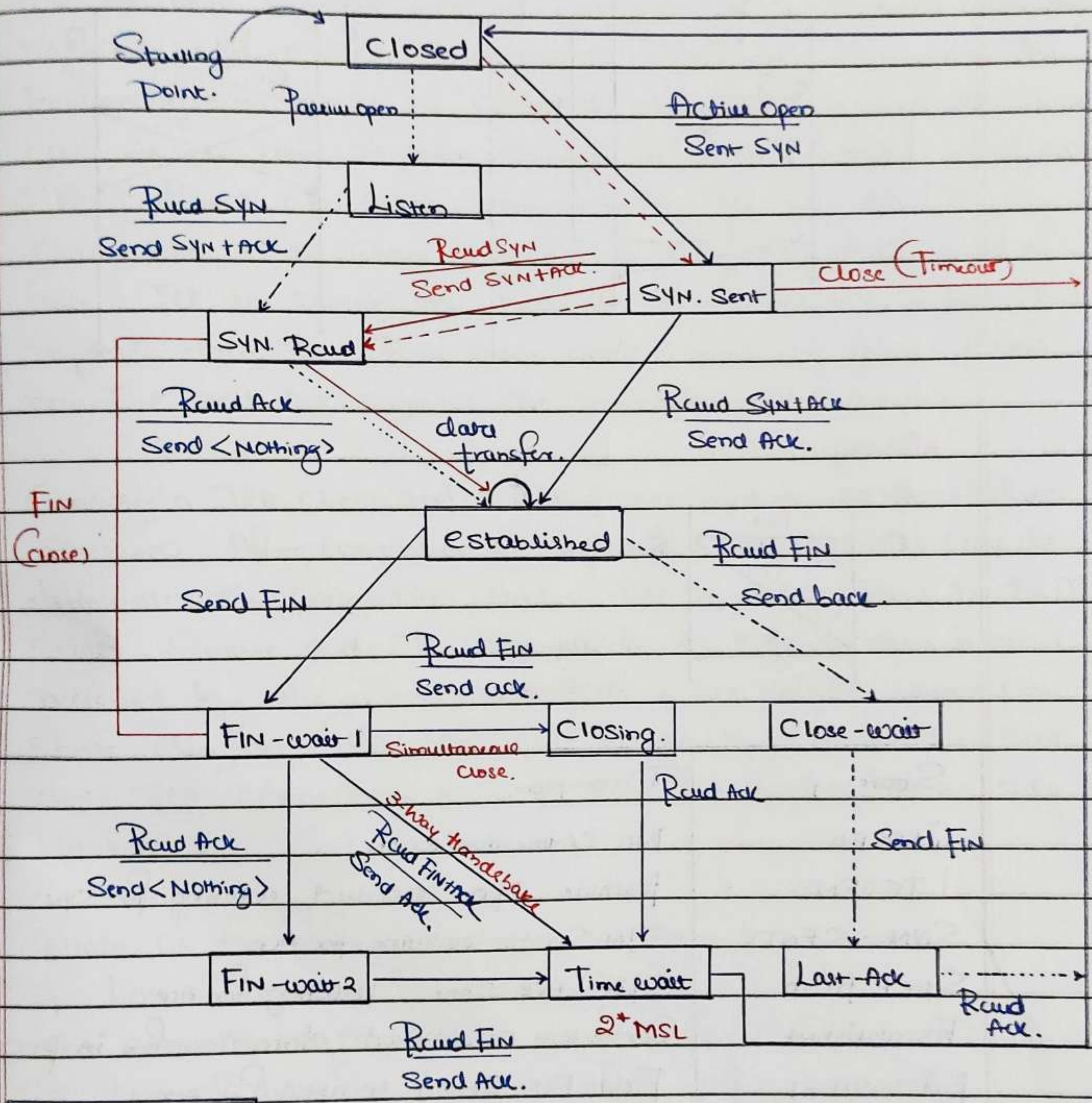
SEQ number = Y,

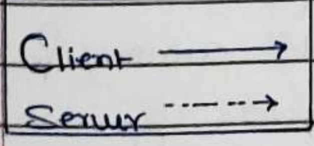
Ack bit = 1.

Ack number = x+1

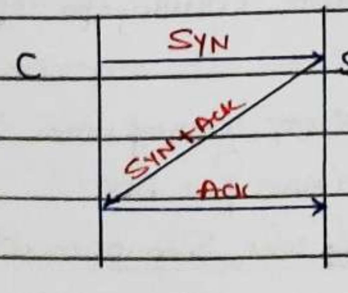
FIN bit = 0

TCP : State Transition Diagram

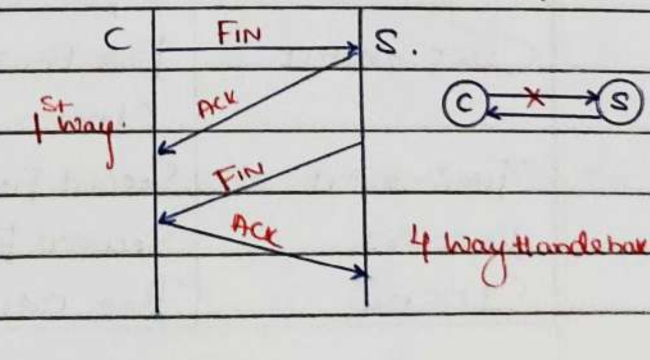




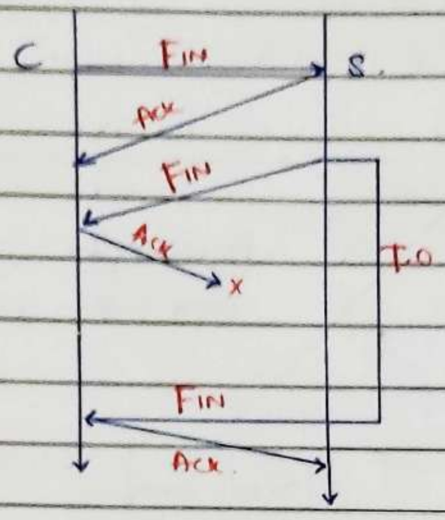
Conn. establishment.



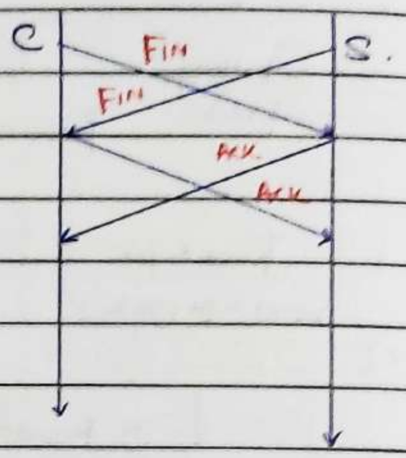
Connection termination.



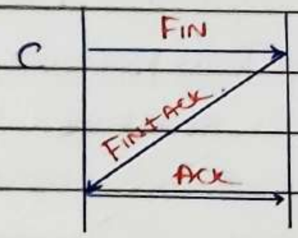
4 way Handshake



Connection termination
2nd way.



Connection termination.
3rd way



3-way
Handshake.

State	Description.
CLOSED	No connection exists
LISTEN	Passive open recieved, 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 recieved; waiting for second FIN
CLOSE-WAIT	First FIN recieved, ACK Sent; waiting for application to Close
TIME-WAIT	Second FIN recieved, ACK Sent, waiting 2MSL time out
LAST ACK	Second FIN sent; waiting for ACK
CLOSING.	Both sides decide to Close Simultaneously

Time wait Timer

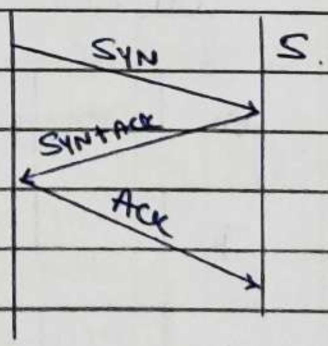
The time wait timer (2MSL) is used during connection termination. The maximum segment life time (MSL) is the amount of time any segment can exist in the network before being discarded. The implementation needs to choose a value for MSL. Common values are 30 sec, 1 min or even 2 min. The 2MSL timer is used when TCP performs an Active close and send the final ACK. The connection must stay open for 2 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 recieved by the client side TCP. As per the TCP connection state diagram (RFC ~~973~~ 793). 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?

S_1: Loss of SYN+ACK from server will not establish a connection.



S_2: Loss of ACK from the client cannot establish the connection.

S_3: The server moves LISTEN→SYN-RCVD → SYN-SENT → Established in the state machine on no packet loss.

S_4: The server moves from LISTEN → SYN-RCVD → established in the state machine on no packet loss.

Ans. S_1 and S_4 are True

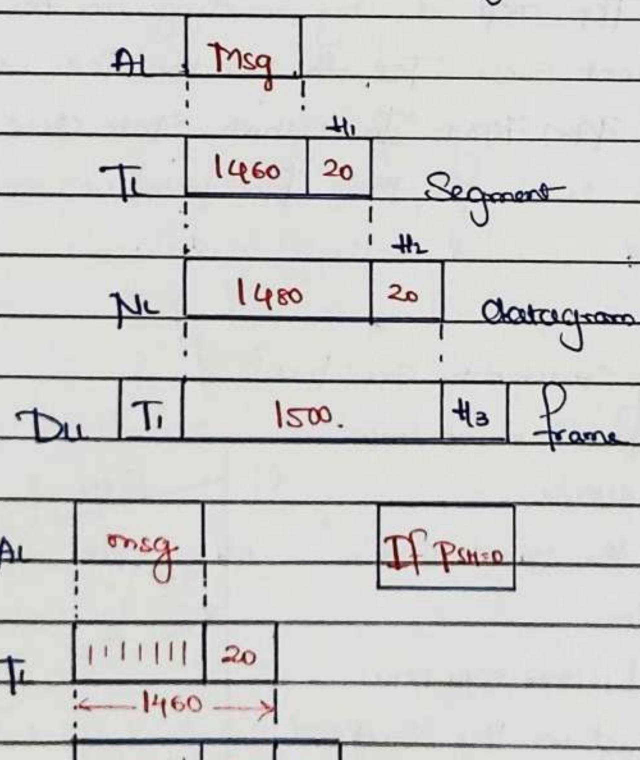
Q2. Consider a TCP server is in close wait State in TCP state transition diagram, which State TCP Server moves after Sending FIN segment to TCP client?

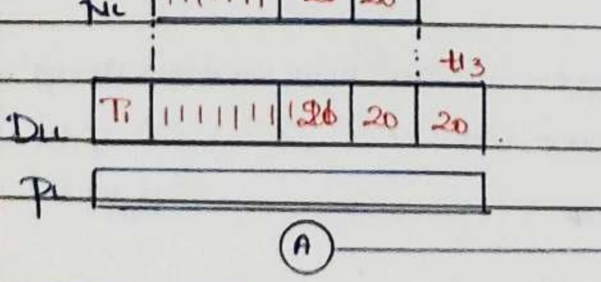
Ans. LAST-ACK.

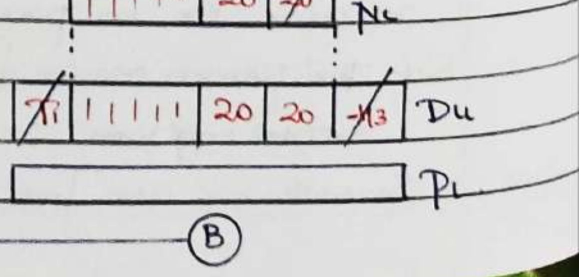
Flags.

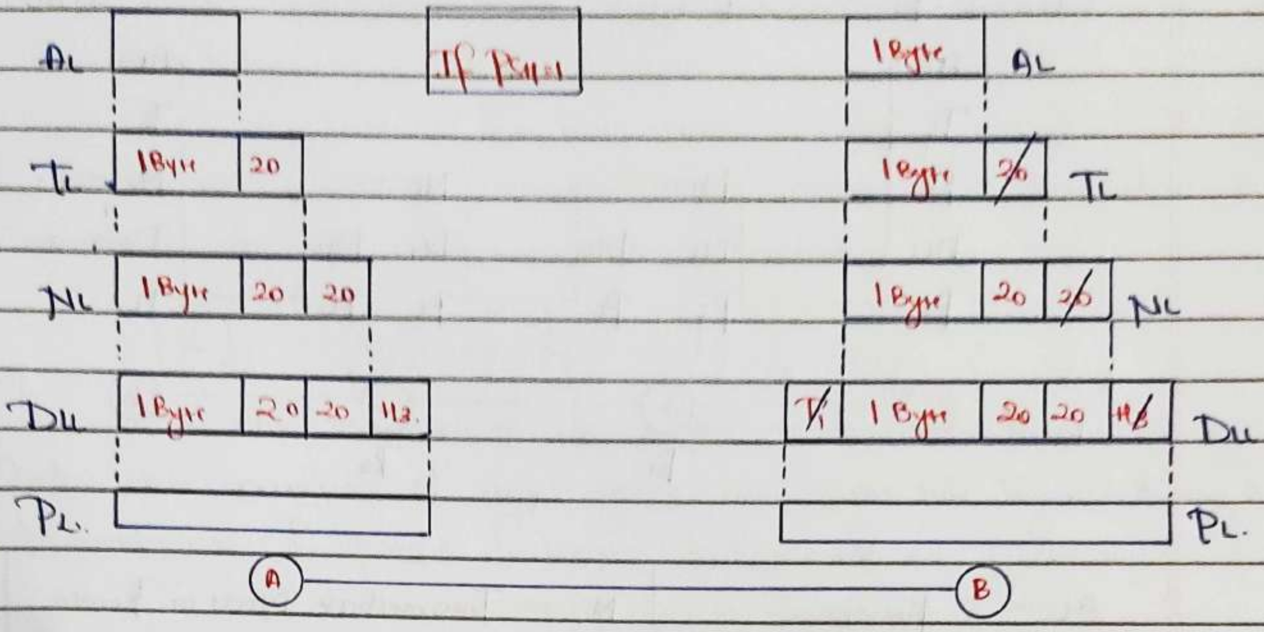
1. SYN } Connection establishment phase
2. ACK
3. FIN } connection termination phase
4. URG
5. PSH
6. RST

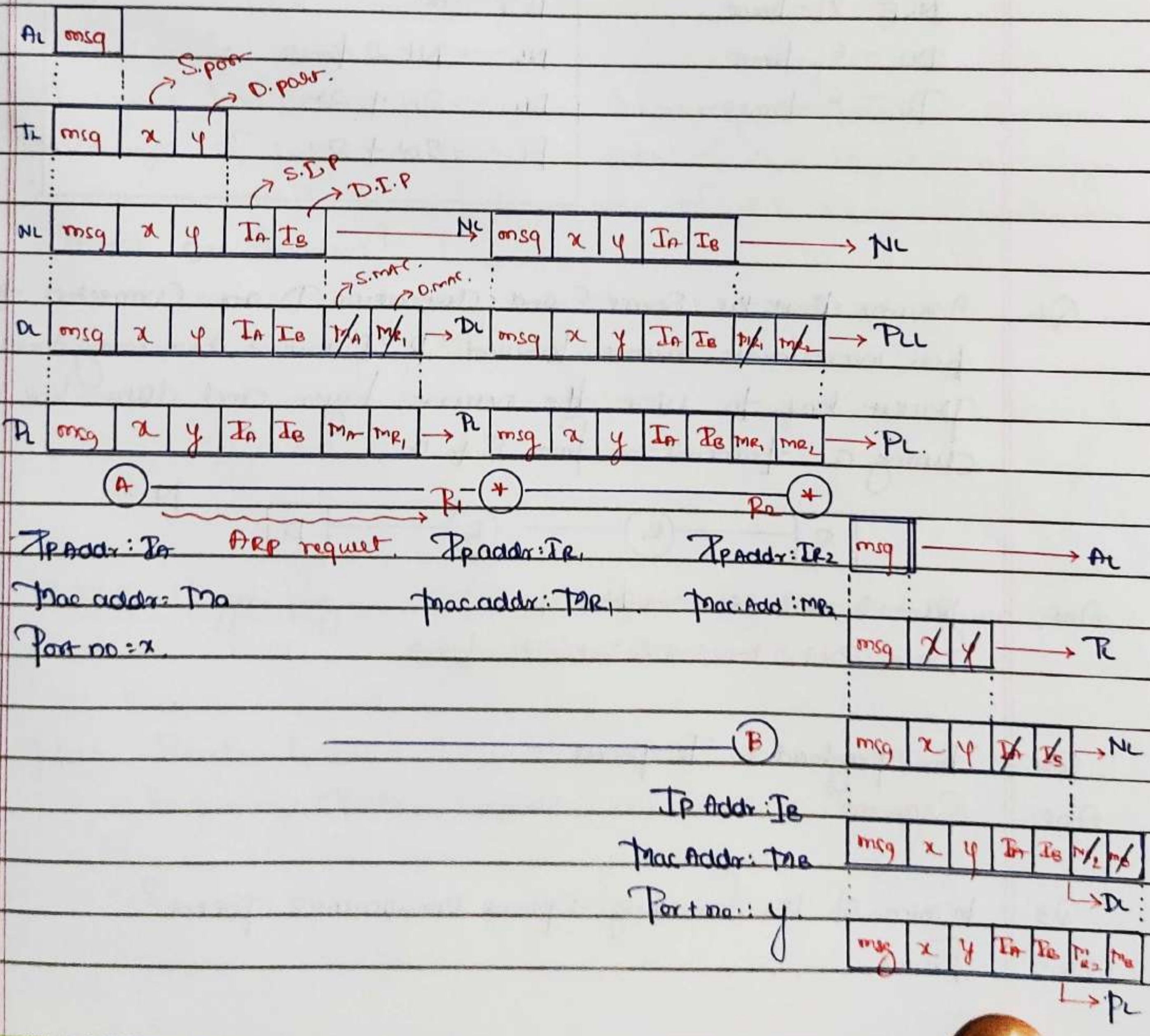
Push Flag: Push flag (PSH) is used to indicate that data should not be buffered it must be pushed immediately to the lower layer or upper layer.

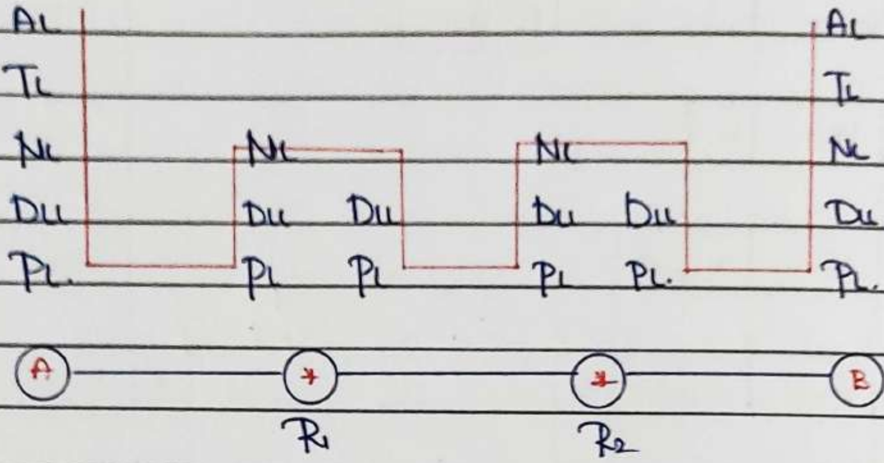







AL
TL
NL
DLL
PL
1 Byte
20
20
113
A
B

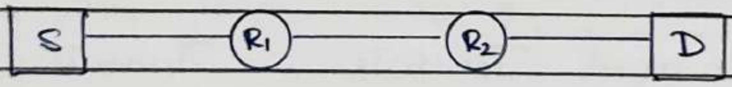

AL msg
S.port
D.port
TL msg x y
S.I.P
D.I.P
NL msg x y I_A I_B
NL msg x y I_A I_B
S.MAC
D.MAC
DL msg x y I_A I_B M_A M_{R_1}
DL msg x y I_A I_B M_{R_1} M_{R_2}
PLL
PL msg x y I_A I_B M_A M_{R_1}
PL msg x y I_A I_B M_{R_1} M_{R_2}
A
R_1
R_2
ARP request
IP Addr: I_A
Mac addr: M_A
Port no: x
IP addr: I_{R_1}
mac addr: M_{R_1}
IP Addr: I_{R_2}
Mac Add: M_{R_2}
msg
AL
msg x y
TL
B
msg x y I_A I_B
NL
IP Addr: I_B
Mac Addr: M_B
Port no: y
msg x y I_A I_B M_{R_2} M_B
DL
msg x y I_A I_B M_{R_2} M_B
PL



AL – 2 times
TL – 2 times
NL – 4 times
DLL – 6 times
PL – 6 times

N → Intermediate Node or Router
AL → 2x
TL → 2x
NL → N+2 times
DLL → 2N + 2x
PL. → 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. NL = N+2 times = 2+2=4 times
DLL = 2N+2 times = 2*2+2=6. times

Q2. The payload in IP 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.

Q6. Consider the following Scenario where Source and destination are connected via three intermediate Router.

S — R_1 — R_2 — R_3 — D

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

NL – $N+2 = 3+2 = 5$ (P)

DL – $2N+2 = 6+2 = 8$ (Q) $\therefore P+Q = \underline{13}$.

Q7. 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 byte

Header size = h Byte, 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.

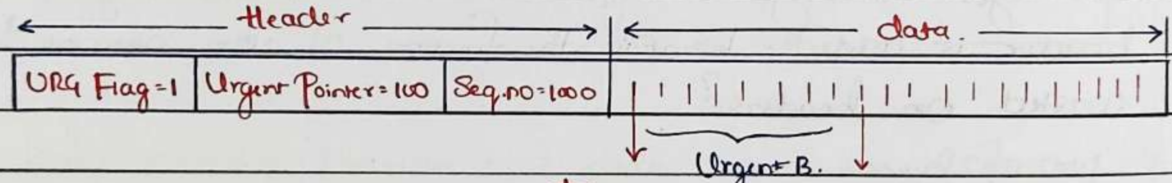
→ If URG Flag = 0, then we have no need to read the urgent pointer.

→ 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 where 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.



First urgent Byte ↓ Seq no = 1000.

last urgent Byte ↓ Seq. no = 1100.

Note:
If urgent pointer = x
then no. of urgent bytes = $x+1$.

Q. If size of TCP segment is 1KB and header length value is 6, the 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 Byte
HLEN = 6
Header size = 6×4 = 24 Byte.

Data size = 1024 − 24 = 1000 Byte
Seq no = 3500
URG flag = 1

Urgent Pointer = 45
No. of Urgent byte = 45+1 = 46.

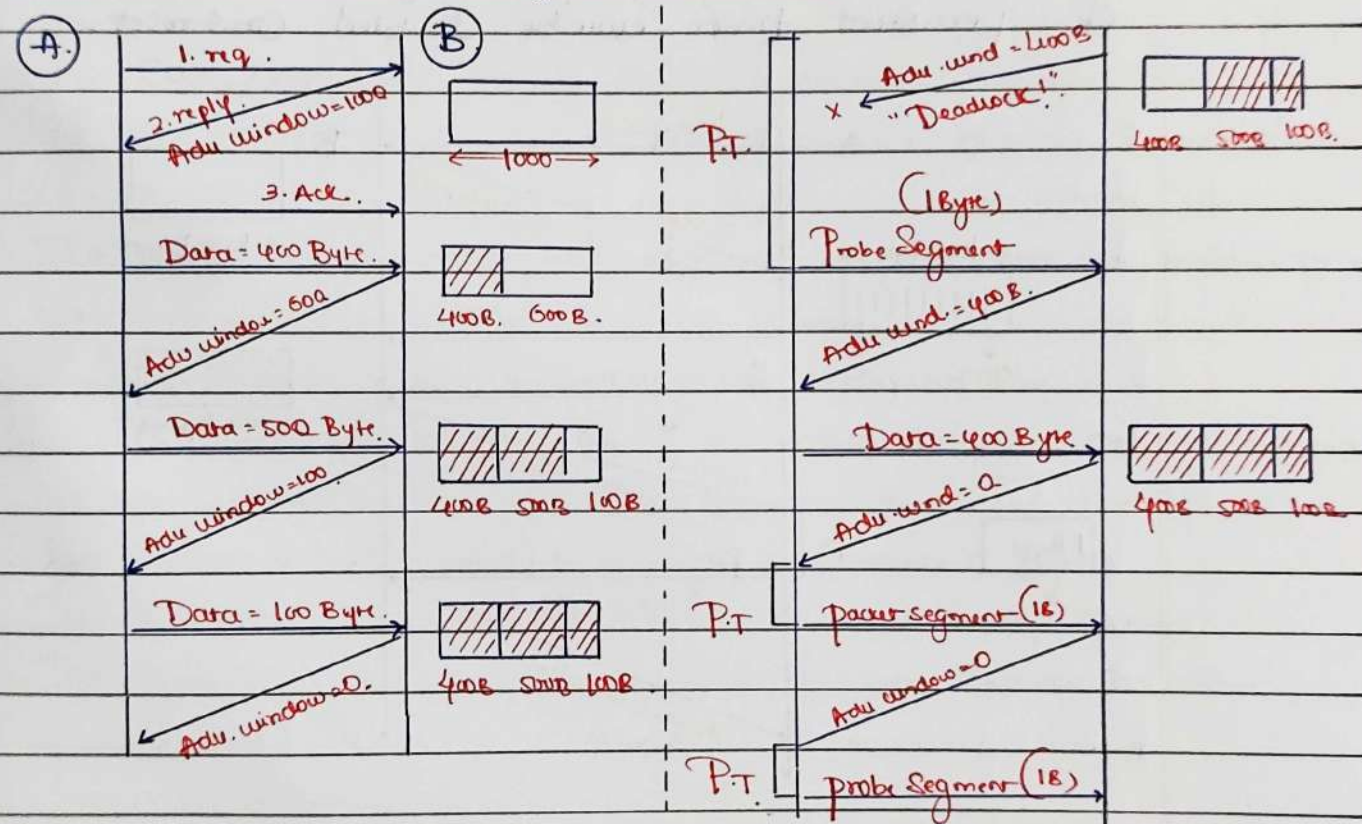
Last urgent byte sequence no
= 3500+45 = 3545.

Urgent Bytes = $\underbrace{3500 - 3545}_{46 \text{ urgent bytes}}$

∴ 1000 Byte, 46 Byte, Sequence no = 3500-3545.

Flow Control In TCP

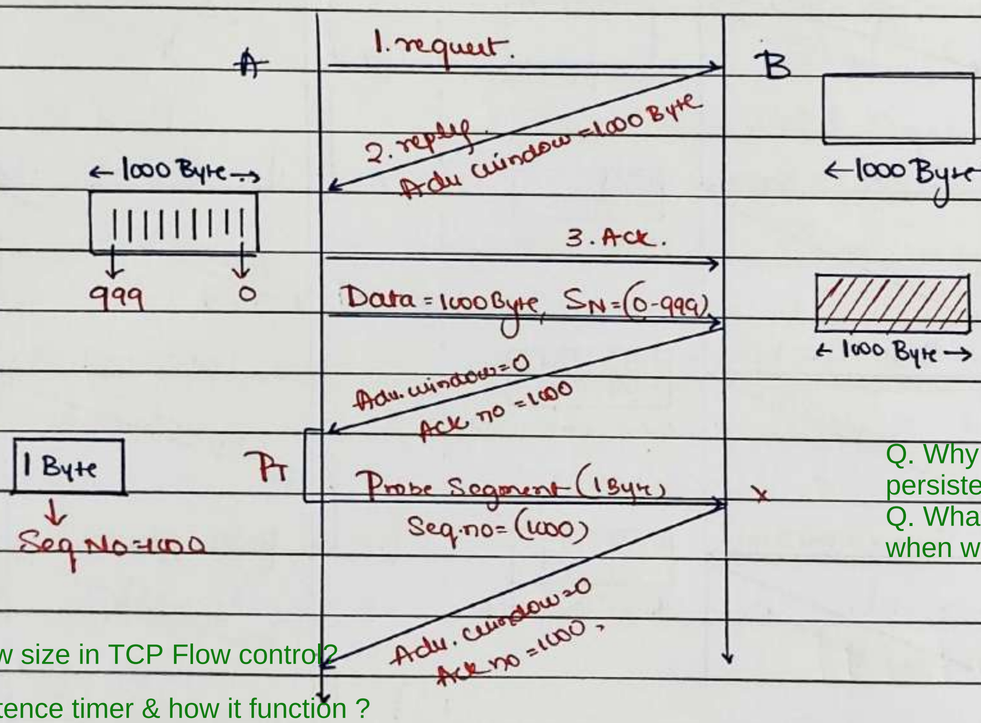
Window size or Advertising window (16 bit) [used for flow control]



Persistent Timer.

* Whenever reciever announce that my recieving 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 recieve an acknowledgement with a window size zero, it Start a Persistent timer.
* When the Persistent timer goes off, the Sender Send a special segment called as Probe segment.

* This segment contain only one Byte of data. It has a Sequence number, but it's sequence number is never acknoledged.
* It is even ignored in calculating the sequence number for the rest of the data
* Probe segment alerts the recieving TCP 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 recieved from the reciever, another Probe segment is sent and the value of persistent timer will be doubled and reset.



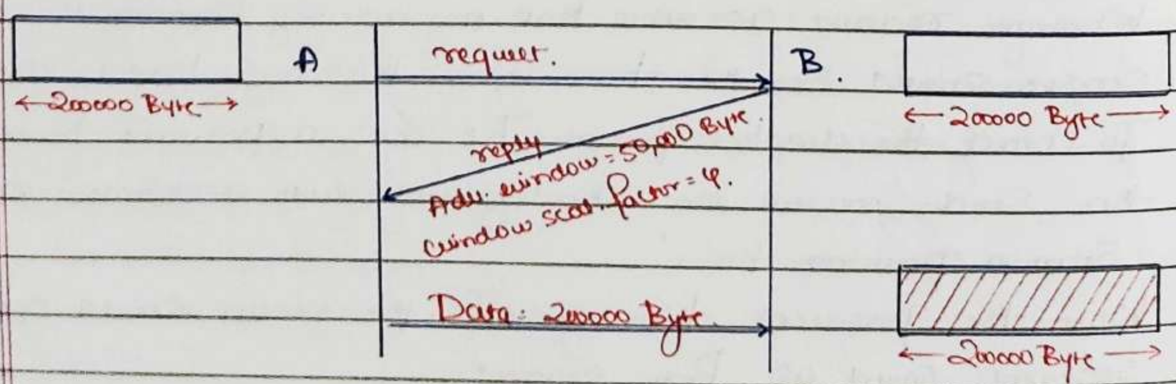
Q. Why we are using persistence timer ?
Q. What side effect occurs, when we use frequent PT?

Q. What is window size in TCP Flow control?

Q. What is Persistence timer & how it function ?

Window Size = 16 bit.

Maximum no = $2^{16} - 1 = 65,535$



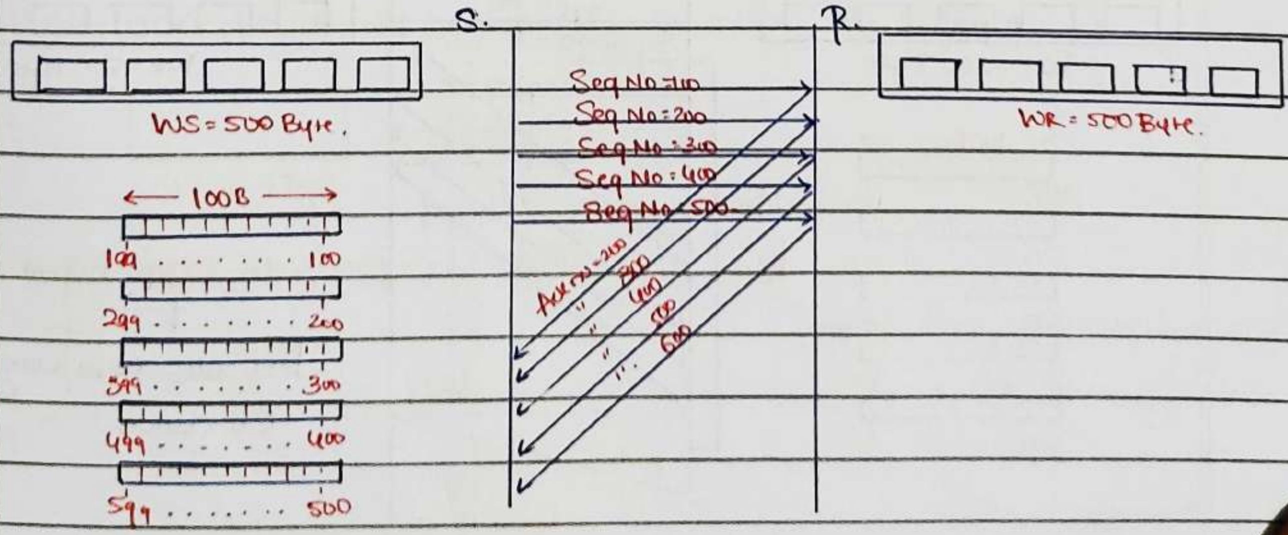
Note: According to RFC-1312 the maximum window size by using the window scale option = 2^{30} Byte = 1 GB.

$$= \underbrace{2^{16}}_{\text{window size}} \times \underbrace{2^{14}}_{\text{window scaling factor (option)}} = 2^{30}.$$

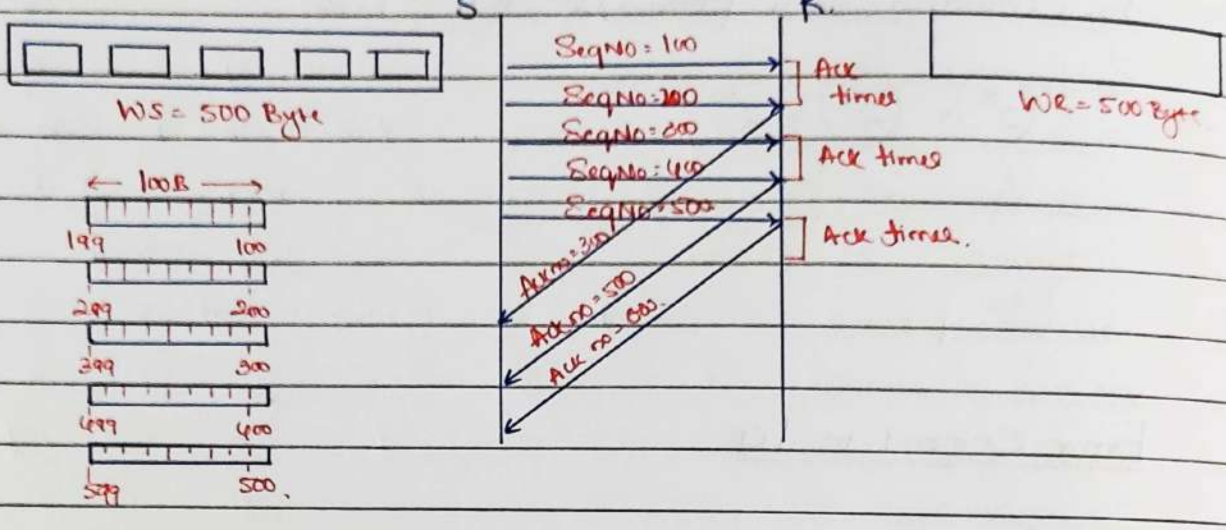
Error Control in TCP:

* TCP can use both Selective and Cumulative acknowledgement.
* Reciever may choose to send independent ACK or Cumulative ACK.
* TCP uses a combination of Selective repeat and Go-back-N protocol protocol for error control and flow control
* In TCP Sender window size = reciever window size
* In TCP out of order packets are accepted by the reciever. Whenever reciever recieves 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 gurantee that data are delivered to process in order.

Selective Acknowledgement / Independent Ack



Cumulative Acknowledgement.



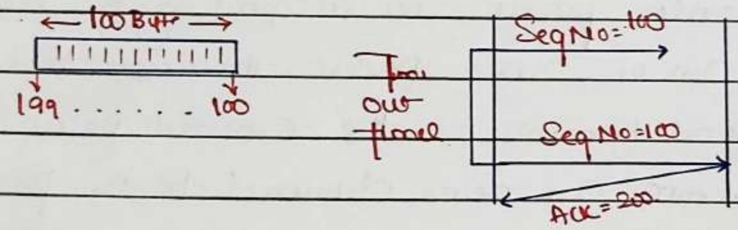
Retransmission in TCP

(i) Retransmission after timeout timer

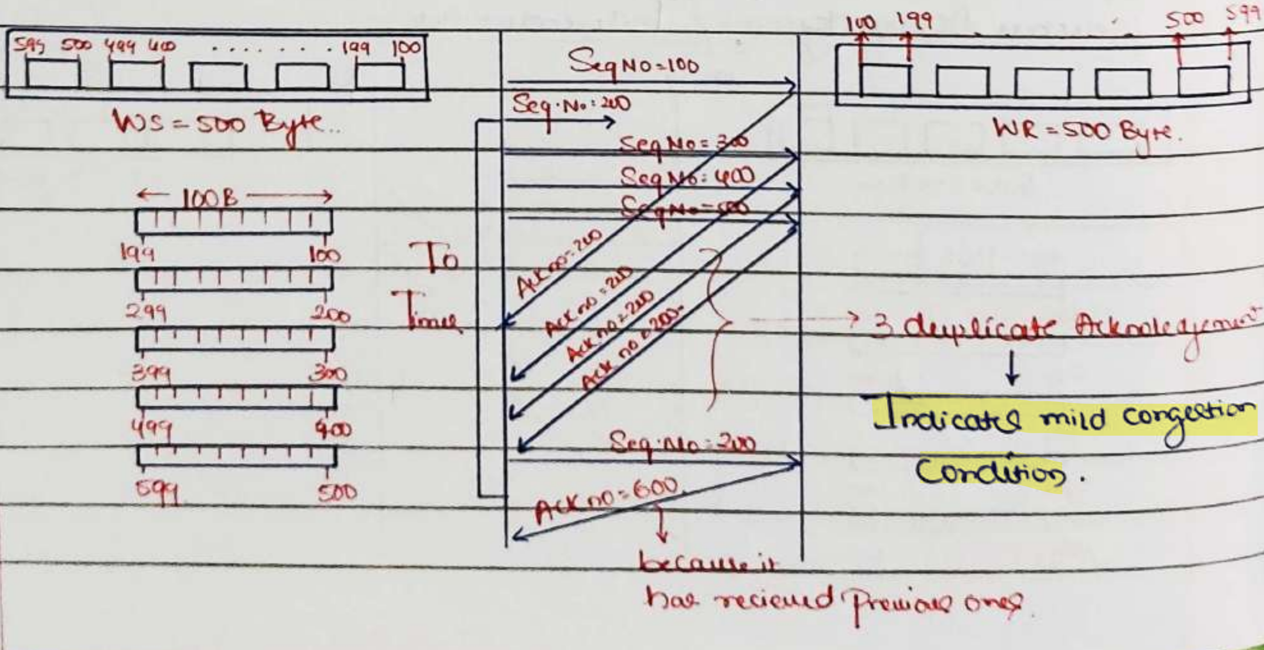
(ii) Retransmission after 3-duplicate acknowledgement.

Q. What is the benefit of 3-duplicate ACK & what is indicate?

Retransmission After TO timer



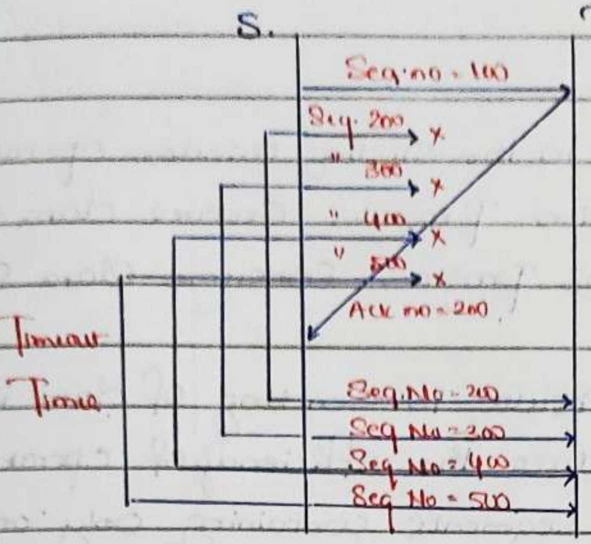
Retransmission after 3-duplicate acknowledgement [Fast Retransmission]



→ 3 duplicate Acknowledgement

↓

Indicates mild congestion Condition.



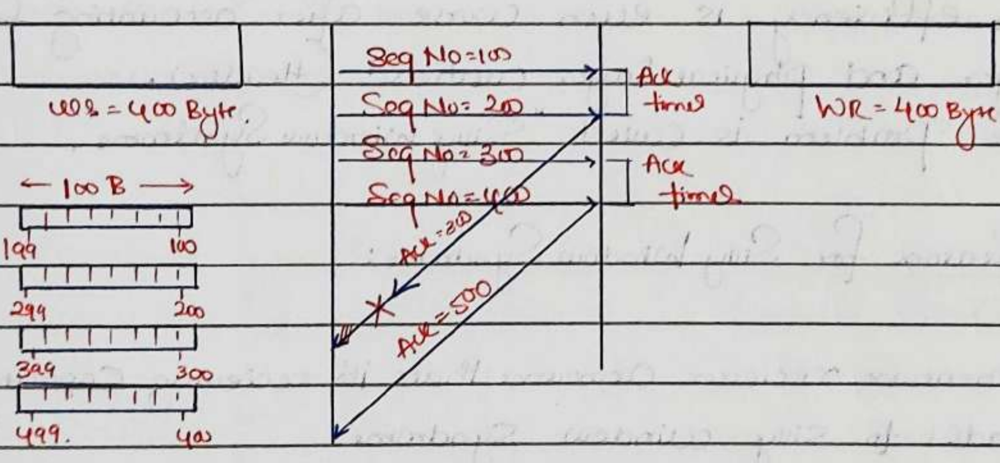
Note:

(i) If 3 duplicate acknoledgment not Possible then we use timeout timer concept for retransmitting the lost packet.

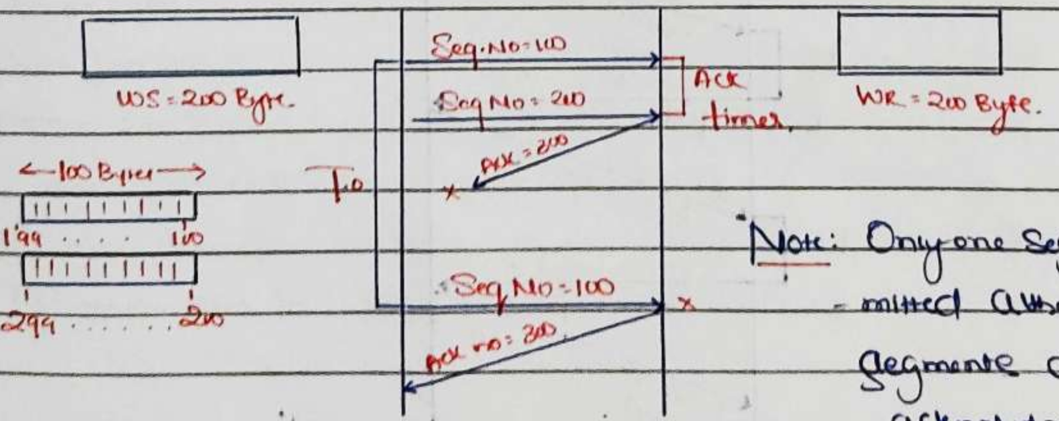
(ii). Timeout timer indicates severe Congestion Condition.

Lost Acknoledgement : 1. Automatically Corrected lost Ack
2. Lost Ack Corrected by resending Segment.

① Automatically Corrected Lost Ack.



② Lost acknoledgement Corrected by resending the Segment.



Note: Only one Segment is retransmitted although two segments are not acknoledgement.

when sender receive retransmitted ack, it knows that both segment are safe & sound because ACK is cumulative.

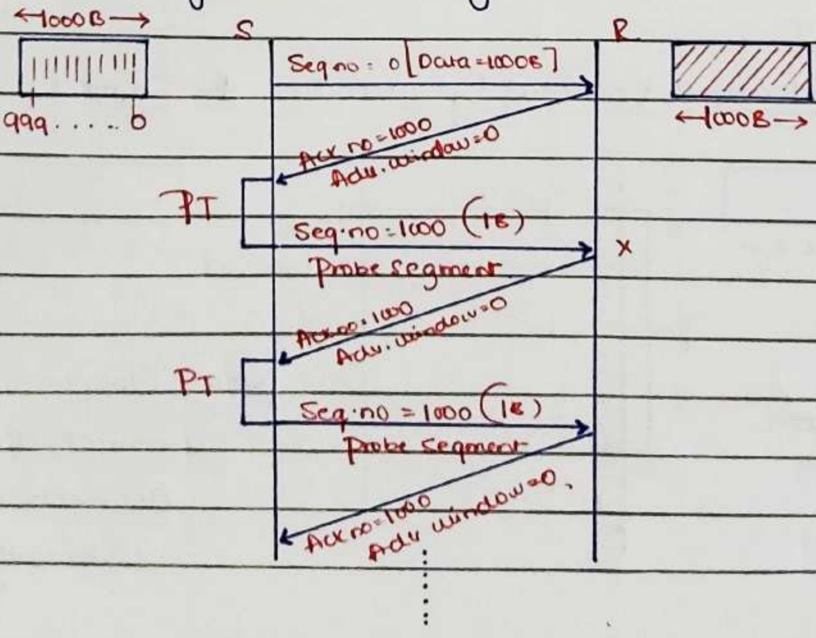
Date 16/6/23

Silly Window Syndrome:

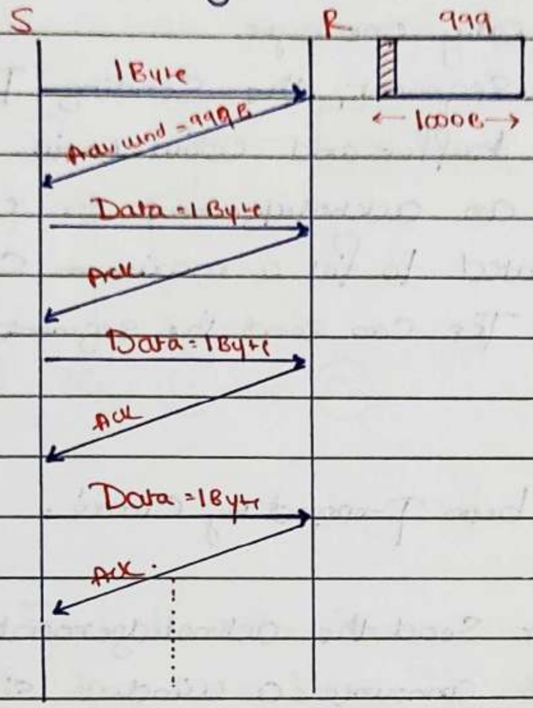
* A Serious problem can arise in the sliding window operation when either the Sending application program creates data slowly or the recieving application program consume data slowly or both.
* Any of these situations results in sending of data in very small segments, which reduce the efficiency of operation.
* 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 indicates that we are using the capacity of network very inefficiently.
* The efficiency is even worse after accounting for the datalink layer and physical layer overhead (Header).
* This problem is called "Silly window Syndrome".

Reasons for Silly Window Syndrome:

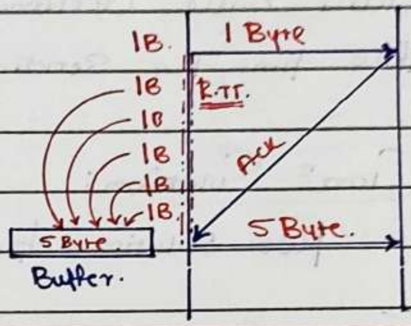
1. Whenever reciever announce that its recieving capacity is zero it leads to silly window syndrome.



(2) Whenever Sender Produce only one byte at a time it leads to Silly window Syndrome.

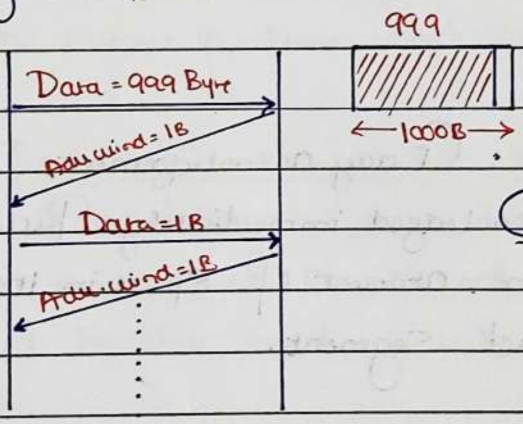


Nagle's Algorithm



$\boxed{\text{If data size in 1 RTT > MSS.}}$

(3) Whenever reciever consume only one byte at a time, it leads to Silly window Syndrome.



Clark's Solution:

$\frac{1}{2}$ Buffer empty.

Or

1 MSS

eg::	
1 Byte/sec	1 Byte/sec
RTT = 100 sec	RTT = 100 sec
MSS = 200 Byte	MSS = 50 Byte
In one RTT = 100 Byte	In one RTT = 100 Byte
So we transfer 100 Byte.	So we transfer 50 Byte
→ If data size In 1 RTT < MSS.	→ data size in one RTT > MSS

Nagle's Algorithm:

1. The Sending TCP send first piece of data it recieve 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 recieving TCP sends an acknoledgement or until enough data have accumulated to fill a maximum Size Segments. At this time the Sending TCP can send the segment.

Clark's Solution:

Two solutions has been proposed by Clark.

First Solution: Reciever Send the acknoledgement as soon as the data arrive, but to announce a window size of zero until either there is a enough space to accomodate a segment of maximum Size or until atleast half of the reciever buffer is empty.

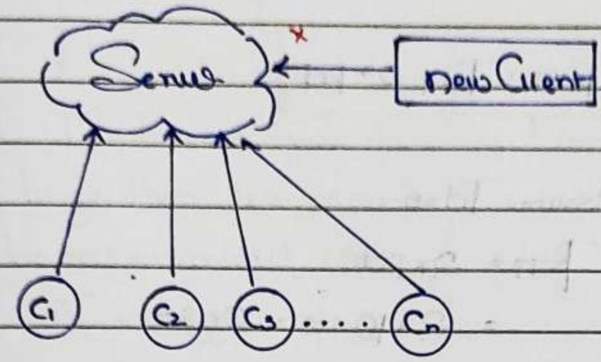
Second Solution: (Delay acknoledgement) When a segment arrives, it is not acknoledged immediately. Reciever wait until ~~it is~~ there is decent amount of space in it's buffer before acknoledging the arrived segment.

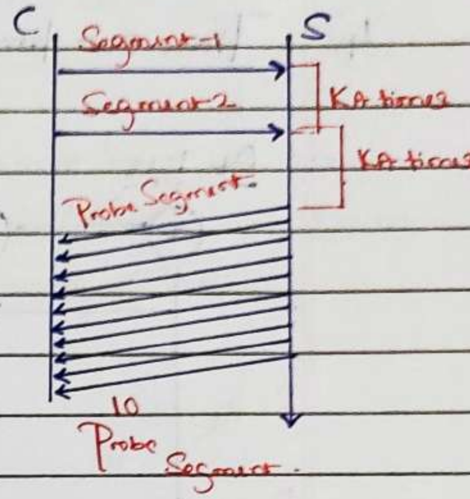
TCP Timer management

1. Keep alive timer
2. Persistant timer
3. Acknoledgment timer
4. Time wait timer
5. Time out timer.

Date 19/6/23
Page

(1.) Keep alive timer : It is used to keep track of ideal connection. Server will close the connection if client does not send any data for a fixed amount of time.





Note:

Each time the Server recieve the packet from a client, it reset the keep alive timer. If the server does not recieved packet from the client and keep alive timer expired, it send a probe segment, if there is no response from it after 10 probes, it assume that the client is down and terminates the connection.

(2) Acknoledgement Timer: Whenever reciever recieve a segment. It will start a timer called 'acknoledgement timer.' Whenever Ack timer goes off the reciever send one acknoledgement for all the segment recieved in this timer, also known as 'cumulative acknoledgement.'

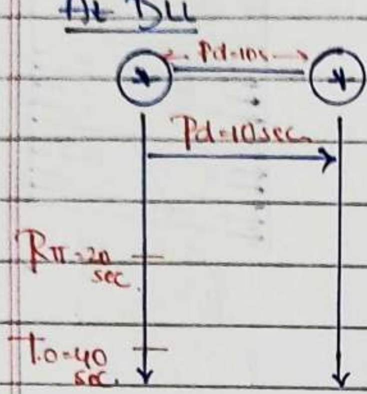
(3.) Time Wait Timer: The time wait timer (2MSL) is used during connection termination. The maximum segment life time is the amount of time any segment can exist in the Network before being discarded. The implementation needs to choose a value for MSL. Common value are 30sec, 1min or even 2min. The 2MSL timer is used when TCP performs an Active close and send 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 RTO timer at the other end times out and new FIN and Ack segment are resent.

(4.) Time out timer :

$$\boxed{RTT = Td + 2 * pd}$$

At DLL



- Assume $Td = 0$

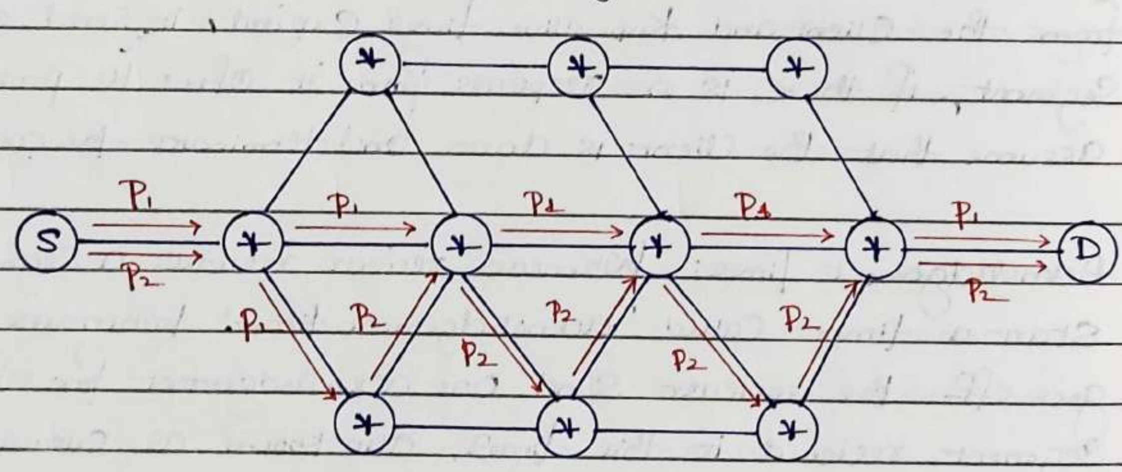
$\rightarrow RTT = 2 \times pd$

$= 2 \times 10\ sec = \underline{20\ sec}$

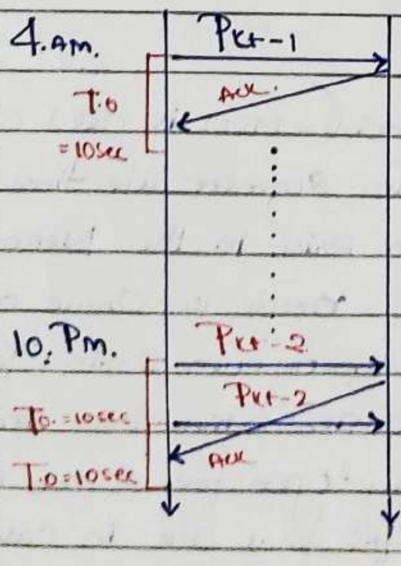
$\rightarrow TO = 2 * RTT$

$= 2 \times 20 = \underline{40\ sec.}$

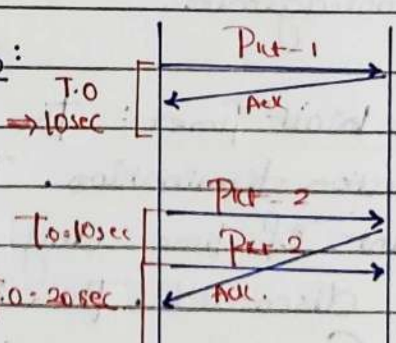
Timeout timer of Transport Layer.



eg:

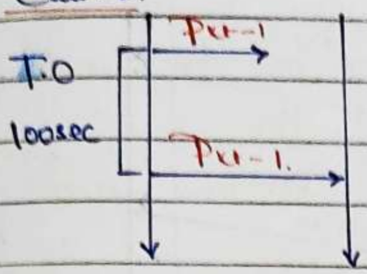


Solution:

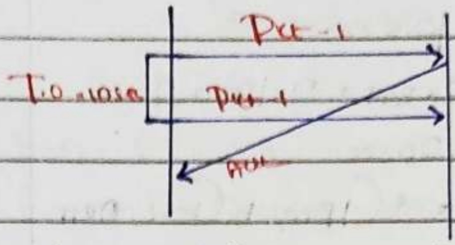


$\rightarrow$ Sol^n : If traffic increases then increase the timeout time.

Case : I.



Case : II.



Note: If timeout timer is very large then lost packet will be retransmitted late. eg: After 100 sec.

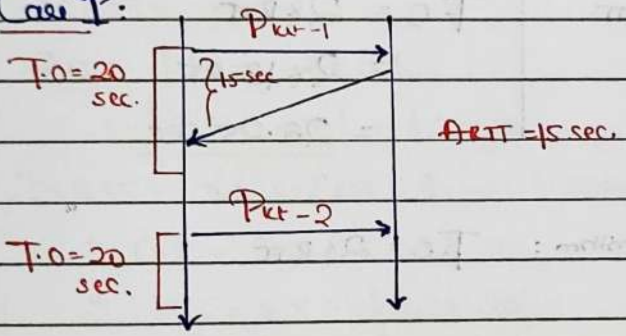
Note: If timeout timer is very small then unnecessarily packet will be retransmitted.

→ 1. RTT = 10 sec (Assumption)

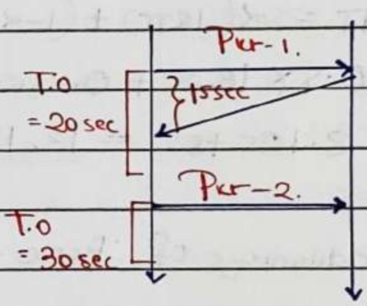
T.O = 2 * RTT

T.O = 2 * 10 sec = 20 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 a high traffic in the network.

Basic Algorithm.

$$\boxed{NRTT = \alpha(IRTT) + (1-\alpha)ARTT}$$

$0 \le \alpha \le 1$, $\alpha = \frac{1}{2} = 0.5$.

Packet-1.

I RTT = 10 sec

T.O = 2·RTT = 2×10 = 20 sec

ARTT = 15 sec

NRTT = α(IRTT) + (1-α) ARTT

= 0.5×10 + 0.5×15

= 12.5 sec

Pkt-2

$IRTT = 12.5\ sec$

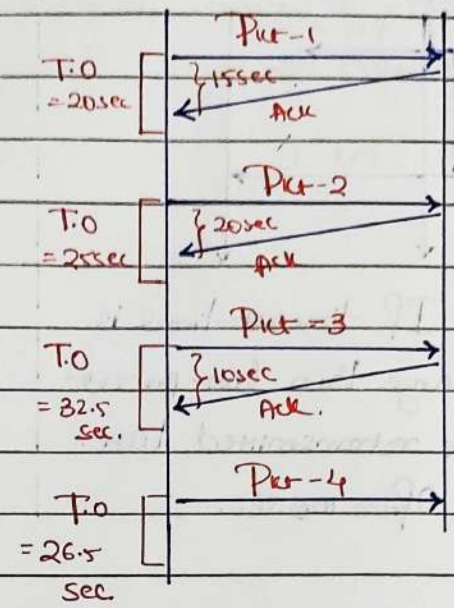
$T.O = 2 \times RTT = 2 \times 12.5 = 25 sec$

$ARTT = 20 sec$

$NRTT = \alpha(IRTT) + (1-\alpha) ARTT$

$= 0.5 \times 12.5 + 0.5 \times 20$

$= 6.25 + 10 = \underline{16.25}$



Packet-3

$IRTT = 16.25 sec$

$T.O = 2 \times RTT = 2 \times 16.25 = 32.5 sec$

$ARTT = 10 sec$

$NRTT = \alpha(IRTT) + (1-\alpha) ARTT$

$= 0.5 \times 16.25 + 0.5 \times 10$

$= 8.125 + 5 = \underline{13.125}$

Packet-4

$IRTT = 13.125$

$T.O = 2 \times RTT$

$= 2 \times 13.25$

$= \underline{26.25 sec}$

* Disadvantage of Basic Algorithm: $T.O = 2 \times RTT$

Jacobson's Algorithm

$\boxed{T.O = 4 \times I.D + R.T.T}$

Packet-1

$IRTT = 10 sec, ID = 5$

$\alpha = \frac{1}{2} = 0.5$

$T.O = 4 \times ID + RTT$

$= 4 \times 5 + 10 = 30 sec$

$ARTT = 20 sec.$

$AD = |IRTT - ARTT|$

$= |10-20| = 10.$

$NRTT = \alpha(IRTT) + (1-\alpha) ARTT$

$= 0.5 \times 10 + 0.5 \times 20$

$= 5 + 10 = 15 sec$

$ND = \alpha(ID) + (1-\alpha) AD$

$= 0.5 \times 5 + 0.5 \times 10 = 7.5$

Packet 2

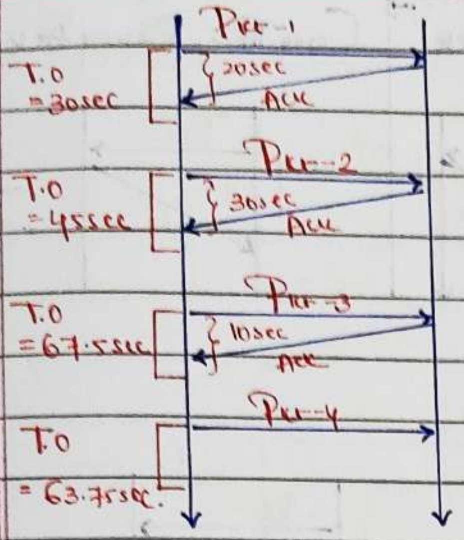
$IRTT = 15 sec$

$ID = 7.5 sec$

$T.O = 4 \times ID + RTT = 4 \times 7.5 + 15 = 45 sec$

$ARTT = 30 sec$

$AD = |IRTT - ARTT| = |15-30| = \underline{15}.$



$NRTT = \alpha(IRTT) + (1-\alpha)ARTT$

$= \cancel{\ldots} \; 0.5 \times 15 + 0.5 \times 30$

$= 22.5$ sec

$ND = \alpha(ID) + (1-\alpha)AD$

$= 0.5 \times 7.5 + 0.5 \times 15 = \underline{11.25 \text{ sec}}$

Packet 3

$IRTT =$

$ID = 11.25$

$T.O = 4 \times ID + RTT$

$= 4 \times 11.25 + 22.5$

$= 45 + 22.5 = 67.5$

$ARTT = 10$ sec.

$AD = |IRTT - ARTT|$

$= |22.5 - 10| = 12.5$ sec.

$NRTT = \alpha(1 - IRTT) + (1-\alpha)ARTT$

$= 0.5 \times 22.5 + 0.5 \times 10$

$= 11.25 + 5 = 16.25$ sec

$ND = \alpha(ID) + (1-\alpha)AD$

$= 0.5 \times 11.25 + 0.5 \times 12.5$

$= 5.625 + 6.25 = 11.875$

Packet 4

$IRTT = 16.25$

$ID = 11.875$

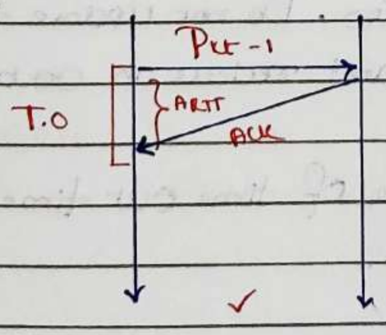
$T.O = 4 \times ID + RTT$

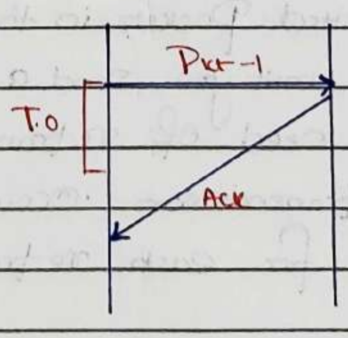
$= 4 \times 11.875 + 16.25$

$= 47.5 + 16.25$

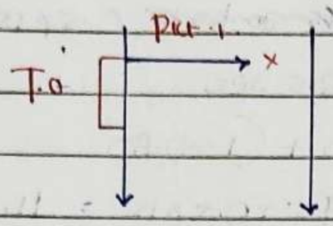
$T.O = \underline{63.75}$

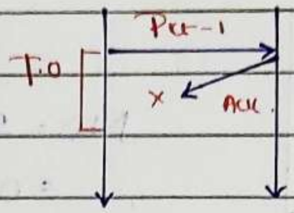
Problem in Basic and Jacobson's Algorithm

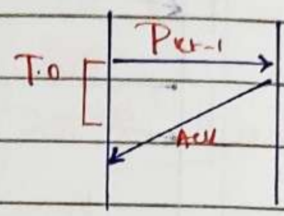




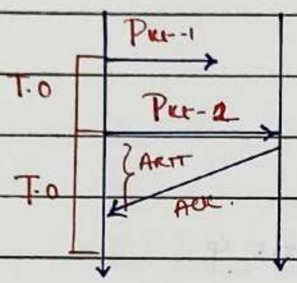
Case I: Lost data Packet. | Case II: Lost Ack | Case III: Delay Ack.

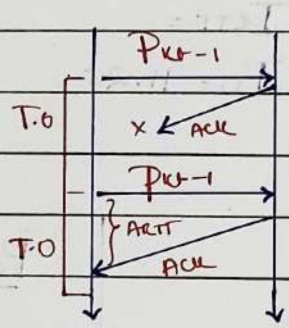


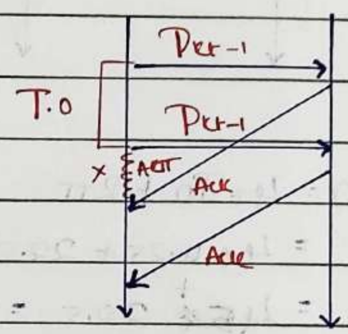




Solutions:







Note:

If there is a time out timer then there is a possibility to recieve two acknoledgement.

(i) from original packet

(ii) from retransmitted Packet.

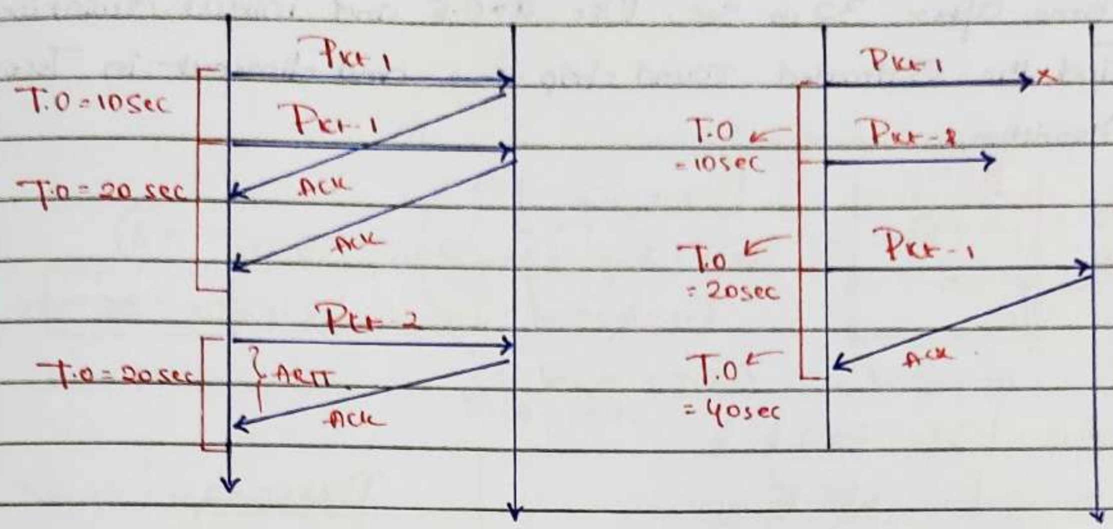
Then there is an ambiguity that which acknoledgement must be considered for next Calculation and what must be the time out timer for retransmitted packet. Therefore Karn's has solved this problem by Proposing the following strategy:

Karn's Modification:

Do not considere the round trip time of a retransmitted Packet in the Calculation. Do not update the value of RTT until you send a Segment and recieve an acknoledgment without need of retransmission.

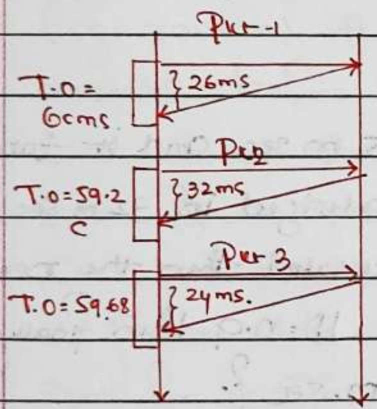
If retransmission occurs value of time out timer is doubled for each retransmission.

Case III Solution (According to Karn's Algorithm).



Q 1. If the TCP round-trip time, RTT, is currently 30msec 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

RTT = 30ms

T.O = 2×RTT = 60ms

ARTT = 26msec

NRTT = α(IRTT) + (1−α) ARTT

= 0.9×30 + 0.1×26

= $\underline{29.6ms}$

Packet 2

IRTT = 29.6 msec

T.O = 2×RTT = 59.2msec

ARTT = 32 msec

NRTT = α(IRTT) + (1−α) ARTT

= 0.9×29.6 × 0.1×32

= 26.64 + 3.2

= $\underline{29.84}$ msec

Packet 3

IRTT = 29.84 msec

T.O = 2×RTT = 59.68 msec

ARTT = 24 msec

NRTT = α(IRTT) + (1−α) ARTT

= 0.9×29.8 + 0.1×24

= 26.856 + 2.4

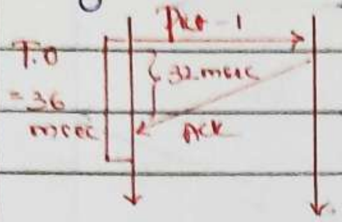
= $\underline{29.256 \text{ msec}}$

Packet 4

IRTT = 29.256

Q2. In TCP, the current RTT is 20 msec and acknowledgements come after 32 m sec. Use $\alpha = 0.5$ and initial deviation as 4. Find the estimated round-trip time and timeout in Jacobson's Algorithm.

Ans.



Packet - 1

IRTT = 20 msec, $\alpha = 0.5$, ID = 4

T.O = 4 × ID + RTT = 4 × 4 + 20 = 36 msec

ARTT = 32 msec.

AD = | IRTT − ARTT |

= | 20 − 32 | = 12

NRTT = α (IRTT) + (1 − α) ARTT

= 0.5 × 20 + 0.5 × 32

= 10 + 16 = 26 msec

ND = α (ID) + (1 − α) AD

= 0.5 × 4 + 0.5 × 12

= 2 + 6 = 8.

Packet - 2

IRTT = 26 msec

ID = 8

T.O = 4 × ID + RTT

= 4 × 8 + 26

= 32 + 26 = 58 msec

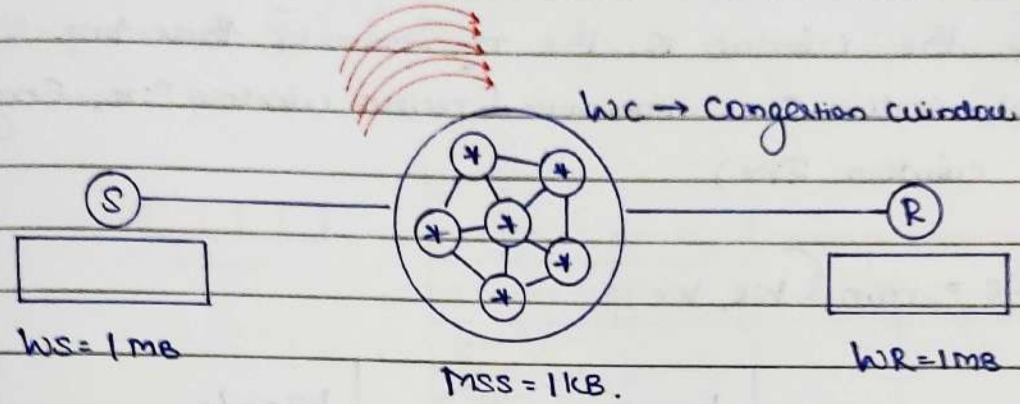
⇒ 26 msec, 58 msec

HW

Q3. The T.C.P round trip time is currently 35 m sec and it takes a segment at this moment to be acknowledged in 32 m sec after which the new RTT value is to be calculated then the next acknowledgement comes in after 40 m sec, ID = 0.9 then finally what will be new estimated RTT in m.sec ?

TCP Congestion Control

1980's
Jacobson.



No. of segments = 1024

No. of Segments $= \frac{1MB}{1KB}$

$= \frac{2^{20}}{2^{10}} = 2^{10}. = 1024.$

$$\boxed{\begin{gathered} WS = \min\{\text{Network Capacity}, \text{Reciever Capacity}\} \\ WS = \min(WC, WR) \end{gathered}}$$

An internet is a combination of networks and connecting devices (eg. routers). A packet from a sender may pass through several routers before reaching it's final destination. A router has a buffer that stores the incoming packets, process them, and forwards them. If a router recieves packets faster than it can process, congestion might occur and some packets could be dropped. When a packet does not reach the destination, no acknowledgment 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 retransmission 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 reciever but also by congestion in the network.

The sender has two piece of information: the reciever-advertised window size and the congestion window size. The actual size of the window is the minimum of these two.

→ Actual window size = minimum (recieve window size, congestion window size).

$$\boxed{W_S = \min(W_R, W_C)}$$

→ $W_C = 1$	$W_C = 2$	$W_C = 4$
$W_S = \min(W_C, W_R)$	$W_S = \min(W_C, W_R)$	$W_S = \min(W_C, W_R)$
$W_S = \min(1, 1024)$	$= \min(2, 1024)$	$= \min(4, 1024)$
$W_S = 1$.	$= 2$	$= 4$ ..

→ $W_R = 1024$ Segment, $T_H = \frac{1}{2} W_R = 512$ Segments.

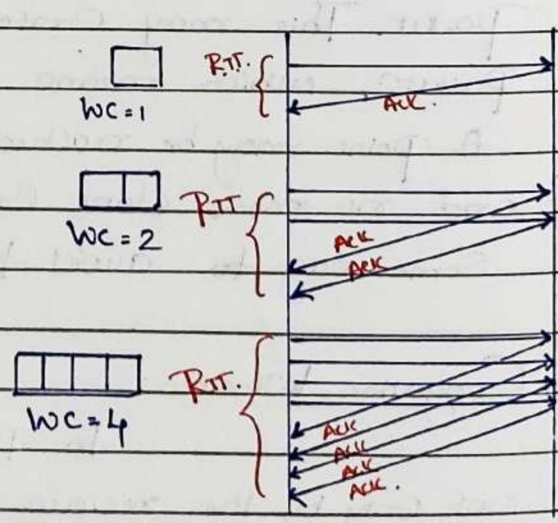
→ $W_C = 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, \underset{}{\overset{T_H}{|}}\, 513, 514, 515 \ldots 1024, 1024, 1024 \ldots$

Congestion Control Algorithm.

It has 3 phases:

1. Slow Start phase (exponential increase)
2. Congestion avoidance (additive increase)
3. Congestion detection (multiplicative decrease).

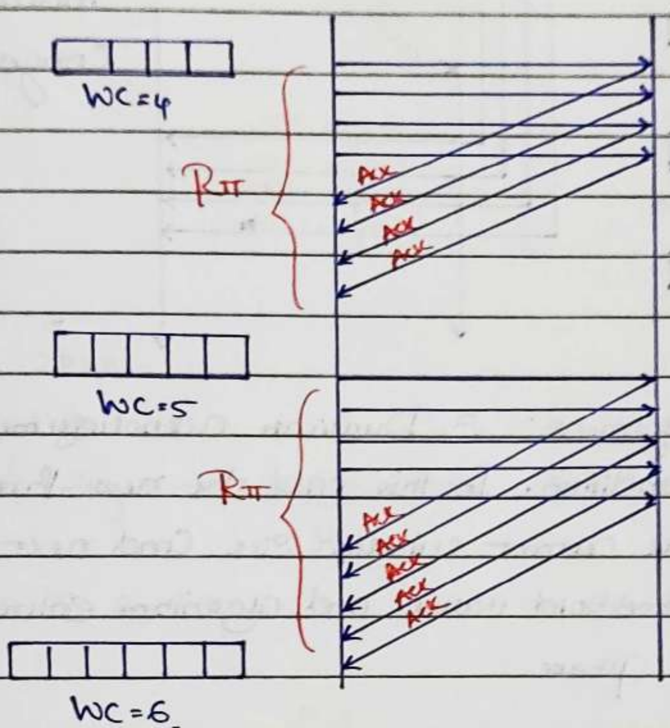
Slow Start Phase:



* 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 $\boxed{W_C = W_C + 1}$

Congestion Avoidance

* To avoid congestion before it happens we must slow down its exponential growth. In congestion avoidance we use additive increase instead of exponential increase.



$4+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}=5$

$5+\frac{1}{5}+\frac{1}{5}+\frac{1}{5}+\frac{1}{5}+\frac{1}{5}=6$

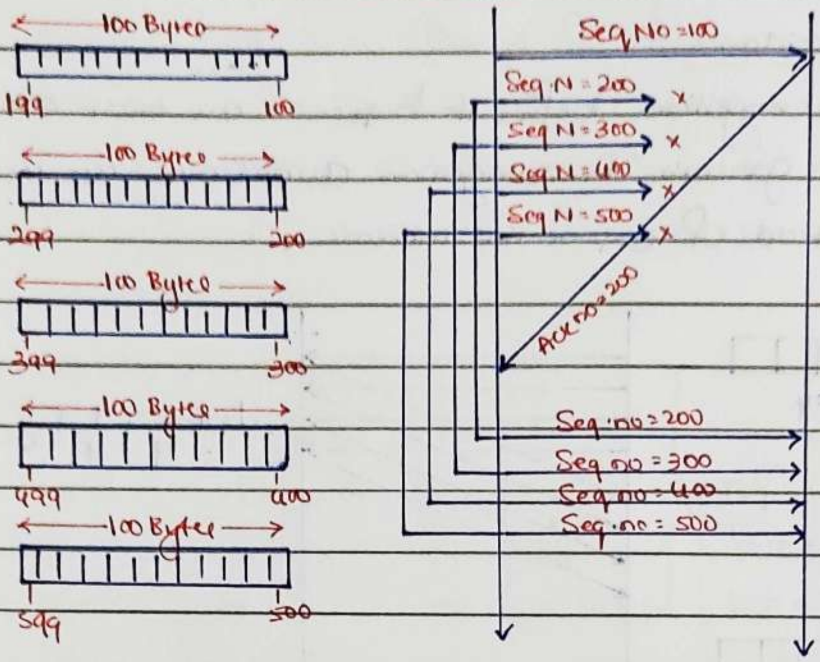
* After one RTT the congestion window will be increased by one only
* If one Ack arrives $\boxed{wc = wc + \frac{1}{wc}}$

Congestion Detection:

Congestion can be detected in two ways:

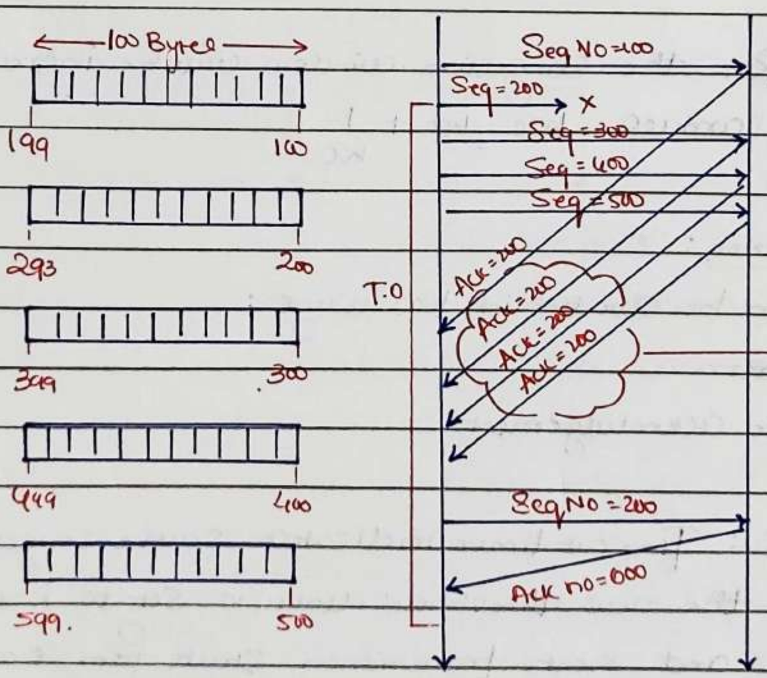
1. Time out timer
2. 3 duplicate acknowledgement

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 Acknoledgement: 3 Duplicate acknoledgement indicate mild congestion condition. In this case the new threshold value is set to half of the current window size and next transmission start from new threshold value and algorithm enters into a congestion avoidance phase.



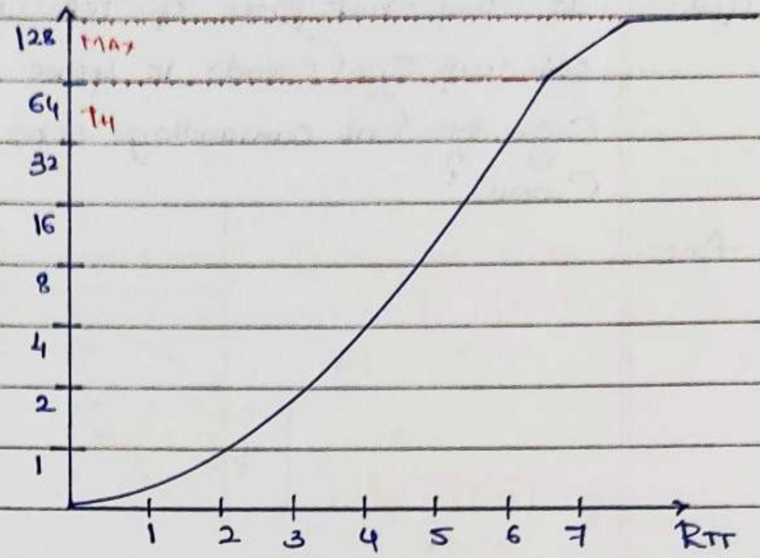
3 duplicate Ack indicating mild congestion condition.

Q1. WR = 128 KB

MSS = 1 KB   No. of Segments $= \frac{128\text{KB}}{1\text{KB}} = 128$

$TH = \frac{1}{2} \times 128 = 64$ segments.

Wc = 1, 2, 4, 8, 16, 32, 64^{TH}
65, 66, ... 128, 128 ...



Q2. WR = 128KB
MSS = 1KB
No. of Segments = $\frac{128KB}{1KB}$ = 128, $TH = \frac{1}{2}$ WR = 64 Segments.

→ 1, 2, 4, 8, 16, 32, 64^{TH}, 65, 66, 67, 68 ↑ (NTH = 34, 3.dup.ack.) 34, 35, 36, 37, 38 ↑ (NTH = 19, T.O) 1, 2

→ 4, 8, 16, 19, 20 ↑ (NTH = 10, 3 dup. ack) 10, 11, 12 ↑ (NTH = 6, T.O) 1, 2, 4, 6, 7 ... 128, 128 ....

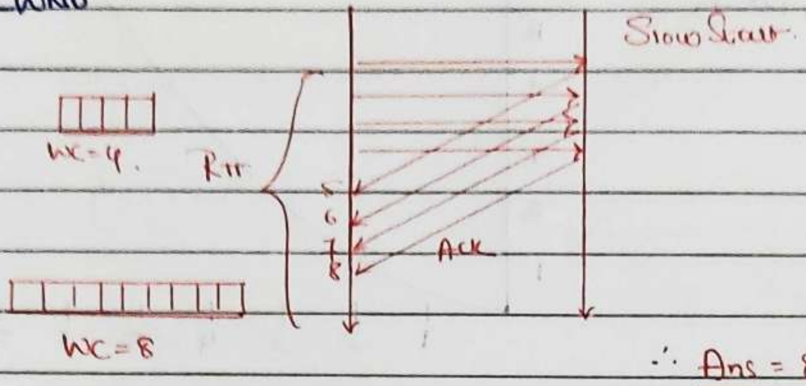
eg: 19 ↑ (NTH = 9.5, 3 dupl. ack) 9, 10, 11, 12
(Start with 9)

Q1. Consider the following Statements regarding the Slow start phase of the TCP Congestion control algorithm. Note that cwnd stand for the TCP Congestion window and MSS denotes the Maximum Segment Size.
(i) The cwnd increases by 2MSS on every successful acknowledgment.
(ii) The cwnd approximately doubles on every successful acknowledgment.
(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?

Ans. Only IV is true

Q2. In slow start phase of TCP congestion control, current congestion window size (cwnd) is 4mss and sender gets 4 successful ACKs of segments (no outstanding ACK) then what should be the value of cwnd?

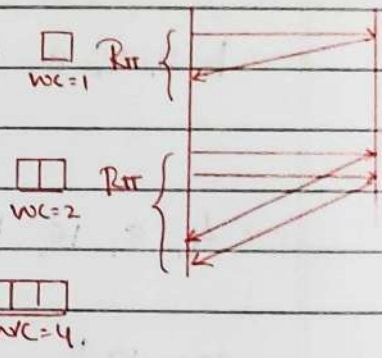
Ans.



∴ Ans = 8mss

Q3. If reciever window size is 16000 Byte and maximum segment size is 1000 Byte then after how many RTT sender will send full window?

Ans



WR = 16000 Byte

MSS = 1000 Byte No. of segments = $\frac{16000B}{1000B}$ = 16

TH = $\frac{1}{2}$ WR = 8 segments

RTT | | TH
1 | 2 | 4 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

∴ Ans = 11 RTTs

Q4. If reciever window size is 8000 Byte and maximum segment size is 1000 Byte then after how many RTTs sender will send full window?

Ans. WR = 8000 Byte

MSS = 1000 Byte No of segments = $\frac{8000 B}{1000 B}$ = 8

TH = $\frac{1}{2}$ WR = 4 segment

TH
1 | 2 | 4 | 5 | 6 | 7 | 8
1, 2, 3, 4, 5, 6

∴ Ans = 6 RTTs

Q5. Consider the effect of using Slow Start on a line with a 10-msec round-trip time. The recieve window is 24KB and the maximum segment size is 2KB. How long does it take before the first full window can be sent?

Ans. RTT = 10msec, WR = 24KB, MSS = 2KB, No. of segments = $\frac{24KB}{2KB} = 12$

$TH = \frac{1}{2} WR = 6$

RTT

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

9RTT

$9 \times 10msec = \underline{90msec}$

OR

WR = 24KB

$TH = \frac{1}{2} WR = 12KB$

2KB	4KB	8KB	12KB	14KB	16KB	18KB	20KB	22KB	24KB
	1	2	3	4	5	6	7	8	9

after 9RTTs = $9 \times 10msec = \underline{90msec}$

Q6. On a TCP connection current congestion window size is Congestion window = 4KB. The window size advertised by the reciever is advertise window = 6KB. The last byte sent by the sender is LastByteSent = 10240 and last byte acknowledged by reciever is last byte acknowledged = 8192. The current window size at sender is?

Ans WC = 4KB, WR = 6KB

WS = min (WC, WR) = 4KB

= 4×1024B = 4096 Byte

∴ Ans = 4096 Byte

Last byte sent = 10240

Last byte ack = 8192

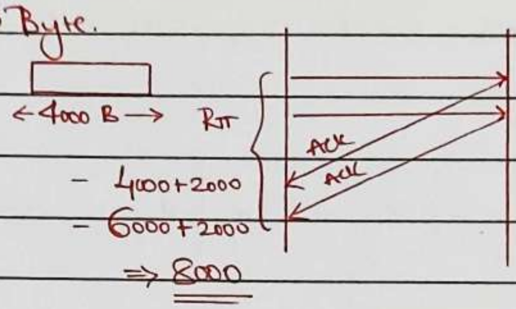
10240 − 8192

2048 Byte

Just to confuse

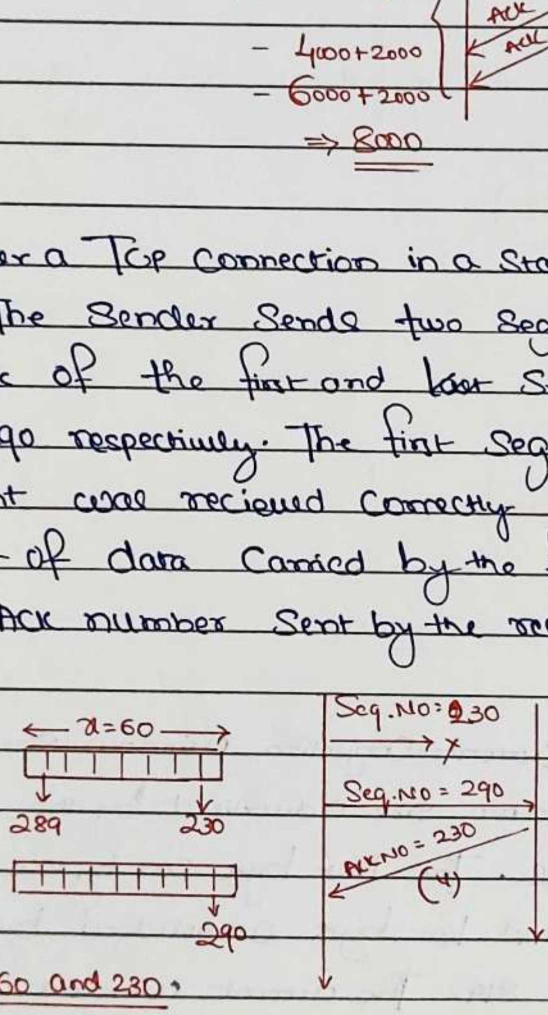
Q7. Suppose that the maximum transmit window size for a TCP connection is 12000 bytes. Each packet consist of 2000 bytes. At some point of time, the connection is in Slow-start phase with a current transmit window of 4000 bytes. Subsequently the transmitter recieves the acknowledgements. Assume that no Packets are lost and there are no time-outs. What is the maximum possible value of the current transmit window?

Ans Packet 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 ~~Second~~ segments are 230 and 290 respectively. The first segment was lost, but the second segment was recieved correctly by the reciever. Let x be the amount of data carried by the first segment (in bytes), and y be the ACK number sent by the reciever. The values of x and y.

Ans



∴ Ans = 60 and 230.

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.

Ans. T.O. NTH = 5

2 4 8 9 10 1, 2, 4 5 6 7

1st 2nd 3rd 4th 5th 6th 7th 8th 9th 10th ⇒ 7MSS ✓

classmate

Date ______
Page ______

(OR) 2 4 8^{th} 9 10 ↑(NTH = 5, T.O) 2 4 5 6 7 8
1^{st} 2^{nd} 3^{rd} 4^{th} 5^{th} 6^{th} 7^{th} 8^{th} 9^{th} 10^{th} ⟹ 8 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

32KB ↑ T.O	2KB	4KB	8KB	16KB	18KB	20KB	22KB	24KB	26KB	28KB
		1	2	3	4	5	6	7	8	9

30KB	32KB
10	11

RTT = 100 msec
Signal Size = 2KB
11 RTT
11 * 100 msec = 1100 msec

Q11. Consider a TCP connection between a client and server with the following specifications, the round trip time is 6ms, the size of the reciever 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 all acknowledgement are processed is ______

RTT = 6 msec
WR = 50 KB
Slow Start threshold = 32KB
Segment Size = 2KB
t = 0

At t=0 → 2KB
At t+6 → 4KB
At t+12 → 8KB
At t+18 → 16KB
At t+24 → 32KB (TH)

} Slow Start phase

At t+30 → 34 KB
At t+36 → 36 KB
At t+42 → 38 KB
At t+48 → 40 KB

At t+54 → 42KB

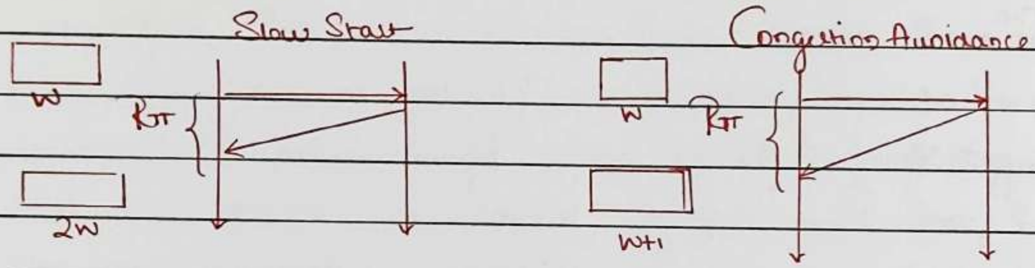
At t+60 → 44KB

OR

2KB	4KB	8KB	16KB	32KB	34KB	36KB	38KB	40KB	42KB	44KB
1	2	3	4	5	6	7	8	9	10	

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 size 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 18K bytes and a timeout occurs. How big the window be in the fifth transmission if the next four transmission burst are all successful? Assume that the maximum segment size is 1KB

Ans

NTH = 9 KB

18KB ↑ (T.O) 1KB (1st) 2KB (2nd) 4KB (3rd) 8KB (4th) 9KB (5th) ⇒ 9KB

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 4KB. The time taken by the TCP connection to get back to 64KB congestion window is

Ans

NTH = 32KB

64KB ↑ T.O	4KB	8KB	16KB	32KB (TH)	36KB	40KB	44KB	48KB	52KB	56KB	60KB	64KB
	1	2	3	4	5	6	7	8	9	10	11	

classmate

Date 22/6/23

Page

11 RTT, 11×80 msec

→ 880 msec

H/W

Q15. While establishing TCP connection both WS and WR 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. increases exponentially upto threshold value after that increase linearly

C. increases exponentially upto threshold value after that increases linearly upto sender window size

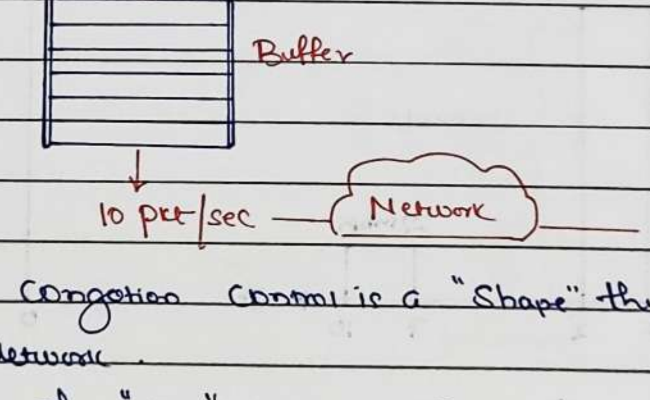
D. None of the above

Q17. In TCP congestion control AIMD algorithm 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

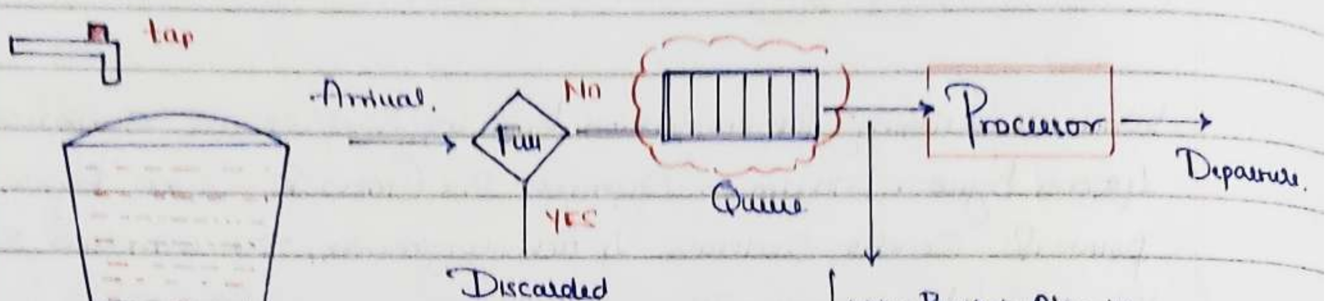
(i) Leaky bucket

(ii) Token bucket



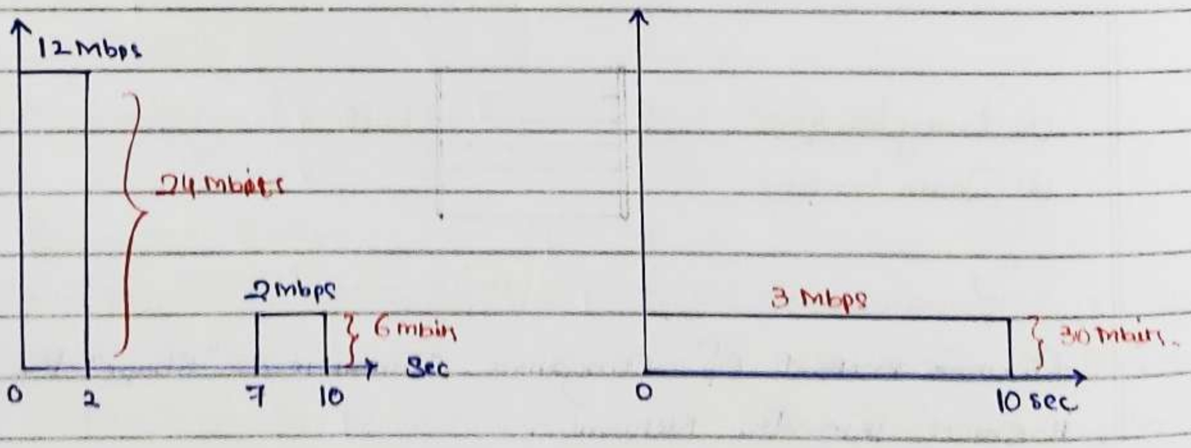
* Another method of congestion control is a "Shape" the traffic before it enters into the Network.
* Traffic shaping control the "rate" at which packet are sent.
* During connection establishment, the sender and carrier negotiate a traffic pattern

Leaky Bucket.



Leaky Bucket Algorithm
- Fetch the packet from the queue at constant rate

1. If a bucket has a small hole at the bottom, the water leaks from the bucket at a constant rate as long as there is water in the bucket.
2. The rate at which the water leaks 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 sec → 24 Mbits + 6 Mbits
→ 30 Mbits.

10 sec ⟹ 30 Mbits
Fixed data rate.

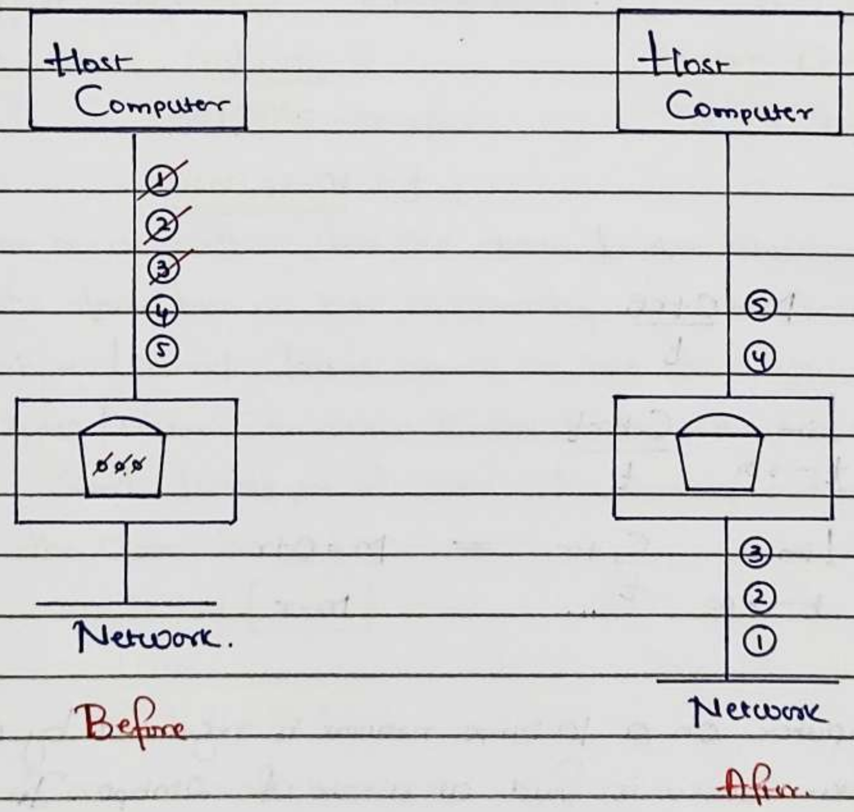
Disadvantage of Leaky Bucket:

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 tokens

* In 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.



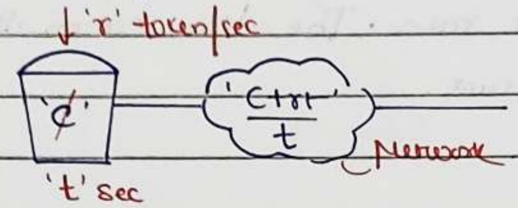
Let the capacity of token bucket is 'C' token and token enter the bucket at the rate of 'r' token per second.

Maximum no. of packets that can be entered into the network during any time interval of length 't' is

Maximum No. of packets $= C + rt$

Maximum avg rate for token bucket $= \frac{C + rt}{t}$

t sec $\rightarrow C + rt$
1 sec $\rightarrow \frac{C+rt}{t}$



Q1. Consider a token bucket of capacity 250KB 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: $C = 250$ KB, $r = 2$ MB/sec, $M = 25$ MB/sec

$M = \frac{C + rt}{t}$

$Mt = C + rt$

$Mt - rt = C$

$(M - r)\,t = C$

$\boxed{t = \frac{C}{M - r}}$

$t = \frac{250 \text{ KB}}{25 \text{MB/sec} - 2 \text{MB/sec}}$

$= \frac{250 \text{KB}}{23 \text{MB/sec}}$

$t = 10.86$ Msec

Note: $M = \frac{C + rt}{t}$

$= \lim_{t \to \infty} \frac{C + rt}{t}$

$= \lim_{t \to \infty} \frac{C}{t} + r = M = 0 + r$

$\boxed{M = r}$

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: $r = 2$ Mbps, $C = 16$ Mbits, $M = 10$ mbps

classmate

Date
Page

$t = \frac{C}{m-r} = \frac{16\text{ mbits}}{10\text{ mbps} - 2\text{ mbps}} = \frac{16\text{ mbits}}{8\text{ mbps}} = \frac{16\text{ mbits}}{8\text{ mbits/sec}} = \underline{2\text{ sec}}$

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: $M = 6\text{ mbps}$, $r = 1\text{ Mbps}$, $C = 8\text{ mbits}$

$t = \frac{C}{m-r} = \frac{8\text{ mbits}}{6\text{ mbps} - 1\text{ mbps}} = \frac{8\text{ mbits}}{5\text{ mbits/sec}} \Rightarrow \underline{1.6\text{ sec}}$

Q4. Imagine that the maximum packet size is 1000 bytes, the token bucket rate is 10 million bytes/sec, the token bucket size is 1 million bytes, and the maximum transmission rate is 50 million bytes/sec. How long can a burst at maximum speed last?

Ans. $r = 10\text{ MB/sec}$, $C = 1\text{ MByte}$, $M = 50\text{ MB/sec}$

$t = \frac{C}{m-r} = \frac{1\text{ MByte}}{50\text{ MB/sec} - 10\text{ MB/sec}} = \frac{1\text{ MByte}}{40\text{ MB/sec}} \Rightarrow 0.025\text{ sec}$

$\Rightarrow \underline{25\text{ msec}}$

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 MBytes/second. Tokens arrive at rate to sustain output at a rate of 10 MBytes/second. The token bucket is currently full and the machine needs to send 12 MBytes of data. The minimum time required to transmit the data is <u>1.1</u> seconds.

Ans. $C = 1\text{ MB}$, $M = 20\text{ MB/sec}$, $r = 10\text{ mb/sec}$

$t = \frac{C}{m-r} = \frac{1\text{ MB}}{20\text{ MB/sec} - 10\text{ MB/sec}} = \frac{1\text{ MB}}{10\text{ MB/sec}} = \underline{0.1\text{ sec}}$ (time taken to empty the bucket)

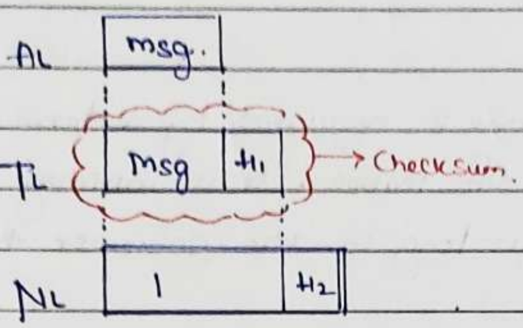
In 0.1 sec we can transfer data $= 0.1 * 20\text{ MB} = 2\text{ MByte}$

Total data $= 12\text{ MB}$, Remaining data $= 12\text{ MB} - \cancel{10}^{2}\text{ MB} = 1\cancel{2}0\text{ MB}$

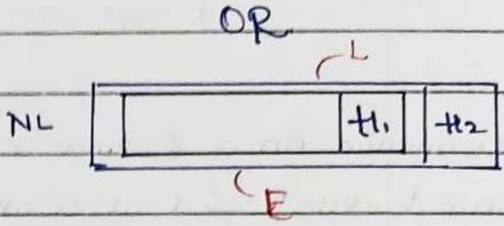
∴ for transmitting 10 MB data we need only 1 sec (bcz $r = 10\text{ mb/sec}$)

Total time $= 0.1\text{ sec} + 1\text{ sec} \Longrightarrow \underline{1.1\text{ sec}}$

TCP CheckSum



OR



$\boxed{\text{TCP Checksum = TCP data + TCP header + IP Pseudo Header.}}$

IP PseudoHeader.

S.I.P (32 bit)			→ 4B
D.I.P (32 bit)			→ 4B
Reserved 00000000 (8 bit)	Protocol (8 bit)	Tcp Segment Length (16 bit)	→ 4B
			12 Byte.

Transport Layer Protocol.

Transport layer can be connection oriented or connection less.

TCP (Transmission control Protocol). Connection Oriented

UDP (User Datagram Protocol). Connection less

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 window
6. TCP use "three way handshake" to ~~use~~ 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 provide end to end error control and flow control.
10 Data will be recieved 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 arrive.
* However that out of order segment never delivered to process.

Note: Data may arrive out of order and be temporarily stored by recieving TCP, but TCP gurantee 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 ie 8 byte

UDP-Header

Source Port. (16bit)	Destination Port (16bit)	—32bit = 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 recieving the segment.

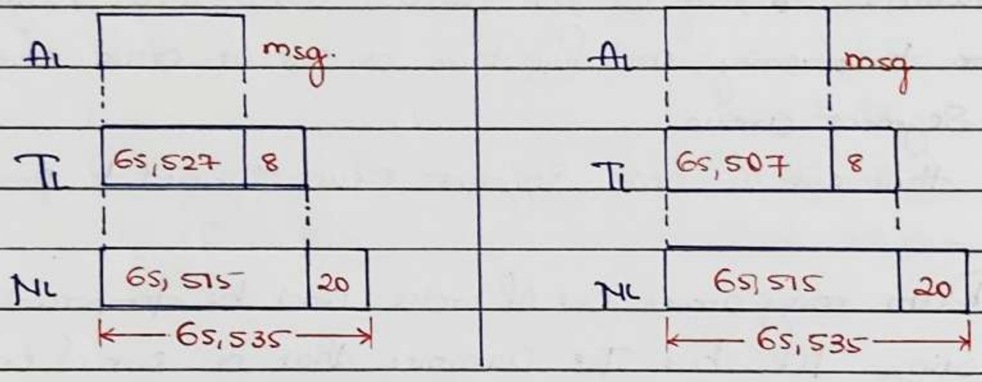
Total length = 16 bit.

Maximum number = $2^{16}-1$ = 65,535

TL = Data + Header

65,535 = Data + 8

Max UDP data = 65,535 − 8 ⇒ 65,527.

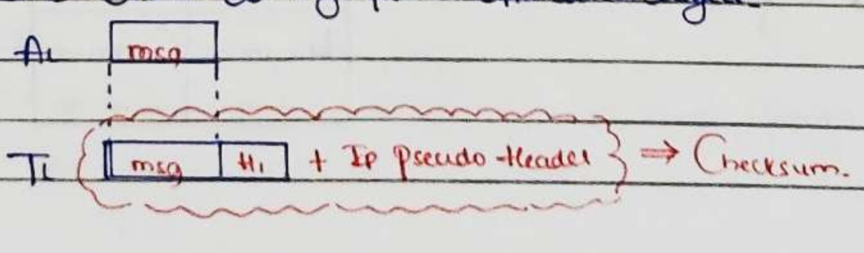


Note:

1. Practically data size at Transport layer for UDP is maximum 65,507 Bytes.
2. Only those Processes sending short message less than 65,507 byte (65535 − 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.



IP Pseudo Header

S.I.P (32 bit)			→ 4B
D.I.P (32 bit)			→ 4B
Reserved (8 bit)	Protocol (8 bit)	UDP Total length (16 bit)	→ 4B
			12B

Q. The following is the content of a UDP header in hexadecimal format.

S.port	D.port	TL	Checksum
CB84	000D	001C	001C

a. What is the source port number?

$S.port = (CB84)_{16}$

$= 12 \times 16^3 + 11 \times 16^2 + 8 \times 16^1 + 4 \times 16^0 = 52,100.$

b. What is the destination port number?

$D.port = (000D)_{16} = 13 \times 16^0 = 13.$

c. What is the total length of the user datagram?

$TL = (001C)_{16} = 1 \times 16^1 + 12 \times 16^0 = 28.$

d. What is the length of the data?

Total length = data + header, 28 = Data + 8, ∴ Data = 20 byte.

e. Is the packet directed from a client to server or vice versa?

D port no = 13 (well known port no) → {0 - 1023}

↓

Server

∴ 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 compliments the sum, the result is all 0's, the sender compliments the result again before sending. The value sent for the Checksum is all 1's. The second compliment 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 pseudoheader have non zero values.

classmate
Date 24/6/23
Page

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. Application that required multimedia data transfer, application that requires fastness then 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 realtime and multimedia protocols.

Note:

* Client Server application such as DNS uses the services of UDP because a client need to send a short request to server and to recieve 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~~ by the application into different user datagrams. Here the connectionless service may create problems. The user datagrams may arrive and be delivered to the reciever application out of order. The reciever application may not be able to reorder the pieces.

24/6/23

MEDIUM ACCESS CONTROL

Multiple Access Protocols

- **Random Access Protocols**
  - ALOHA
  - CSMA
  - CSMA/CD
  - CSMA/CA
- **Control Access Protocols**
  - Reservation
  - Polling
  - Token passing.
- **Centralized Access Protocols**
  - FDMA
  - TDMA
  - CDMA

IEEE

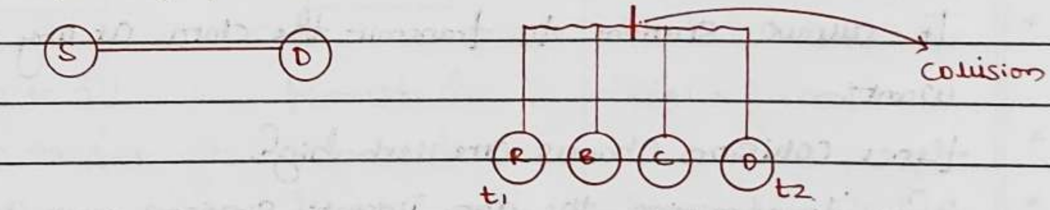
NL
DLL
PL

DLL — LLC — Error Control, Flow Control

DLL — MAC — Access Control.

Links

- Point to Point Link
- Broadcast Link.



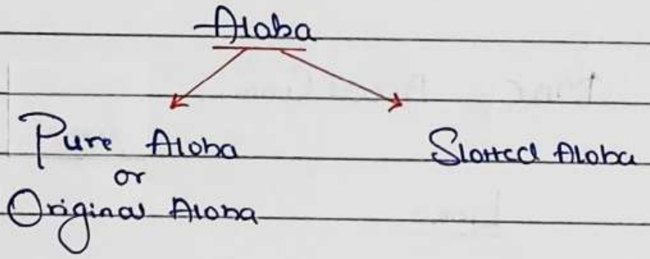
Random Access Protocols

1. In random access, no station is superior to another station and none 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 frames will be either destroyed or modified).

4. To avoid collision station must send data by executing a procedure or a condition defined by the protocal.
5. There is no fixed order in which station send data so these are called Random access protocols.
6. Each station competes for the channels hence these are also known contention methods.

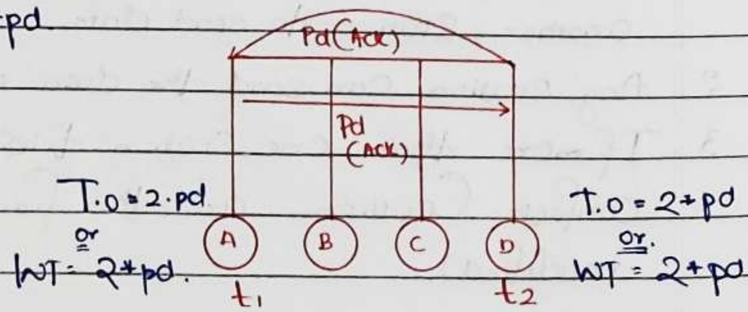
Introduction to Aloha.

* Aloha was developed at university of hawaii in 1970's.
* 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 acknoledgement does not arrive after a time out period, the station assume that frame (or the acknoledgement) has been destroyed.
* The timeout period is equal to the maximum possible round trip propogation delay i.e $2 * pd$.



* After the timeout, Station will again send data but if it is immediately 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 station must not send frame immediately after timeout.
* It must wait for random amount of time called back off time.

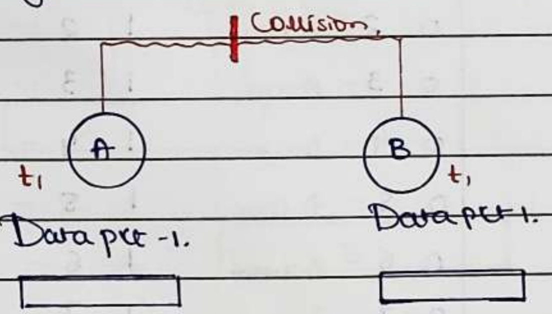
Back off time = K x slot time.
↓
$(0 \text{ to } 2^n - 1.)$

K → Any random number in btw $0 - 2^n - 1$.
n → collision number.

Note : Collision number is with respect to data pkt
→ Slot time = (RTT (2xpd) or Td or Pd).

Note : Maximum number of attempts for the station is 15.

Binary exponential Back off Algorithm (2 station).



n=1.

$K \to 0 \text{ to } 2^n - 1$

$K \to 0 \text{ to } 2^1 - 1$

$K \to 0, 1$

n=2

$K \to 0 \text{ to } 2^n - 1$

$K \to 0 \text{ to } 2^1 - 1$

$K \to 0, 1$

A	B	
0	0	→ Collision
0	1	→ A won
1	0	→ B won
1	1	→ Collision

$P(A) = \frac{1}{4} = 25\%$

$P(B) = \frac{1}{4} = 25\%$

$P(\text{collision}) = \frac{2}{4} = 50\%$

→ If we choose (0, 1)

Back off time for A = K * slot time
= 0 x slot time = 0

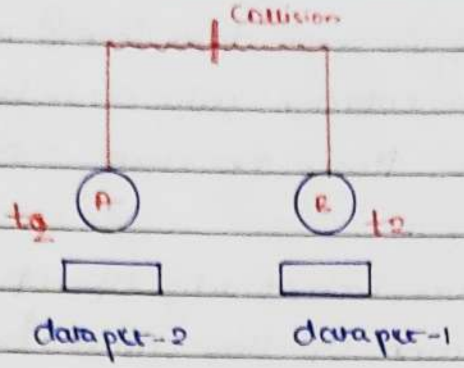
Or

WT for A

Back off time for B = K * Slot time
= 1 * slot time.

Or

Waiting time for B



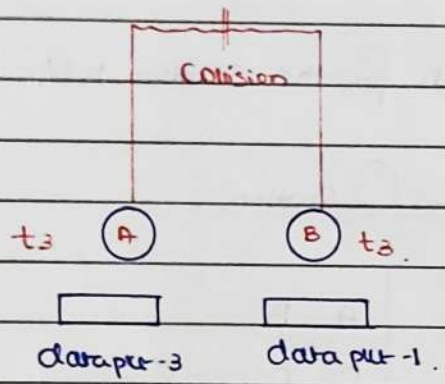
$n=1$	$n=2$
$K \to 0$ to 2^n-1	$K \to 0$ to 2^n-1
$K \to 0$ to 2^1-1	$K \to 0$ to 2^2-1
$K \to (0,1)$	$K \to 0$ to 3.
	$K \to (0,1,2,3)$

A	B	
0	0	→ Collision
0	1	→ A won
0	2	→ A won
0	3	→ A won
1	0	→ B won
1	1	→ Collision
1	2	→ A won
1	3	→ A won.

$P(A) = \frac{5}{8} = 0.625 = \underline{62.5\%}$

$P(B) = \frac{1}{8} = 0.125 = \underline{12.5\%}$

$P(\text{collision}) = \frac{2}{8} = \frac{1}{4} = \underline{25\%}$



$n=1$	$n=3$
$K \to 0$ to 2^n-1	$K \to 0$ to 2^n-1
$K \to 0$ to 2^1-1	$K \to 0$ to 2^3-1
$K \to (0,1)$	$K \to (0-7)$.

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

$P(A) = \frac{13}{16} = 0.8125 = 81.25\%$.

$P(B) = \frac{1}{16} = 0.0625 = 6.25\%$.

$P(\text{collision}) = \frac{2}{16} = 0.125 = 12.5\%$.

→ Initially the Probability of collision = 100%
After 1st collision " " " = 50%
After 2nd collision " " " = 25%
After 3rd collision " " " = 12.5%

Date 25/6/24

- 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 have a more Probability for winning in the next collision.

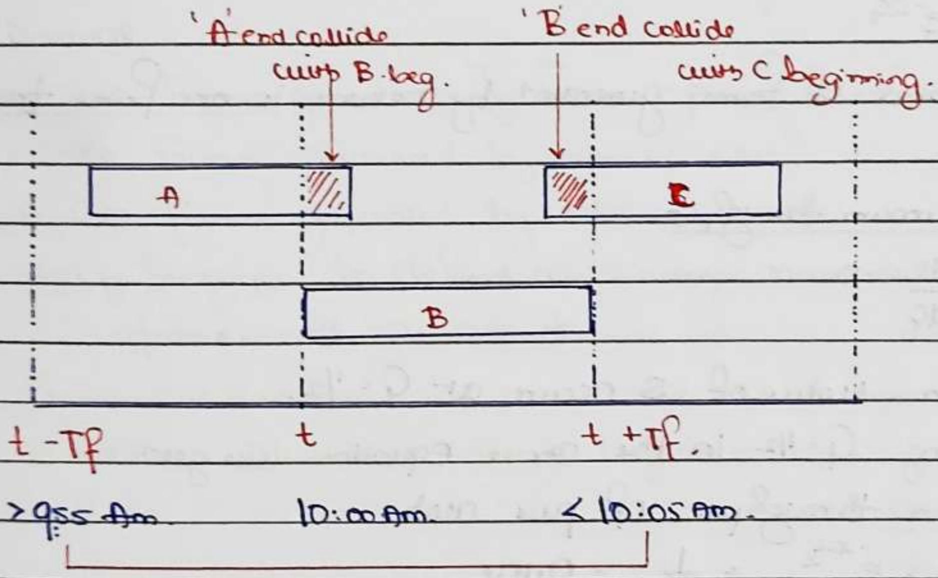
eg: initially $P(A) = 25\%$

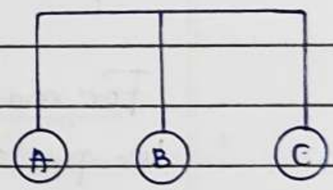
$P(A) = 62.5\%$

$P(A) = 81.25\%$

Vulnerable time for pure Aloha

Vulnerable time is the range of time where collision take place





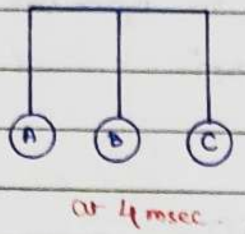
Vulnerable time =10min

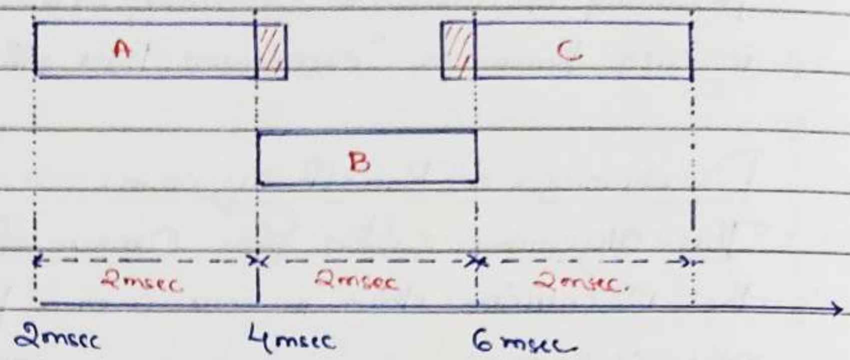
$\boxed{\text{Vulnerable time for pure aloha} = 2 * Tf.}$

$\boxed{\text{Transmission time for single frame } (Tf) = \frac{\text{Frame Size}}{\text{Bandwidth}} = \frac{L}{B}}$

Assume Transmission time for single frame Tf = 5min — above diagram

2.





Assume $T_f = 2$ msec.

A starts at 2.001 msec
A → 2.001 msec to 4.001 msec
C starts at 5.98 msec.

2 msec —— 6 msec
Vulnerable time = 4 msec

$\boxed{\text{Vulnerable time for pure aloha} = 2 * T_f}$

Throughput of pure aloha

$$\boxed{S = G \times e^{-2G}}$$

G = number of frames generated by network in one frame transmission t

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

$$= \frac{1}{2} \times e^{-2 \times \frac{1}{2}} = \frac{1}{2e} = 0.184$$

∴ 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 Sucessfully
2. $S_{max} \rightarrow G = \frac{1}{2}$
   One half frame should be generated in one frame transmission tim

classmate

Date ____
Page ____

to achieve maximum throughput.

OR

One frame should be generated in two frame transmission time to achieve maximum throughput → vulnerable time = $2 * T_f$

(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. A pure aloha network transmits 200 bit frames on shared channel of 200kbps. What is the throughput if the system (all station together) produces.

(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 bit

Bandwidth = 200 Kbps = 200×10^3 bit/sec

Transmission time = $\frac{\text{Frame}}{\text{Bandwidth}}$

$= \frac{200 \text{ bit}}{200 \times 10^3 \text{ bit/sec}} = 10^{-3} \text{ sec} = \underline{1 \text{ msec}}$

Solution (i):

1 Sec. —— 1000

1 msec —— 1000×10^{-3} Frame

$\boxed{G = 1}$ (No. of frames generated in one frame transmission time).

Throughput = $S = G \times e^{-2G}$

$= 1 \times e^{-2 \times 1} = \frac{1}{e^2} = 0.135$, ∴ Throughput = $\underline{13.5\%}$

Avg. no. of frames generated successfully transmitted per sec = 1000×0.135
$= \underline{\underline{135}}$

Solⁿ (ii)

1 sec ⟶ 500 frame

1 msec ⟶ 500×10^{-3} frame

$= 5 \times 10^{-1}$

$= 5/10$ fram ⇒ $\boxed{G = \frac{1}{2}}$

Throughput $S = G \times e^{-2G}$

$= \frac{1}{2} \times e^{-2 \times 1/2}$

$= \frac{1}{2e} = 0.184$

$= \underline{\underline{18.4\%}}$

Avg no of frames successfully transmitted per sec = $500 \times 0.184 \Rightarrow 92$.

Solⁿ (iii)

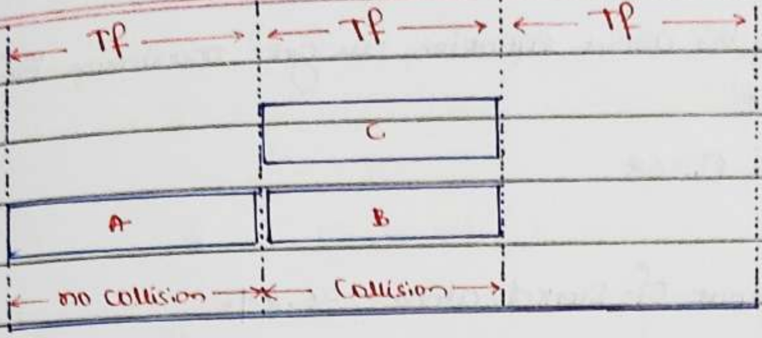
$\boxed{G = \frac{1}{4}}$ Throughput $= 0.152 \rightarrow 15.2\%$.

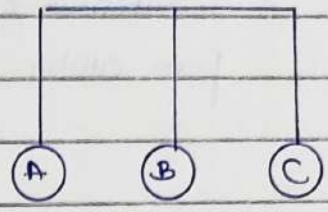
Average no. of frames successfully transmitted/sec $= 0.152 \times 250$
$= \underline{\underline{38}}$

Slotted Aloha.

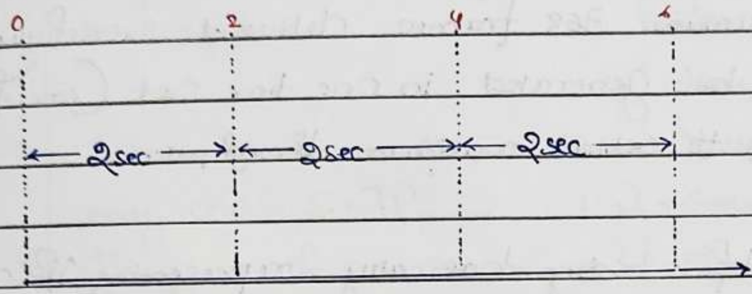
* Slotted aloha divides the time of shared channel into discrete intervals called as time slot (time slot = Transmission time for one frame).
* Any station can transmit its data in any time slot.
* The only condition is that station must start its transmission from beginning of time slot.
* If the beginning 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 ⟶ Variable time is the range of time where collision take place (T_f).





$\boxed{\text{Vulnerable time for Slotted Aloha} = T_f}$



2\. Note
- A — 2.3 sec
- B — 3.1 sec
- C — 3.3 sec

} 4 sec

Assumed $T_f = 2$ sec

Station A Start at 2.3 sec → 4 sec
Station B Start at 5.2 sec → 6 sec
} 1. Note.

Note:

1. For example $T_f = 2$ 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 5.2 sec then it will send at 6 sec.
2. 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 frame generated by n/w in one frame transmission time.

For maximum throughput:

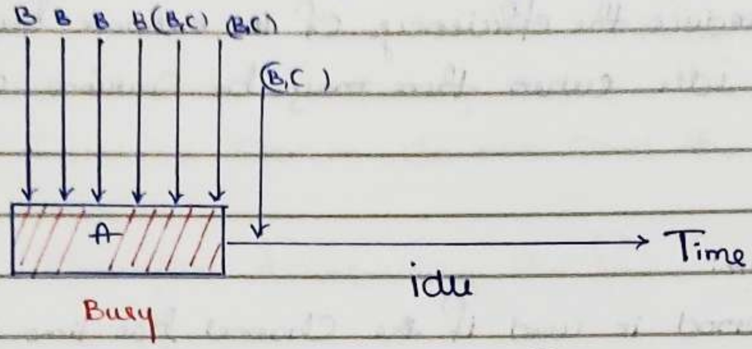
* We put $\frac{dS}{dG} = 0$
* Maximum value of s occurs at $G = 1$

classmate
Date 29/6/23
Page

Persistent Methode In CSMA:

1. Persistent CSMA

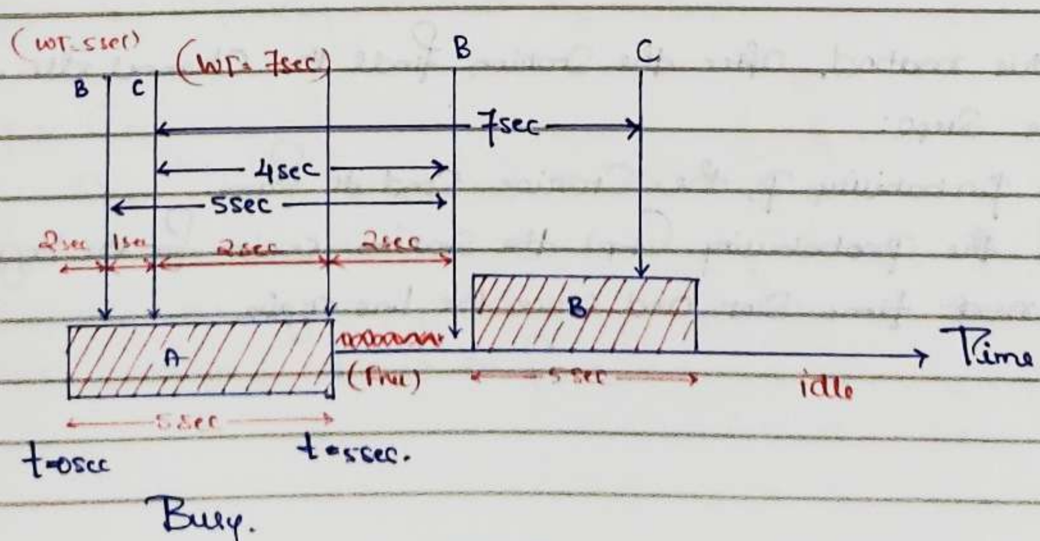
In case of 1-persistent CSMA Station will continously sense the channel and once the channel is idle. It send it's frame immediately (with probability 1).



* Probability of collision is high for example, if two Station become ready in the middle of the third transmission, both will wait politely until the transmission ends, and then both will begin transmitting exactly simultaneously then collision will occur.
* Ethernet LAN uses 1-persistent method.

2. Non-persistent CSMA:

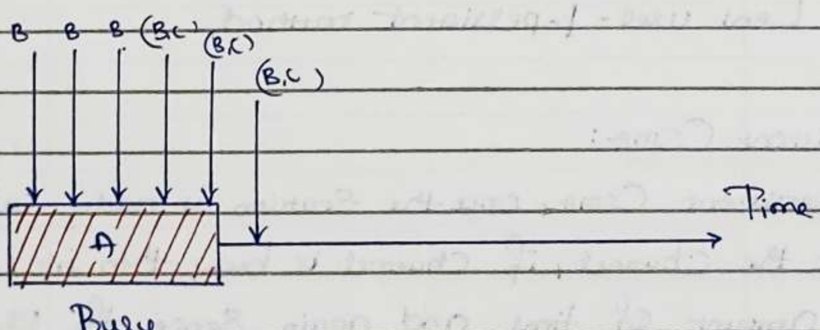
In non Persistent CSMA, once the Station is ready with the data it will sense the channel, if channel is busy then it will wait for random amount of time and again sense the channel



* Once the Channel is free: then it immediately transmit the frame.

Note:
→ In non persistent CSMA finding the channel idle at the same time by different Station is less. So collision is less compared to 1-persistent.
→ This method reduce the efficiency of the network because the medium remains idle when there may be Stations with frame to send.

P-Persistant CSMA:
* P- persistant 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 reduce the Chance of collision and improve efficiency



* In this method, after the Station finds the Channel idle it follows these Steps:
1. With probability P, the Station Send its frame.
2. With the probability (1-p) the Station wait for the beginning of the next time Slot and check the line again.

classmate
Date
Page

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 station 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 station do not send the entire frame and then look for collision.
* In CSMA/CD transmitting the frame and detecting the collision are continous process.
* Sender needs two different port ie. one for sending the data and another for detecting the collision.
* If collision is detecting then sender immediately stop transmitting the data.

S.P	→ Sending port : for sending the data
L.P	→ Listening port : for detecting the collision.

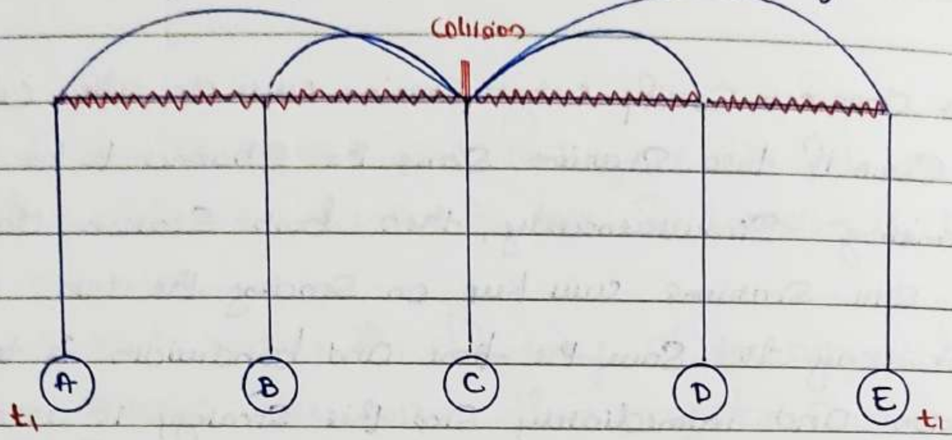
No Acknowledgement :

There is no need of acknowledgement, if collision is not detected then frame is definetely recieved by reciever.

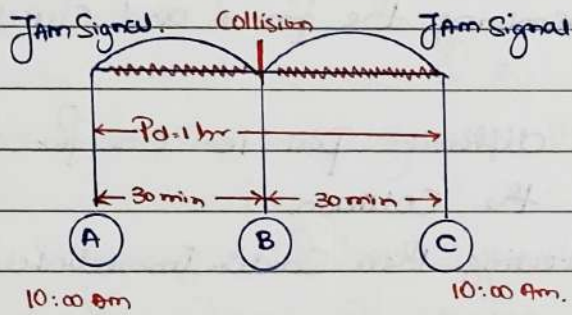
No Copy :

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 reciever has successfully recieved the frame.

Collision Signal or JAm Signal.



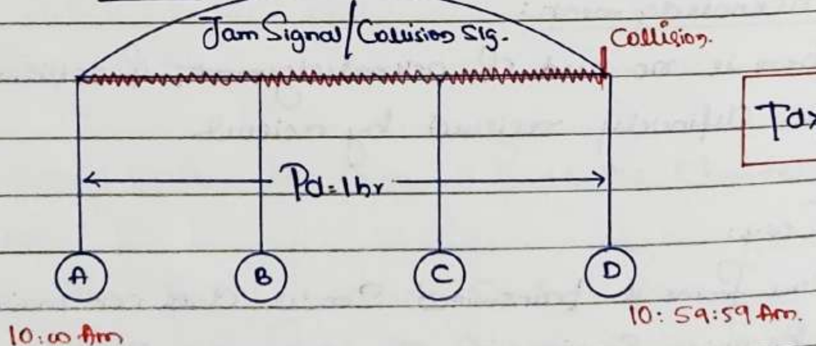
Minimum Frame to detect the collision :



$\boxed{T_d \geq P_d}$

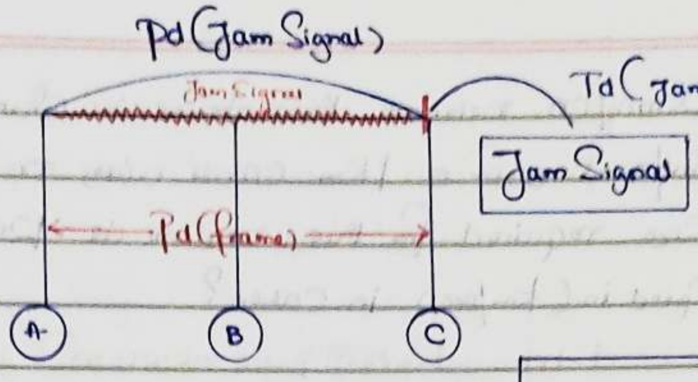
At 10:00 Am → Both 'A' and 'C' Start transmitting the data.
At 10:30 Am → Collision
At 11:00 Am → Both A and C recieve Collision Signal.

Pd (1hr)



$\boxed{T_d \geq 2 * P_d}$

10:00 Am → 'A' Start transmitting the data.
10:59:59 Am → 'D' Start transmitting the data
11:00 Am → Collision
12:00 Pm → 'A' recieve Collision Signal.



$$\boxed{Td(\text{Jam Signal}) = \frac{\text{Jam Signal Size}}{\text{Bandwidth}}}$$

$Td(\text{Frame}) \geq Pd(\text{frame}) + Td(\text{Jam S.}) + Pd(\text{Jam S.})$

$$\boxed{Td(\text{Frame}) \geq 2*pd + Td(\text{Jam Signal})}$$

Minimum frame size to detect the collision

$$\frac{\text{Frame Size }(L)}{\text{Bandwidth }(B)} \geq 2*pd + Td(\text{Jam Signal})$$

$$\boxed{\text{Frame Size} \geq (2*pd + Td(\text{Jam Signal})) * \text{Bandwidth}}$$

$$\boxed{L \geq (2*pd + Td(\text{Jam Signal})) * B}$$ (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.

Ans $B = 1\text{Gbps} = 10^9 \text{ bits/sec}$, $d = 1\text{Km}$

$v = 200000 \text{ km/sec}$

$Td \geq 2 \times Pd + \cancel{Td(\text{Jam Signal})}_0$

$\frac{L}{B} \geq 2 \times Pd$

$L \geq 2 \times Pd \times B$

$L \geq 2 \times \frac{d}{v} \times B$

$L \geq 2 \times \frac{1\text{ Km}}{200000 \text{ Km/sec}} \times 10^9 \text{ bits/sec}$

$L \geq 10^4 \text{ bits}$

$\underline{L \geq 10000 \text{ bits.}}$

Q2. Consider a CSMA/CD network that transmits data at a rate of 100 Mbps (10^8 bits/sec) over a 1 Km cable with 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 $B = 10^8$ bits/sec, $d = 1$ Km, $L = 1250$ Byte $= 8 \times 1250 = 10{,}000$ bits

$T_d \geq 2 * P_d + T_d(\text{Jam/Signal})$ ($\to 0$)

$T_d \geq 2 \times P_d$

$\frac{L}{B} \geq 2 \times P_d \Rightarrow \frac{10{,}000 \text{ bits}}{10^8 \text{ bits/sec}} \geq \frac{2 * 1 \text{ Km}}{v}$

$= \frac{1}{10^4} \geq \frac{2}{v}$

$v = 2 \times 10^4$ Km/sec

$v = \underline{20{,}000 \text{ Km/sec}}$

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 $B = 20 \times 10^6$ bits/sec

$P_d = 40\,\mu\text{sec} = 40 \times 10^{-6}$ sec

$L = ?$

$T_d \geq 2 \times P_d + T_d(\text{Jam/Signal})$ ($\to 0$)

$\frac{L}{B} \geq 2 \times P_d$

$L \geq 2 \times P_d \times B$

$L \geq 2 \times 40 \times 10^{-6}\,\cancel{\text{sec}} \times 20 \times 10^{6}$ bits/$\cancel{\text{sec}}$

$L \geq 1600$ bits

$L \geq \frac{1600}{8}$ Byte $\Rightarrow \underline{L \geq 200 \text{ Byte}}$

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 → Token ring

IEEE 8.02.11 → Wireless: LAN (CSMA/CD)

IEEE 802.16 → Wireless WAN

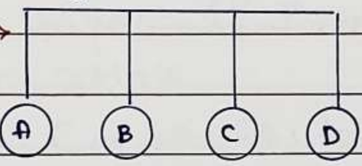
Standard Lan Technology

↓

(Ethernet) (Token ring.)

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 recieve it.
7. Ethernet uses Manchester encoding technique for converting data bits into signal.

(Baud rate = 2× bit rate)
Bit rate = 1/2 baud rate.

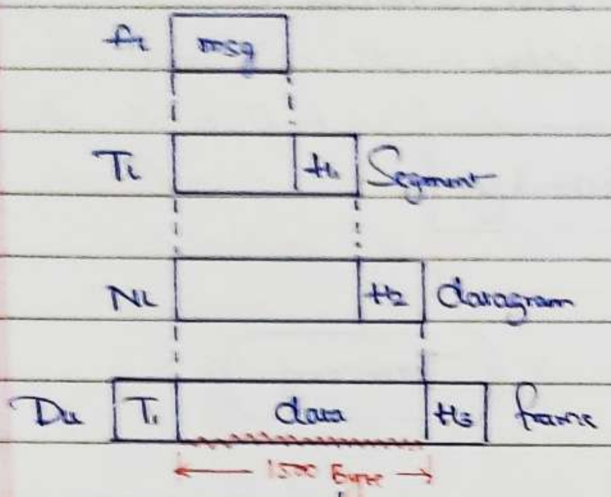
Ethernet Evolution

↓

Standard Ethernet	Fast Ethernet	Gigabit Ethernet	10 Gigabit Ethernet.
10 mbps	100 Mbps	1 Gbps	10 Gbps

30/6/23

IEEE 802.3 Ethernet Frame Format:



← H3 →						← T1 →
Preamble (101010)	SFD (10101011)	DA	SA	Length of Data or type	data	CRC
7 byte	1 byte	6B	6B	2B	46-1500	4 Byte
← Physical layer header →	← DLL			→		← DLL →

Preamble (7 Byte)

* It is a 7 byte field, it is an alternating pattern of 1's and 0's.
* It alerts the station that frame is going to start.
* It also enables the sender and reciever to establish bit synchronization.

Start Frame Delimeter [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 '11' and alerts the reciever 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 byte.

Destination Address [DA]

* It is a 6 byte field that contains the MAC address of the destination.

Destination MAC Address

1. Unicast MAC address
2. Multicast MAC address
3. Broadcast MAC address

Unicast MAC address: If last bit of the first byte is 0. It indicate unicast MAC address.

3A : 2B : C3 : 5A : 9B : 70

| 0011101 | 0 | → It indicates unicast MAC address.

Multicast MAC address: If the last bit of the first byte is 1. It indicate multicast MAC address.

A3 : 2B : C3 : 5A : 9B : 70.

| 1010001 | 1 | → It indicates multicast MAC address.

Broadcast MAC address: If all 48 bits are 1. It indicates 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 in between 46 byte - 1500 byte
* In 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 extra 0's.

Note:

Minimum size is needed to sense the collision.

Ethernet uses CSMA/CD as an access control method to deal with collision. $\boxed{Td(\text{frame}) \geq 2 \times PD + Td(\text{Jam Signal})}$ → 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 application where data size very less.

MIN	MAX	
46B	1500	→ Data
64B	1518	→ Frame

$46B + 6B + 6B + 2B + 4B = 64B$

Data DA SA | CRC |

length of data — Min frame size.

2. It is not suitable for realtime application. Realtime 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 application. Client-Server applications requires that server must be given higher priority than clients. In ethernet there is no facility to set priorities.

Problems on Ethernet.

Q1. Ethernet when Manchester encoding is used, the bit rate is:

Ans Baud rate = 2 * bit rate

bit rate = $\frac{1}{2}$ Baud rate ∴ Half the baud rate

Q2. What is the Baud rate of Standard 10 mbps 802.3 LAN?

Ans Bit rate = 10 mbps

Baud rate = 2 * bit rate ⇒ 20 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 propogation delay for a 10mbps Ethernet having 48-bit jamming signal is 46.4 μs. The minimum frame size is :

Ans

$B = 10\ mbps = 10 \times 10^6$ bits/sec , Jam signal size $= 48$ bits

$RTT = 46.4\ \mu s = 46.4 \times 10^{-6}$ sec

$Td(frame) \geq 2 \times pd + Td(Jam\ Signal)$

$Td(frame) \geq RTT + Td(Jam\ Signal)$

$Td(frame) \geq 46.4\mu s + 4.8 \mu s$

$Td(frame) \geq 51.2\ \mu sec$

$\frac{L}{B} \geq 51.2 \times 10^{-6} sec$

$L \geq 51.2 \times 10^{-6} sec \times B$

$L \geq 51.2 \times 10^{-6} sec \times 10 \times 10^{6}$ bits/sec

$L \geq 512$ bits

$Td(Jam\ Signal) = \frac{Jam\ Signal}{Bandwidth}$

$= \frac{48\ bits}{10 \times 10^6\ bits/sec}$

$= 4.8 \times 10^{-6}$ sec

$= 4.8\ \mu sec$

OR

$L \geq (2 \times Pd + Td(Jam\ Signal)) \times B$

$L \geq (RTT + Td(JS)) \times B$

$L \geq (46.4\ \mu sec + 4.8\ \mu sec) \times B$

$L \geq 51.2\ \mu sec \times B$

$L \geq 51.2 \times 10^{-6} sec \times 10 \times 10^{6}$ bits/sec

$L \geq 512$ bits

Q5 Define the type of the following destination address.

C4A:30:10:21:10:1A in the Ethernet Frame Format.

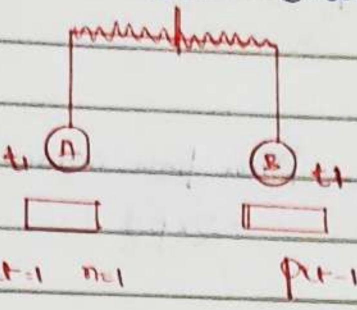
$\boxed{0100101\,|\,0} \rightarrow$ Unicast MAC address.

Ans 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 this successful transmission by A, both A and B attempt to transmit and again collide. The probability that

A wins the second backoff race is:

Ans.



P(A) = 25%

P(A) = 62.5%

P(A) = 81.25%

∴ 0.625

Q7. Suppose the Round-trip propagation delay for 100 Mbps Ethernet has 24.2 μsec. The network has 48 bit jamming signal then what is minimum frame size:

Ans 2468 bit.

Q8. Determine the maximum length of the cable (in Km) for transmitting data at a rate of 500 Mbps in Ethernet LAN with frames of size 10,000 bits. Assume the signal speed in the cable to be 200,000 Km/sec.

Ans. $B = 500 \times 10^6$ bit/sec, L = 10,000 bits

V = 2000000 Km/sec

Td (frame) ≥ 2 * pd

$$\frac{L}{B} \geq 2 \times \frac{d}{V}$$

$$\frac{10000 \text{ bit}}{500 \times 10^6 \text{ bit/sec}} \geq \frac{2 \times d}{200000 \text{ Km/sec}} \quad \therefore d = 2\text{Km}$$

Q9. In an Ethernet local area network, which one of the following statements is true?

Ans The exponential back off mechanism reduces the probability of collision on retransmission.

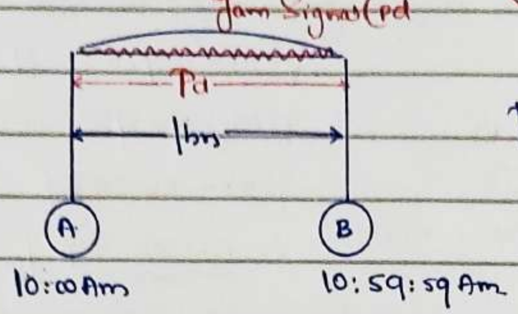
P(collision) = 100%

P(C) = 50%

P(C) = 25%

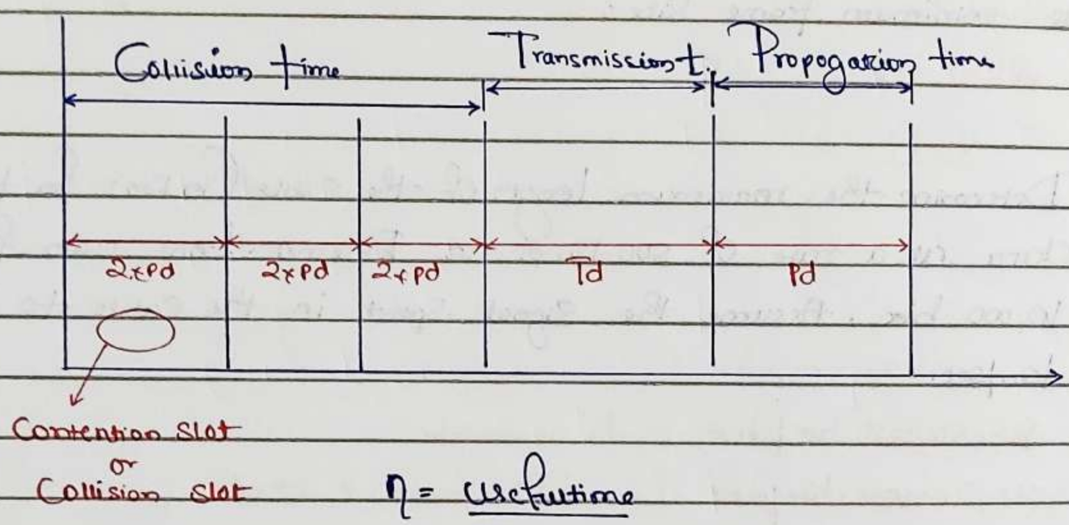
P(C) = 12.5%

Efficiency of Ethernet (CSMA/CD)



Max time waited in One Collision $= 2 \times pd$

Efficiency Calculation of Ethernet (CSMA/CD)



$$\eta = \frac{\text{Usefultime}}{\text{Total time}}$$

$$\eta = \frac{\text{Transmission time}}{\text{Collision time} + \text{Transmission time} + \text{Propogation time}}$$

$$\eta = \frac{Td}{C \times 2 \times pd + Td + Pd} = \frac{Td}{e \times 2 \times pd + Td + pd}$$

$\frac{Pd}{Td} = a$

$$\eta = \frac{Td}{Td\left[e \times \frac{2 \times pd}{Td} + 1 + \frac{Pd}{Td}\right]} \Rightarrow \frac{1}{e \times 2 \times a + 1 + a}$$

$e = 2.72$

$\boxed{\text{C = No. of Contention slot or No. of Collision slot.}}$

Continued next page!

$$\eta = \frac{1}{2.72 \times 2.a + 1 + a}$$

$$\eta = \frac{1}{5.44a + 1 + a}$$

$$\boxed{\eta = \frac{1}{6.44a + 1}}$$

$$\eta = \frac{1}{1 + 6.44a \times \frac{d}{v} \times \frac{B}{L}}$$

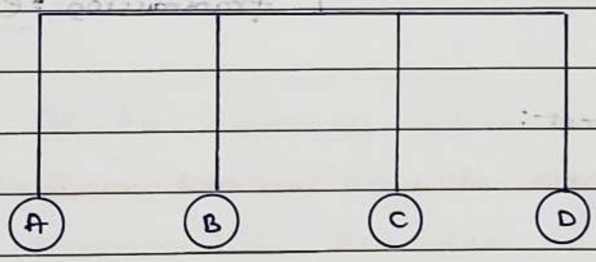
$\left\{ \begin{array}{l} v - \text{fixed} \\ B - \text{fixed} \end{array} \right.$

$d \uparrow \eta \downarrow \rightarrow$ Good for LAN not for WAN

$L \uparrow \eta \downarrow \rightarrow$ Good for larger packet size.

Note:

1. In Ethernet efficiency is high when propogation delay is low and transmission delay is high.
2. In ethernet efficiency is low when propogation 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 succesful transmission of one station the remaining
→ $(N-1)$ station should not transfer the data packet".

→ $(1-p)^{N-1}$ = Probability of $(N-1)$ station not to transfer the data packet.
→ $p(1-p)^{n-1}$ = probability of succes for a single station.
→ $N.p(1-p)^{N-1}$ = probability of succes for any station among 'N' stations.

$$\boxed{P_{succ} = N \cdot p \cdot (1-p)^{N-1}}$$

→ For $Max(P_{succ})$: $\frac{d}{dp}(P_{suc}) = 0$

$$= \frac{d}{dp}\left[N \cdot p (1-p)^{N-1}\right] = N\left[p \cdot \frac{d}{dp}(1-p)^{N-1} + (1-p)\frac{d}{dp}p\right]$$

$$\boxed{p = \frac{1}{N}} \qquad P_{suc} = N \cdot p (1-p)^{N-1}$$

$$= N \times \frac{1}{N}\left(1-\frac{1}{N}\right)^{N-1} = \left(1-\frac{1}{N}\right)^{N-1}.$$

* If there are sufficiently large no. of stations i.e $N \to \infty$ we have:

$$\lim_{N\to\infty} (P_{suc})_{max} = \lim_{N\to\infty}\left(1-\frac{1}{N}\right)^{N-1}. = \frac{1}{e}$$

* 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 high

Q2. Which of the following statements is true about CSMA/CD

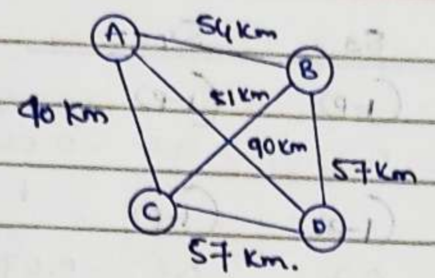
Ans CSMA/CD is not suitable for a high propagation delay network like satellite network.

$$\eta = \frac{1}{1+6.44a} = \frac{1}{1+6.44 \times \frac{Pd}{Td}}.$$

$Pd \uparrow \ \eta \downarrow$

$Td \uparrow \ \eta \uparrow$

Q3. The network consist of 4 hosts distributed as shown below. Assume this network uses CSMA/CD and signal travel at 3×10^5 Km/sec. If sender send at 1mbps, what could be minimum size of the packet?



$V = 3 \times 10^5$ Km/sec

$B = 1$ mbps $= 10^6$ bits/sec

$L = ?$

Ans. $T_d(\text{frame}) \geq 2 \times P_d + T_d(\text{Jam Signal})$ (Jam Signal $\to 0$)

$\frac{L}{B} \geq 2 \times P_d \Rightarrow L \geq 2 \times P_d \times B$

$L \geq 2 \times 30 \times 10^{-5}$ sec $\times 10^6$ bits/sec

$L \geq 2 \times 30 \times 10$ bits

$L \geq 600$ bits ✓

$P_d = \frac{d}{V}$

$P_d = \frac{90 \text{ Km.}}{3 \times 10^5 \text{ Km/sec}}$

$P_d = 30 \times 10^{-5}$ 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. $Np(1-p)^{n-1}$.

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 $S_1 = 0.1$, $S_2 = 0.2$, $S_3 = 0.3$, $S_4 = 0.4$

$P_{succ} = N \cdot p(1-p)^{N-1}$

Explaination continued

P.T.O!

	S1	S2	S3	S4	
For S1	p	(1-p)	(1-p)	(1-p)	
	0.1	0.8	0.7	0.6	= 0.0336
					+
For S2	(1-p)	p	(1-p)	(1-p)	
	0.9	0.2	0.7	0.6	= 0.0756
					+
For S3	(1-p)	(1-p)	p	(1-p)	
	0.9	0.8	0.3	0.6	= 0.1296
					+
For S4	(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 No. of host (N) = 3

each host can transmitting probability (P) = 0.8

Probability that one host transmit data in an idle slot

(Throughput of the channel) $= N \cdot p(1-p)^{N-1}$

$= 0.3 \times 0.8 (0.2)^2$

$= 0.3 \times 0.8 \times 0.2 \times 0.2$

$= \underline{0.096}$

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 is ______

Ans Each host can transmit data in a idle host (P) = 0.75

Total no. of host in LAN = N

Probability that particular host only transmit in an idle slot (throughput of host) = 0.1875.

Throughput of the host = $p(1-p)^{N-1}$

$0.1875 = 0.75 \times (0.25)^{N-1}$

$\boxed{N=2}$

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 data to send and transmits 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 transmissions are unsuccessful due to collision. 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. $p = 0.2$

No of host = N

Throughput of host = 0.16

Throughput of the host = $p(1-p)^{N-1}$

$0.16 = 0.2(0.8)^{N-1}$

$0.8 = (0.8)^{N-1}$

$(0.8)^1 = (0.8)^{N-1}$

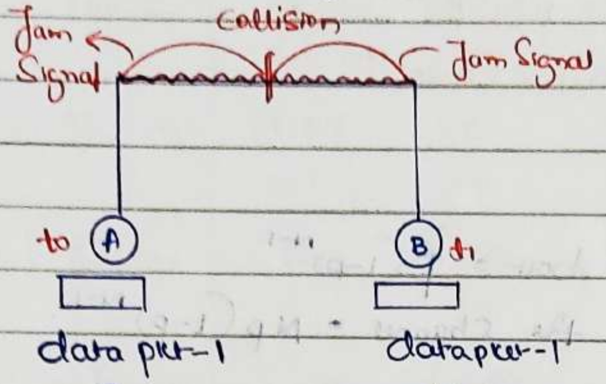
$N-1 = 1$

$\boxed{N=2}$

Q8. Suppose two nodes, A and B are attached to opposite ends of the cable with propagation delay of 12.5 μsec. Both nodes attempt to transmit at time t=0. Frames collide and after first collision, A draws K=0 and B draws K=1 in the exponential backoff protocol. At what time (in μ seconds) is A's packet completely delivered at B, if bandwidth of the link is 10Mbps and packet size is 1000 bits for the following:

(a) With purging ____ μsec. (b) Without purging ____ μsec.

Concept of Purging (cleaning)



$n=1$ | $n=1$

$K \rightarrow 0$ to 2^1-1 | $K \rightarrow 0$ to 2^1-1

$K \rightarrow (0,1)$ | $K \rightarrow (0,1)$

A	B	
0	0	→ collision
0	1	→ A won
1	0	→ B won
1	1	→ collision

If we choose $\overset{A\ B}{(\underset{K}{0},\underset{K}{1})}$

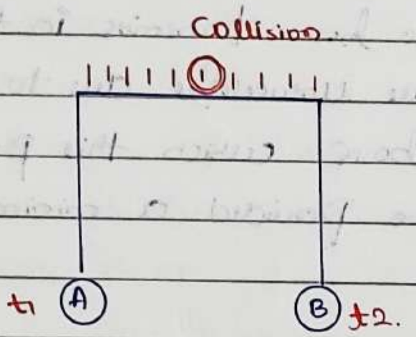
WT of A = K * slot duration

WT of A = 0 × slot duration

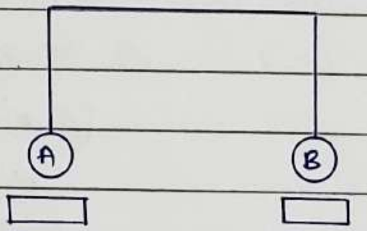
WT of A = 0

WT of B = K * slot duration

= 1 * slot duration.



Concept of Purging (cleaning)



pkt-1 | pkt-1

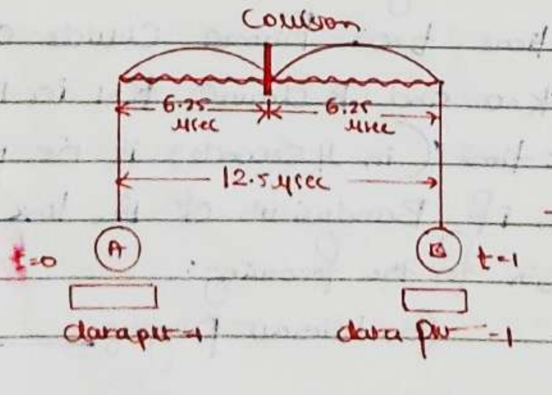
K=0 | K=1

$\boxed{\text{WT of A} = Pd}$

WT of B = K * slot duration

= 1 * slot duration

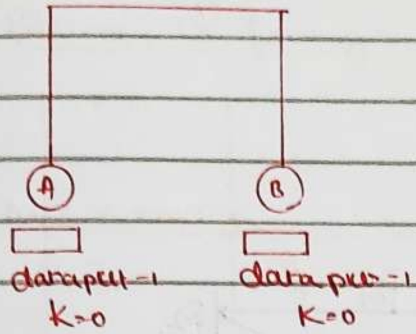
Ans 8th.



→ At t=0 both A&B start transmitting the data pkt.

→ At t=6.25 both A&B datapkt has been colided

→ At t=12.5 both recieved collision signal



WT = Pd

$\boxed{WT = 12.5\mu sec}$ → A can't immediately go, has to wait for one propagat. delay.

$t = 12.5\mu sec + 12.5\mu sec = 25\mu sec$

At $t = 25\mu sec$ A start retransmitting the data pkt.

Pkt size = 1000, $B = 10 \times 10^6$ bit/sec

$$Td(pkt) = \frac{1000 \text{ bit}}{10 \times 10^6 \text{ bit/sec}}$$

$$= 100 \times 10^{-6} \text{ sec} = 100\mu sec$$

At $t = 25\mu sec + 100\mu sec = 125\mu sec$

At $t = 125\mu sec$.

A complete its transmission.

→ At $t = 125\mu sec + 12.5\mu sec = 137.5\mu sec$. A's packet completely delivered to B

Controlled Access Protocols

It can be done in the following two ways:

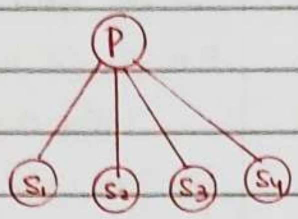
1. We have a concept of primary and secondary station. Primary station will control all secondary station.
2. If concept of primary or secondary station is missing then if any station want to send the data, it can send only in a case if all other station gives permission to it.

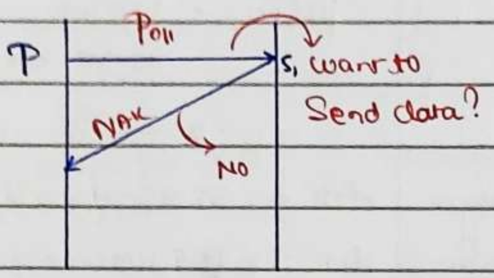
Note: Controlled access protocols are collision free protocol.

Controlled Access Protocols

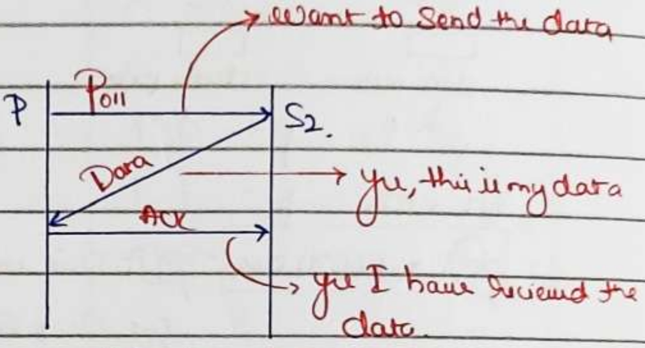
- Polling
- Reservation
- Token Passing

Polling:



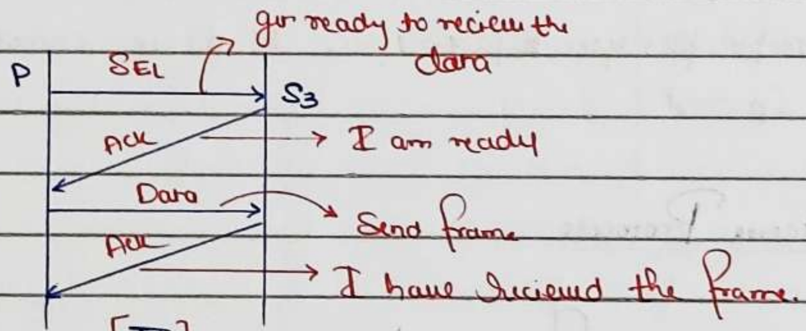


[I.]



[II.]

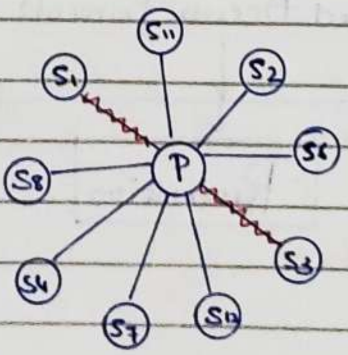
$\boxed{S_2 \rightarrow S_3}$



[III]

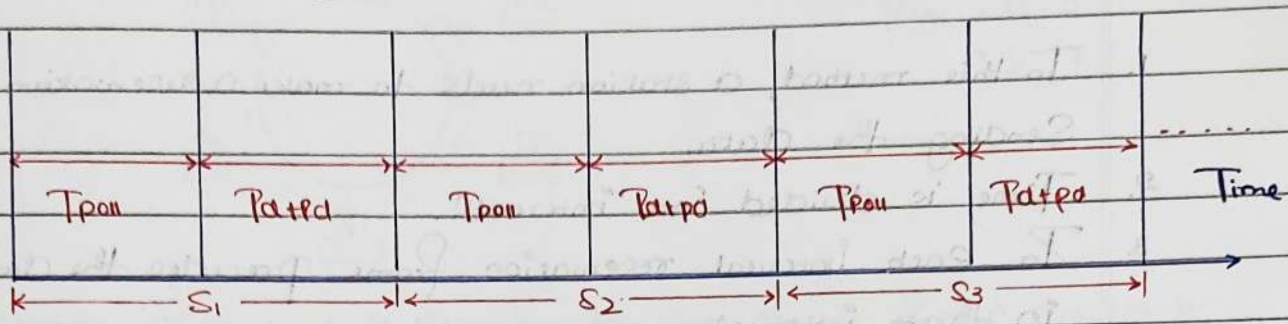
Note:

* Every station will send the data through primary station.
* Two secondary station cannot communicate directly.
* Common topology used in polling mechanism is star topology.
* Bandwidth utilization is low because lots of time is wasted by sending the poll message.
* Drawback of Polling is if primary station fails, the system goes down.



$\boxed{S_1 \rightarrow S_4}$

Efficiency of polling:



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

$$\boxed{\text{Throughput} = \eta \times B.}$$

$$\boxed{\text{efficiency} = \frac{T_d}{T_{poll} + T_d + p_d}}$$

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 μs to poll the next node. Whenever a node is polled, it is allowed to transmit a maximum of 1000 bytes. The maximum throughput of the broadcast channel is:

Ans.
$B = 10\ \text{Mbps}$

$T_{poll} = 80\ \mu\text{sec}$

Frame size $= 1000$ Byte

$$T_d = \frac{\text{Frame Size}}{\text{Bandwidth}} = \frac{8000\ \text{bits}}{10 \times 10^6\ \text{bits/sec}} = 800 \times 10^{-6}\ \text{Sec} = \underline{\underline{800\ \mu\text{sec}}}$$

$$\eta = \frac{\text{useful time}}{\text{total time}} = \frac{T_d}{T_{poll} + T_d + \cancel{P_d}_0}$$

$$= \frac{800\ \mu\text{sec}}{80\ \mu\text{sec} + 800\ \mu\text{sec}}$$

$$= \frac{\cancel{800}^{10}\ \mu\text{sec}}{{}_{11}\cancel{880}\ \mu\text{sec}} = \frac{10}{11}.$$

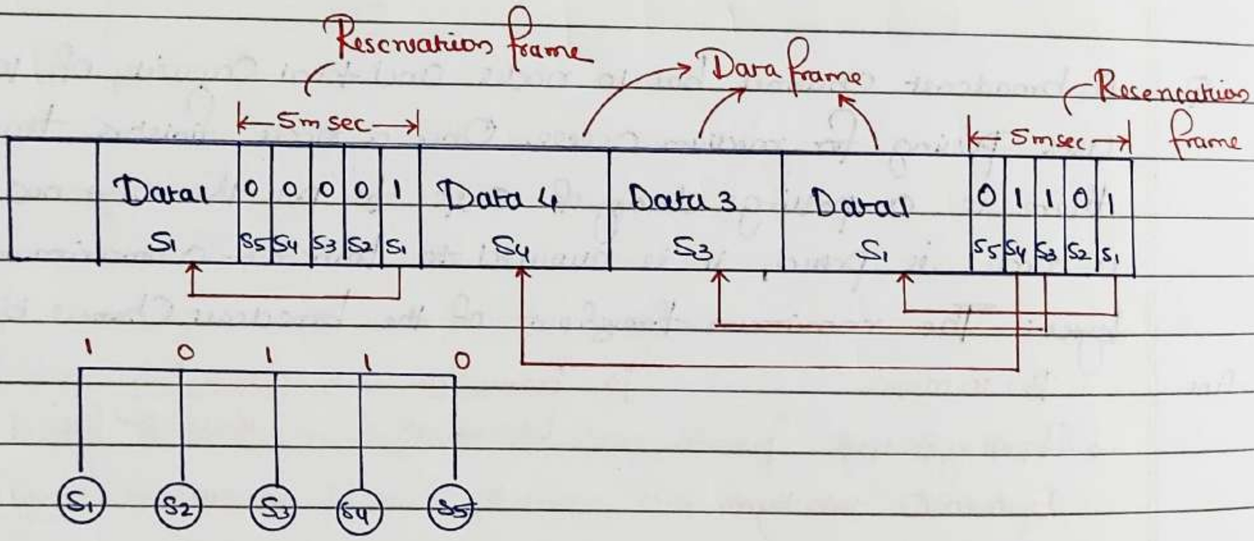
Throughput $: \eta \times B$

$$= \frac{10}{11} \times 10\ \text{Mbps}$$

$$\Rightarrow \underline{\underline{\frac{100}{11}\ \text{Mbps}}}$$

Reservation:

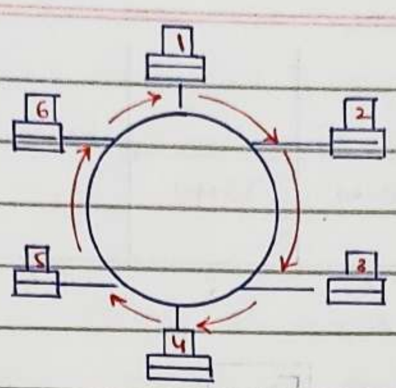
1. In this method, a station needs to make a reservation before sending the data.
2. Time is divided into intervals.
3. In each interval reservation frame precedes the data frames sent in that interval.
4. If there are N stations in the system, there are exactly N reservation minislots in the reservation frame. Means every station have its own minislot.
5. The station 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 tokens.
4. Whenever Station has no more data to send, it release the token.

Note:

* Best technique for broadcasting.
* No acknowledgement.

Channelization Protocols

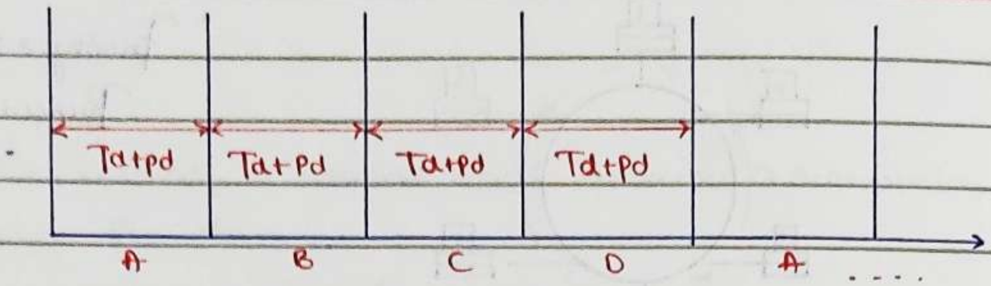
Centralised Access Protocols

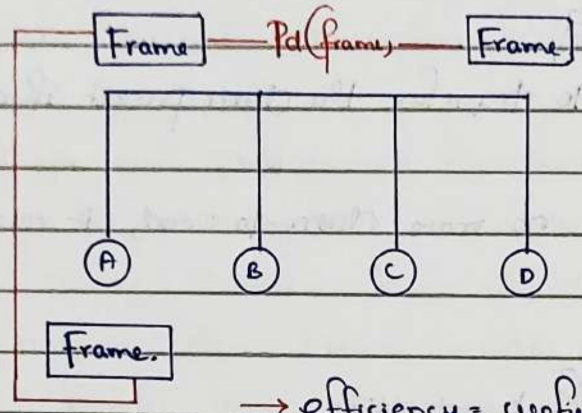
- TDMA ✓
- FDMA ✗
- CDMA ✗ ← not in syllabus.

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 transmit it's data during the time slot allocated to it.
* In case, Station does not have any data to send, it's time slot goes waste.





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

$$\boxed{\therefore \text{efficiency} = \frac{Td}{Td + Pd}} = \frac{Td}{Td\left[1 + \frac{Pd}{Td}\right]}$$

$$\boxed{\eta = \frac{1}{1+a}} \qquad \left\{ \frac{Pd}{Td} = a. \right.$$

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

Throughput = Effenciency * Bandwidth

* Maximum available effective bandwidth (throughput)
  = Total no. of Stations * Bandwidth requirement of 1 station.

Q1. If transmission delay and propogation delay of a packet in TDMA Time division multiplexing is 1msec each at 8mbps bandwidth, then,

(i) What is the efficiency?

(ii) Find the effective bandwidth/throughput?

(iii) How many maximum stations can be connected to the network if each station requires 4kbps bandwidth?

Ans. $Td = 1\,msec$

$Pd = 1\,sec$

$B = 8\,mbps = 8 \times 10^6$ bit/sec

$\eta = \frac{Pd}{Td + Pd} = \frac{1}{1+1} = \frac{1}{2}$

$\therefore \eta = 50\%$ (i)

(ii) Throughput $= \eta \times B$

$= \frac{1}{\cancel{2}} \times \cancel{8}^{4}$

$= 4\,mbps$.

(iii) $N \times 4kbps = 4mbps$

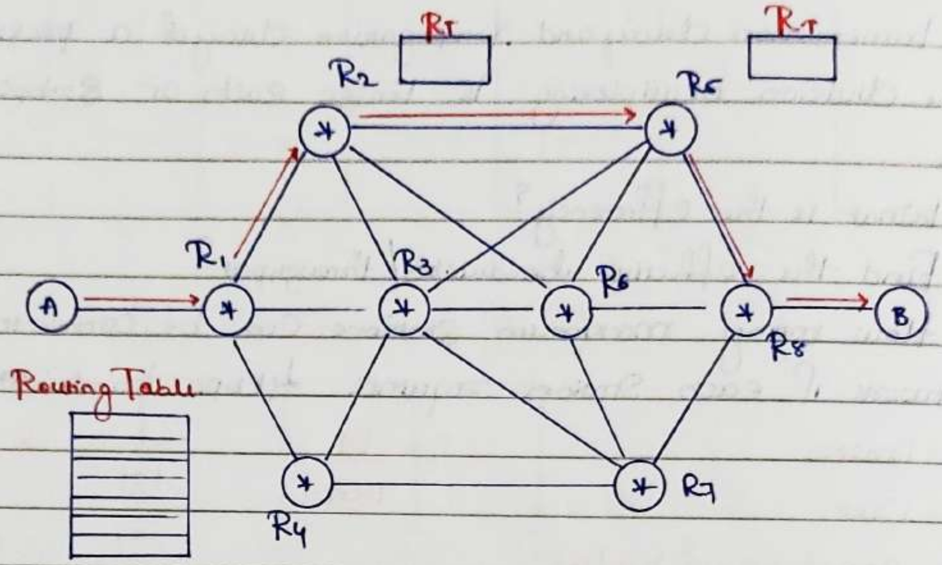
$N = \frac{4mbps}{4kbps}$

$N = \frac{10^6}{10^3} = 1000$

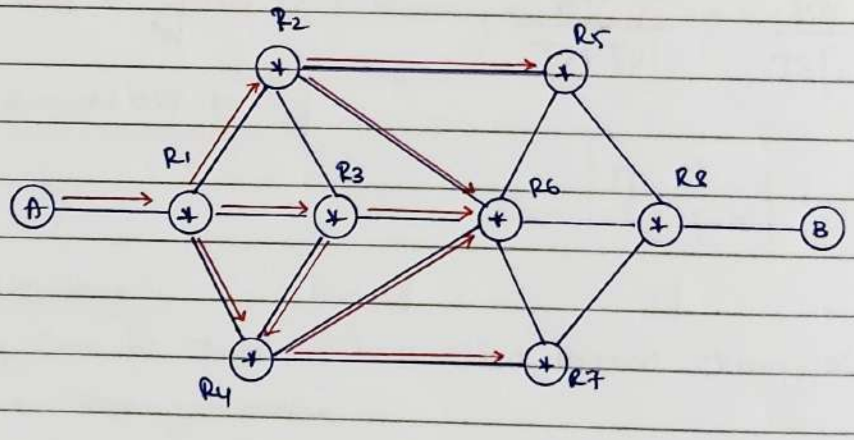
$\therefore N = 1000$ Stations

Date 6/7/23

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 gurantee i.e the packet arrives at destination first.
* It is highly reliable, if one path is down then the packet reach at the destination by choosing another path:

Disadvantages:
* Traffic is very high
* Many duplicates Packets recieved by reciever.

Advantages of Routing:

* Traffic is very less.
* No duplicate packet recieved by the reciever.

Disadvantage of Routing:

* Routing table is required
* Choosen path may be down so it is not highly reliable.
* Shortest path is depends on the algorithm and some algorithms
* fails to find the shortest path.

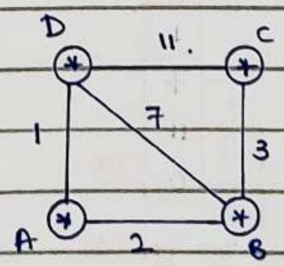
Routing Algorithm
- Static
- Dynamic
  - Distance vector Routing
  - Link State Routing

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	Dist	NH
A	1	A
B	7	B
C	4	C
D	0	D



Dest	Dist	NH
A	∞	—
B	3	B
C	0	C
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 :

At A

A recieved distance vector from B, D

From B	From D
2	1
0	7
3	11
7	0
AB = 2	AD = 1.

$A \rightarrow B = \min \begin{cases} A \xrightarrow{2} B + B \xrightarrow{0} B \\ \text{or} \\ A \xrightarrow{1} D + D \xrightarrow{7} B \end{cases}$

$A \rightarrow B = \min(2, 8) = 2.$

$A \rightarrow C = \min \begin{cases} A \xrightarrow{2} B + B \xrightarrow{3} C \\ \text{or} \\ A \xrightarrow{1} D + D \xrightarrow{11} C \end{cases}$

$A \rightarrow C = \min(5, 12) = 5$

$A \rightarrow D = \min \begin{cases} A \xrightarrow{2} B + B \xrightarrow{7} D \\ \text{or} \\ A \xrightarrow{1} D + D \xrightarrow{0} D \end{cases}$

$A \rightarrow D = \min(9, 1) = 1$

A — new Routing table.

Destination	Distance	NH
A	0	A
B	2	B
C	5	B
D	1	D

Shortcut (AD Rule)

At A : A recieved distance vector from B, D.

From-B	From-D
2	1
0	7
3	11
7	0

AB = 2

0+2 = 2

3+2 = 5

7+2 = 9.

AD = 1.

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

At B

B recieved distance vector from A, C, D

From-A	From-C	From-D
0	∞	1
2	3	7
∞	0	11
1	11	0
BA = 2	BC = 3	BD = 7.

0+2=2	∞+3=∞	1+7=8
∞+2=∞.	0+3=3	11+7=18
1+2=3	11+3=14.	0+7=7

B – New Routing Table

Destination	Distance	NH
A	2	A
B	0	B
C	3	C
D	3	A

At C: New Routing Table

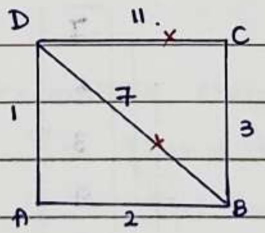
Destination	Dist	NH
A	5	B
B	3	B
C	0	C
D	10	B

At 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	6	A
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"

D —11— C ×

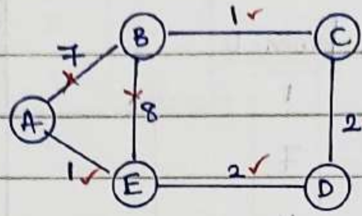
D —7— B ×

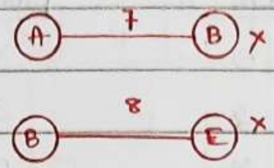
Dest.	Dist.	NH
A	0	A
B	2	B
C	5	B
D	1	D

Dest.	Dist.	NH
A	2	A
B	0	B
C	3	C
D	3	A

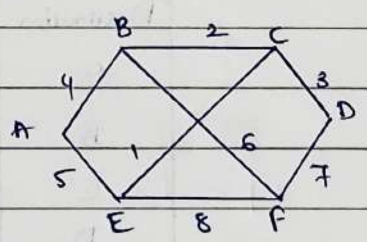
Date 07/7/23
Page

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 Recieved Distance Vector from B, D, E.

From - B	From D	From - E
5	16	7
0	12	6
8	6	3
12	0	9
6	9	0
2	10	4

CB = 6
5+6 = 11
0+6 = 6
12+6 = 18
6+6 = 12
2+6 = 8.

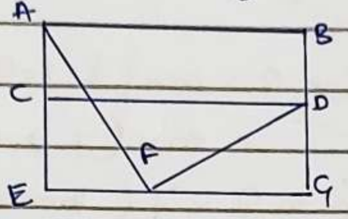
CD = 3
16+3 = 19
12+3 = 15
0+3 = 3
9+3 = 12
10+3 = 13.

CE = 5
7+5 = 12
6+5 = 11
9+5 = 14
0+5 = 5
4+5 = 9

C - New Routing Table

Destination	Distance	NH
A	11	B
B	6	B
C	0	C
D	3	D
E	5	E
F	8	B

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 it's delay to it's neighbours A, E, D and G as 8, 10, 12, and 6 msec respectively and update it's routing table using distance vector routing technique. New Routing table for F?



Ans. <u>At F</u>

F recieved Distance Vector from A, D, E, G

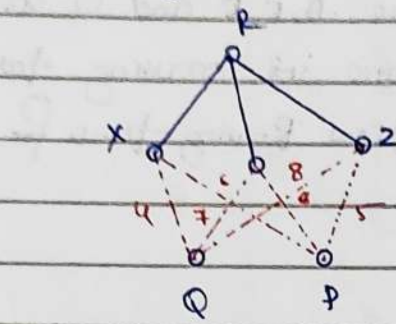
From-A	From-D	From-E	From-G
0	20	24	21
140	8	27	24
14	30	7	22
7	0	20	19
21	14	0	22
9	7	11	10
24	22	22	0
FA = 8	FD = 12	FE = 10	FG = 6
0+8 = 8	20+12 = 32	24+10 = 34	21+6 = 27
40+8 = 48	8+12 = 20	27+10 = 37	24+6 = 30

F → New Routing Table

Destination	Distance	NH
A	8	A
B	20	D
C		
D		
E		
F	0	F
G		

Q4. Consider a computer network using the distance vector routing algorithm in its network layer. The partial topology of the network is as 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 it's distance to it's neighbours X, Y, and Z as 3, 2, and 5 respectively. Router R gets routing vectors from it's neighbours that indicate that the distance to router P from routers X, Y and Z are 7, 6 and 5 respectively.

Ans



[I.] R to P = min{R-X-P, R-Y-P, R-Z-P}
= min (10, 8, 10)
R to P = 8 (Through Y)

[II] R to Q = min{R-X-Q, R-Y-Q, R-Z-Q}
= min (7, 18, 13)
R to Q = 7 (Through X)

Qs The routing vector also indicates 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.

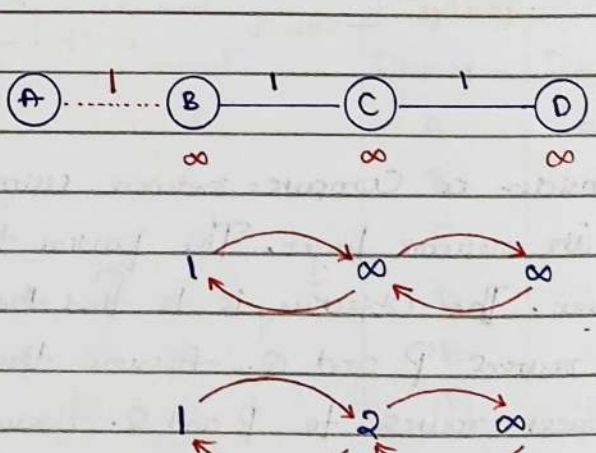
<u>Disadvantage of DVR</u> [Count to infinity problem]

Bad news spreads slow

Good news spreads fast.

<u>Good News.</u>

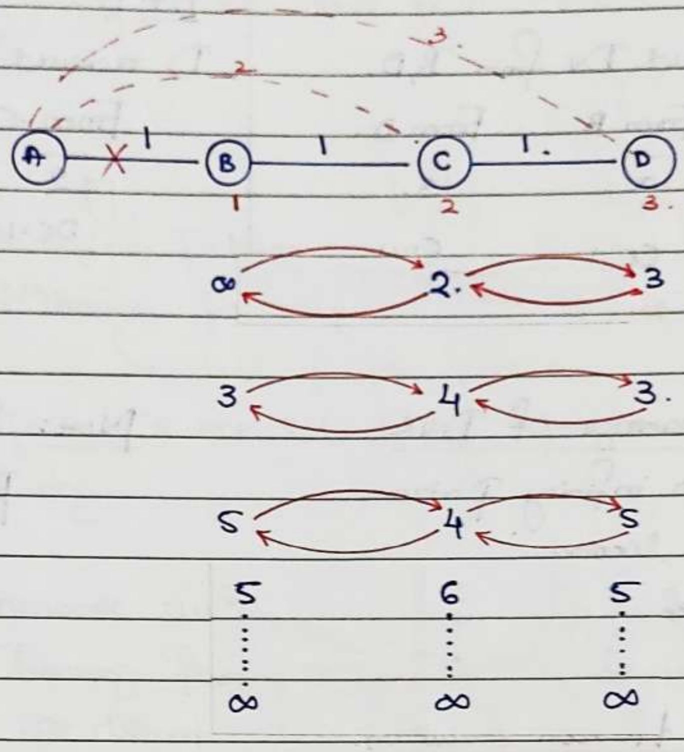
Initially A is not connected to B so
B to A = ∞
C to A = ∞
D to A = ∞



* After sometime A is connected to B with the cost (1).

1 2 3
(Good News)

Bad News

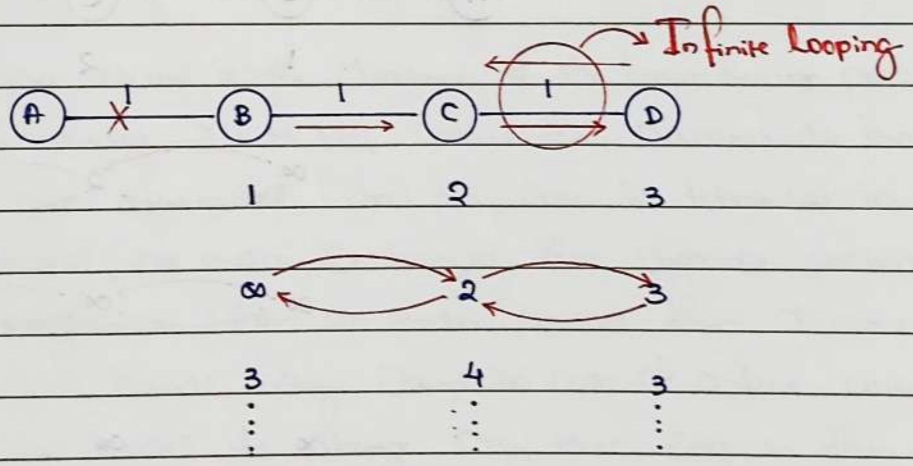


"Count to infinity" Problem!

Dest	Dis	NH
A	~~1~~ ~~∞~~ 3	~~A~~ C

Dest	Dist	NH
A	~~2~~ 4	B D

Dest.	Dist	NH
A	3	C



Note:

~~At B~~

B recieved distance vector from - C.

Dest	Dist.	NH
A	~~1~~ ~~∞~~ 3	~~A~~ C

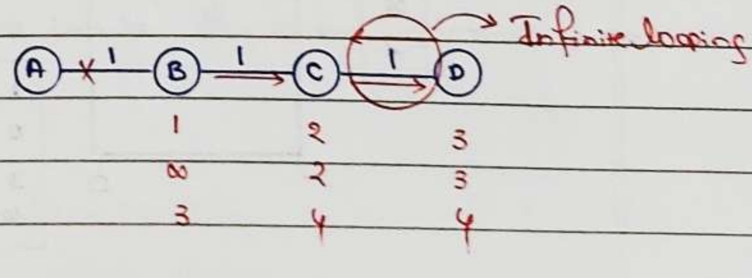
Dest	Dist	NH
A	~~2~~ 4	B D

Dest	Dist	NH
A	3	C

From C

$\boxed{2}$ BC=1

2+1=3



At C

C recieved DV from B, D.

From B: $\boxed{\infty}$, CB=1, ∞+1 = ∞

From D: $\boxed{3}$, CD=1, 3+1 = 4.

At D

D recieved from C.

From-C: $\boxed{2}$, DC=1, 2+1 = 3

Disadvantage of DVR

* Count to infinity problem
* Infinite looping
* Convergence is very slow.

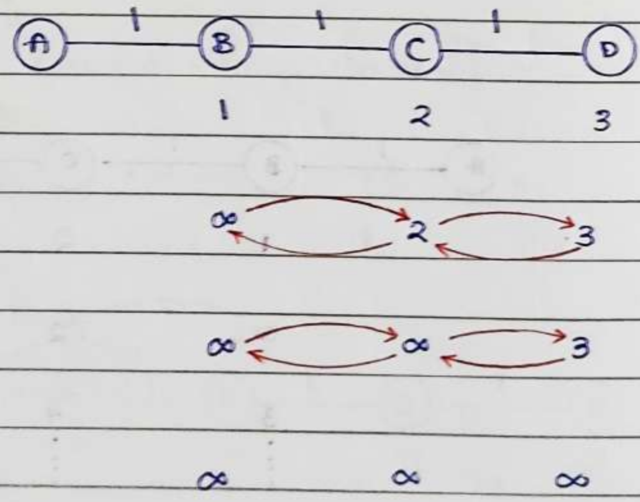
Note: Solution of count to infinity problem is given by Split Horizon.

Split Horizon Solution.

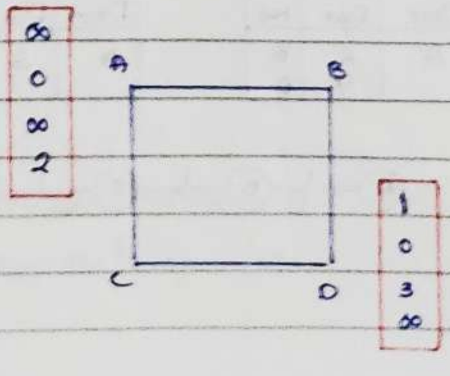
Dest	Dis	NH
A	~~1~~ ∞	A —

Des.	Dis.	NH
A	2	B

Dest.	Dis	NH
A	3	C



Q.1.



Routing Table of B.

Dest	Dis	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 routes have stabilized the distance vectors at different nodes are as follows:

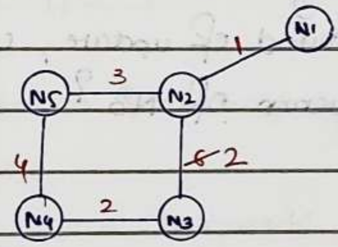
N1: (0,1,7,8,4)

N2: ($\overset{\infty}{1}$, 0, $\overset{2}{\cancel{6}}$, 7, 3)

N3: (7, $\overset{2}{\cancel{6}}$, 0, 2, 6)

N4: (8, 7, 2, 0, 4)

N5: (4, 3, 6, 4, 0)



Each distance vector is the distance of the best known path at the instance to nodes, 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 neighbours. Then all nodes update their distance vectors. 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 reduces to 2 (in both directions). After the next round of update, what will be the next distance vector at node, N3?

Ans. At N3

N3 received distance vector from N2, N4.

From - N2

1
0
2
7
3

N3N2 = 2

1+2=3

0+2=2

7+2=9

3+2=5.

From - N4

8
7
2
0
4

N3N4 = 2

8+2=10

7+2=9

0+2=2

4+2=6

N3 New Routing Table

Dest.	Dist	NH
N1	3	N2
N2	2	N2
N3	0	N3
N4	2	N4
N5	5	N2

$\therefore$ (3, 2, 0, 2, 5)

#Q. After the update in the previous question, the link N1-N2 goes down. N2 will reflect this change immediately in its distance vector as cost, ∞. After the next round of update, what will be the cost to N1 in the distance vector of N3?

At N3

N3 Recieved DV from N2, N4

From N2

∞
0
2
7
3.

N3N2 = 2

∞+2 = ∞

From N4

8
7
2
0
4

N3N4 = 2

8+2=10

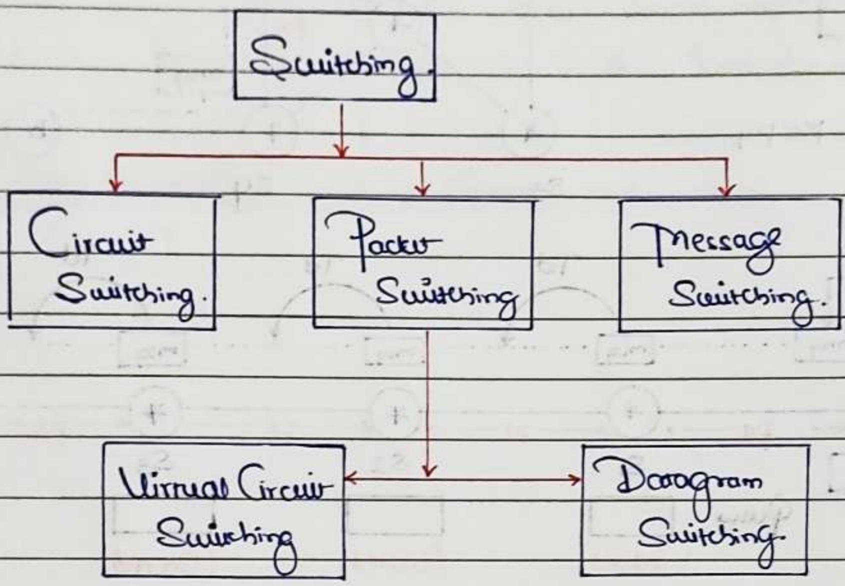
N3 – New Routing Table

Destin.	Dist.	NH
N1	10	N4
N2		
N3	0	N3
N4		
N5		

$\therefore$ Ans = 10.

SWITCHING.

Switching: The Process of forwarding Packets from one port to another port is called switching.

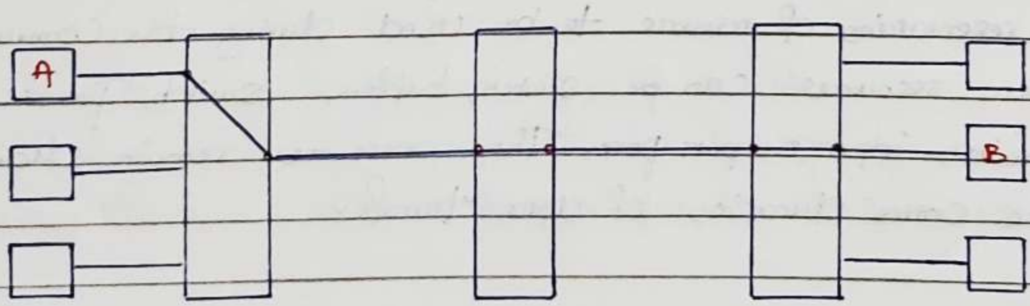


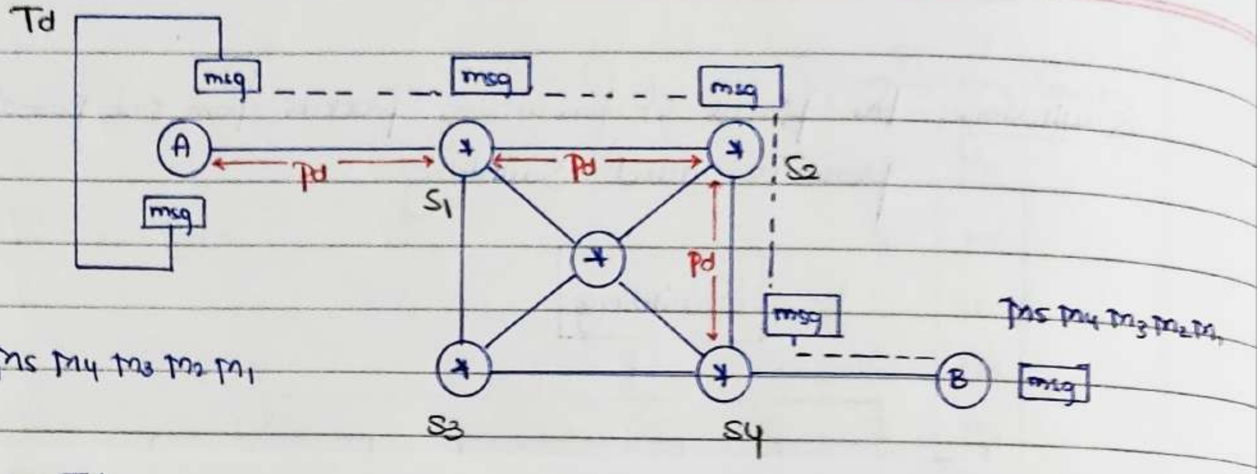
* Switching is done at Network layer but circuit switching is not done at Network Layer.
* Circuit Switching was designed for telephone network.
* When Circuit Switching was invented there was no Concept of OSI layer or TCP/IP layer.

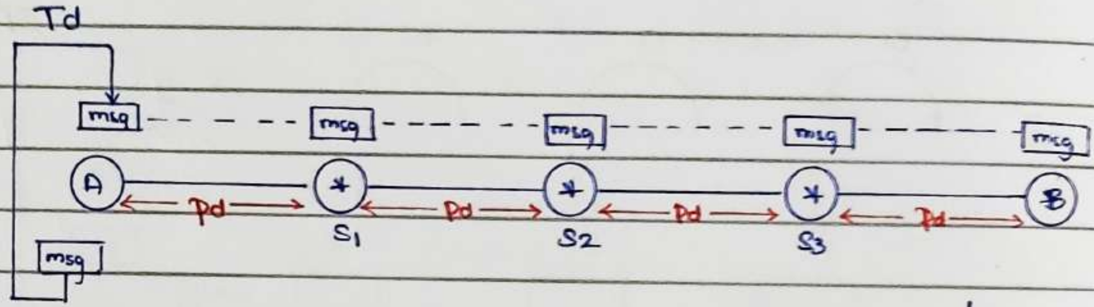
Circuit Switching:

The communication in a circuit Switched network take place in 3 phase:

1. Circuit establishment or setup phase
2. Data transfer phase
3. Circuit disconnection or teardown Phase







Total time taken to send msg from source to destination
⇒ Setup time + Transmission time + Propagation time + Tear down time

$$\boxed{\text{Total time} = S + \frac{m}{B} + x \cdot \frac{d}{v} + T}$$

Msg size = m
Bandwidth = B
Velocity = v
No of hops = x
Length of each hop = d

(1.) 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 reciever.
* The dedicated path establish between sender and reciever is maintained for entire duration of conversation.
* Before starting the conversation/communication the station must make a reservation of resource to be used during the communication.
* These resources can be switch, buffers, switch processing time, switch input output port. These resources remain dedicated during the entire duration of data transfer.

classmate

Date

Page

(2.) Data Transper Phase:

* After the Circuit is established, the entire data travels over the
* dedicated path from sender to reciever.
* The data flows are continous b/w sender and reciever.
* There is no addressing involved in the data transfer ie 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 switch
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 reciever 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.
* Dedidcated Channel required 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

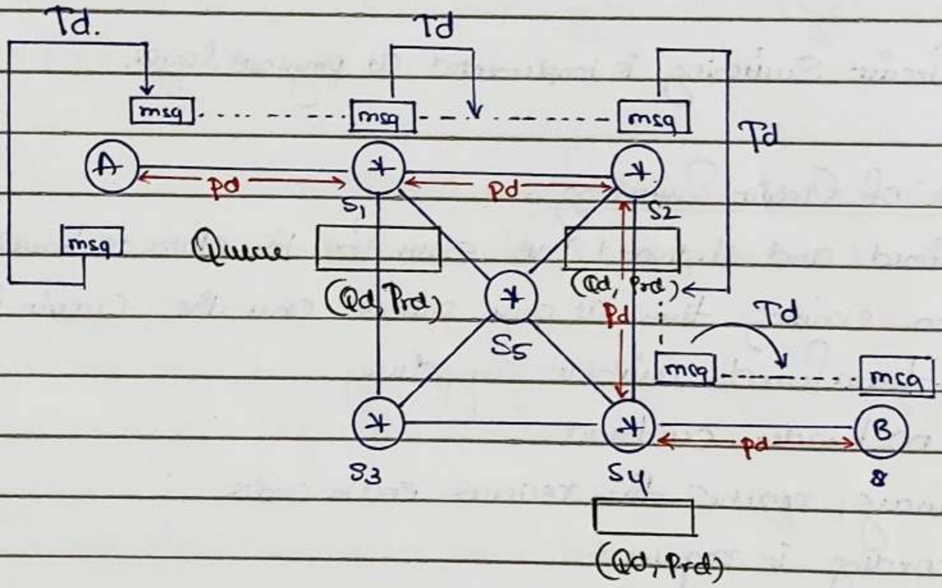
Q1. Consider a circuit switched network. The circuit setup time is 's' sec, the propogation delay is 'd' sec per hop, and the data rate is 'b' bps. What is the delay in sending an x bit message over a k-hop path?

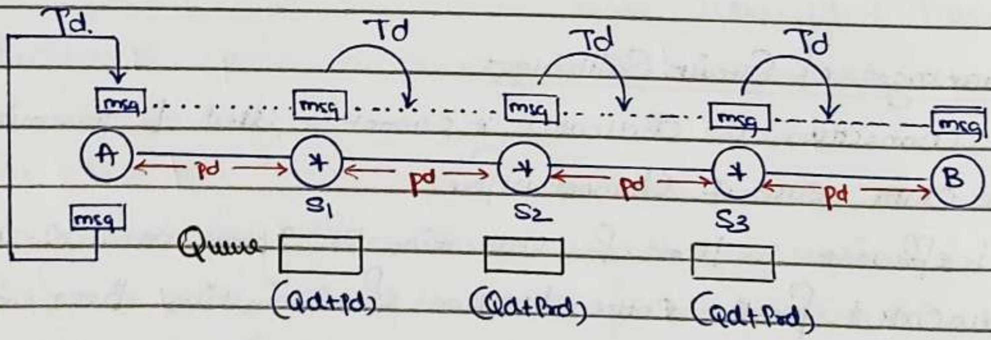
Ans. Circuit Switching

Total time = $S + TT + PT + \cancel{P}^{0}$

→ Total time = $\underline{S + \frac{x}{b} + kd}$

Packet Switching.





Msg size = m

Bandwidth = B

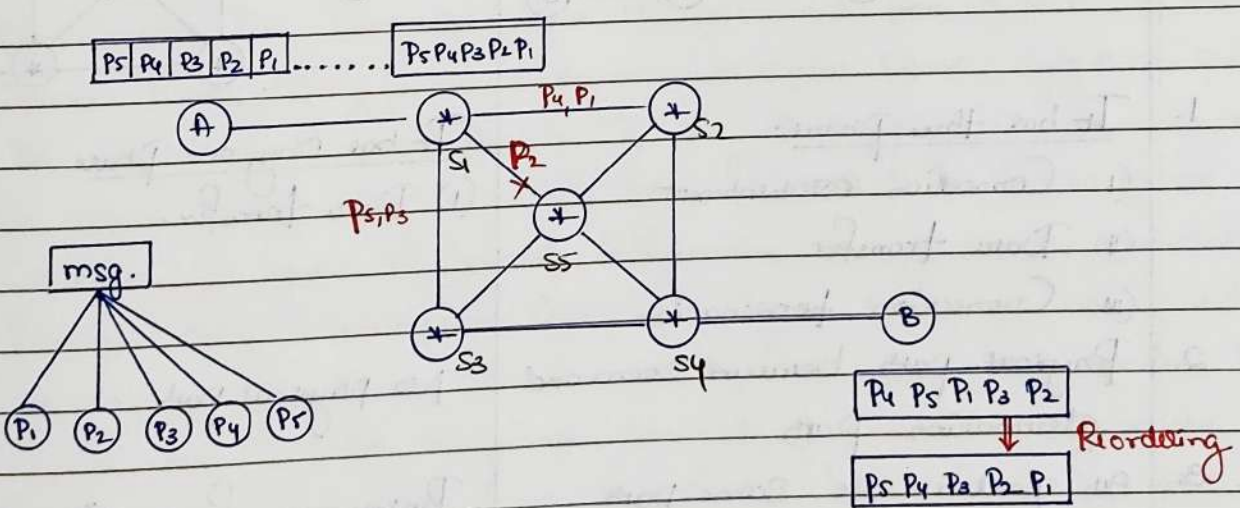
No. of hops = x

length of each hop = d.

Total time = Transmission time + Propogation time + Queuing delay + Processing delay.

$$\boxed{\text{Total time} = x \cdot \frac{m}{B} + x \cdot \frac{d}{v} + x-1\,(Qd - Pd)}$$

* 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 has 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 packets 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.

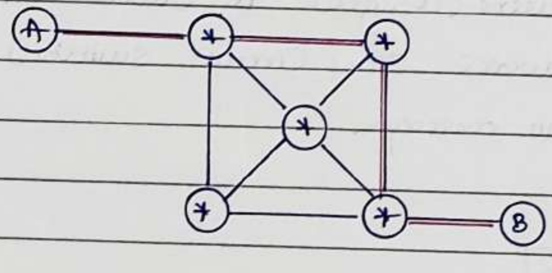
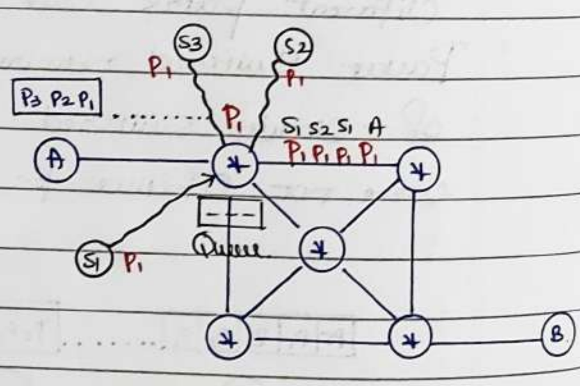


Advantages of Packet Switching
* More fault tolerant because packets may follow different path in case link down
* There is no setup or teardown phase.
* Efficiency of packet switching is better than that of circuit switching

* More reliable as destination can detect the missing packet.
* Cost effective and comparatively cheaper to implement.

Disadvantages 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 un-ordered, we need to provide sequence numbers for each packet.
* Transmission delay is more in packet switching.
* Packet switching is benificial only for small messages, but for large messages circuit switching is better.

	Circuit Switching	Packet Switching
		
1.	It has three phase: (I) Connection establishment (II) Data transfer (III) Connection termination	It has only one phase (1) Data transfer.
2.	Physical path between source and destination pass	No physical path
3.	All packets use same path	Packet may follow different path (travel independently)
4.	Reserve the entire bandwidth in advance	Does not reserve.
5.	Bandwidth wastage	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

Packetization in Packet Switching:

* The process of dividing a single message into smaller size packet is called as Packetization.
* 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 bytes/sec. A user on host A sends a file of size 10^3 bytes to host B through routers R_1 and R_2 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 bytes of header information along with the user data. Consider only transmission time and ignore processing, queuing and processing delays. Assume that there are no errors during transmission. Let T_1, T_2 and T_3 be the times taken to transmit the file in the first, second and third case respectively. Which of the following is correct?

No. of hops $(x) = 3$.

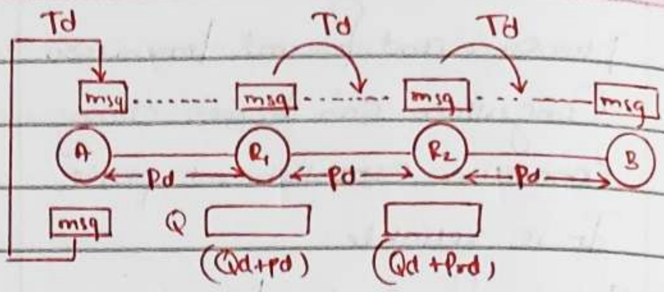
Ans. $B = 10^6$ Byte/sec

A — R_1 — R_2 — B

File size = 10^3 Bytes = 1000 Bytes

Header Size = 100 Byte

Case I



Packet size = Data + Header

= 1000 B + 100 B = 1100 B

$Td(pkt) = \frac{\text{pkt size}}{\text{bandwidth}} = \frac{1100 \text{ byte}}{10^6 \text{ byte/sec}}$

$= 11 \times 10^{-4}$ sec

= 1.1 msec

Total time = $x.Td + x.\cancel{pd} + (x-1)[\cancel{Qd} + \cancel{pd}]$

$\Rightarrow 3 \times 1.1 = \underline{3.3 \text{ msec}}$ (T_1)

Case II : Sending file in 5 packet.

Data in each packet = $\frac{1000B}{5}$ = 200B.

Header size = 100 Byte

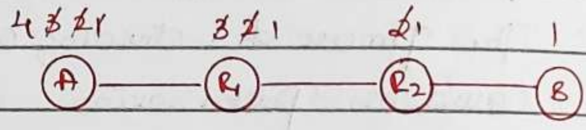
One packet size = Data + Header

= 200 B + 100 B = 300 B.

$Td(pkt) = \frac{\text{Pkt size}}{\text{Bandwidth}} = \frac{300 \text{ Byte}}{10^6 \text{ Byte/sec}}$

$= 3 \times 10^{-4}$ sec $= 0.3 \times 10^{-3}$ sec

= 0.3 msec



Time taken to reach 1^{st} packet from source to destination = 3 * Td = 3 × 0.3 msec

= 0.9 msec

Time taken to reach remaining '4' pkt to reach from source to destination = 4 * Td

= 4 × 0.3 msec = 1.2 msec

Total time = 0.9 msec + 1.2 msec

= 2.1 msec

Case III : Sending file in 10 pkts.

Data in each packet = $\frac{1000B}{10}$ = 100 Byte

Header Size = 100 Byte

One packet Size = data + Header

= 100 B + 100 B = 200 B

$Td(pkt) = \frac{\text{pakt size}}{\text{Bandwidth}} = \frac{200B}{10^6 B/sec}$

$= 2 \times 10^{-4}$ sec $= 0.2 \times 10^{-3}$ sec

= 0.2 msec

Time taken to reach 1^{st} packet from Source to destination = 3 × Td = 3 × 0.2 msec = 0.6 msec

Time taken to reach remaining 9 pkt from Source to destination = 9 × Td = 9 × 0.2

= 1.8 msec

Total time = 0.6 msec + 1.8 msec

= 2.4 msec (T_2)

Case IV : Sending file in 20 pkts.

Data in each packet = $\frac{1000}{20}$ Byte = 50 Byte.

Header size = 100 Byte

One packet size = data + header

$= 50B + 100B = 150 \text{ Byte}.$

$Td(pkt) = \frac{pkt.\ size}{bandwidth} = \frac{150\ B}{10^6\ Byte/sec}$

$= 150 \times 10^{-6} sec = 0.15\ msec$

Time taken to reach 1st packet from Source to destination $= 3 \times Td = 3 \times 0.15 = 0.45\ msec$

Time taken to reach remaining 19 pkt from Source to destination $= 19 \times Td = 19 \times 0.15$

$= 2.85\ msec.$

Total time $= 0.45\ msec + 2.85\ msec$

$= 3.3\ msec\ (T_3)$

⇒

T_1	T_2	T_3
3.3	2.4	3.3

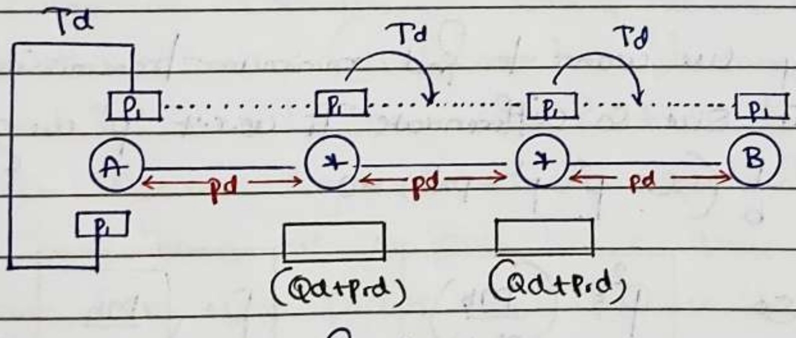
$\boxed{T_1 = T_3 > T_2}$

or

$\boxed{T_2 < T_1 = T_3}$

Case I	Case II	Case III	Case IV	Case V
Single msg	5 pkts	10 pkts	20 pkts	30 pkt
↓	↓	↓	↓	↓
3.3 msec	2.1 msec	2.4 msec	3.3 msec	> 3.3 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

$$\boxed{\text{Total Time} = x[Td + Pd] + x-1[Qd + Prd]}$$

Optimal Packet Size: If the packet size is not choosen 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
h = header size
p = payload/packet data size
assume bandwidth is 'b' bit/sec
No. of hops = x
Total no. of packets = M/p.

Packet Size $(P) = p+h$.
Capital "P".

* When message is Packetised 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 take transmission delay by all the intermediate nodes and source transmission delay on all hops and rest all packet take only one hop transmission delay due to pipeline).

$$\text{Transmission time } (T_T) = \left(\frac{p+h}{b}\right)x + \left(\frac{M}{p}-1\right)\left(\frac{p+h}{b}\right)$$

$$= \frac{1}{b}\left[(p+h)x + \frac{1}{p}(M-p)(p+h)\right]$$

$T_d(pkt) = \frac{\text{Pkt size}}{\text{Bandwidth}}$
$= x\left(\frac{p+h}{b}\right)$.

So resultantly we want to find minimum transmission delay at Optimal Packet size so differentiate T_T w.r.t 'p' we get

$$\frac{d}{dp}T_T = \frac{1}{b}\left(x * p^2 - p^2 - Mh\right) = 0$$

So $\boxed{p^2 = \left(\frac{Mh}{x-1}\right)}$ $\boxed{p = \sqrt{\frac{Mh}{x-1}}}$

So optimum packet size $\boxed{P = p+h}$

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 <u>9</u>

Classmate

Date 11/7/23

Page

Ans

(S) —— (R1) —— (R2) —— (D), No. of hops = 3.

Message size (m) = 24 byte

Header size = 3 byte

$$p = \sqrt{\frac{mb}{x-1}} = \sqrt{\frac{24 \times 3}{8}}$$

$$= \sqrt{36}$$

$$\underline{p = 6}$$

Packet size (P) = p+h

= 6+3 = $\underline{9}$.

Total no. of packets = $\frac{m}{p} = \frac{24}{6} = 4$

Short solution for $\underline{Q1}$ with the formula:

$$p = \sqrt{\frac{mb}{x-1}} = \sqrt{\frac{1000 \times 100}{3-1}}$$

$$= \sqrt{50000}$$

$$p = 223.6$$

Total no. of packets = $\frac{m}{p} = \frac{1000}{223.6} = 4.47 \simeq \underline{5 \text{ pkts}}$

Q3. Consider a source computer (S) transmitting a file of size 10^6 bits to a destination computer (D) over a network of two routers (R1 and R2) and three links (L1, L2 and L3). L1 connects S to R1, L2 connects R1 and R2 and L3 connects R2 to D. Let each link be of length 100 km. Assume signal travels at a speed of 10^8 m/second. Assume that the link bandwidth on each link is 1 Mbps. Let the file be broken down into 1000 packets each of size 1000 bits. Find the total sum of transmission and propagation delays in transmitting the file from S to D?

Ans. File size = 10^6 bits

x = 3 (no. of hops)

(S) —L_1, d=100km— (R1) —L_2, d=100km— (R2) —L_3, d=100km— (D)

$V = 10^8$ m/s $= 10^5$ km/sec

$B = 1$ Mbps $= 10^6$ bits/sec

No. of packets = 1000 (N)

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

$$T_d = \frac{\text{Pkt size}}{\text{Bandwidth}} = \frac{1000}{10^6 \text{ bits/sec}} = 10^{-3} \text{ sec} = \underline{1 \text{ msec}}$$

$$P_d = \frac{d}{v} = \frac{100 \text{ km}}{10^5 \text{ km/sec}} = 10^{-3} \text{ sec} = \underline{1 \text{ msec}}$$

For 'x' hops and 'N' packet

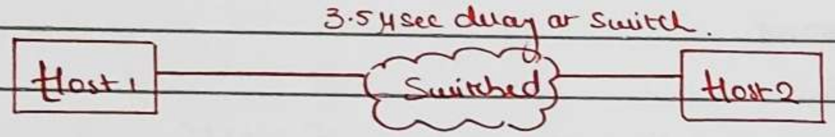
Total time $= x[Td+Pd] + x-1[\cancel{Qd}^{0}+Pd] + N-1(Td)$

$= 3[1+1] + 999\times1$

$= 6 + 999 \Rightarrow \underline{\underline{1005\ msec}}$

Q4 Two hosts are connected via a packet switch with 10^7 bit/second links. Each link has a propagation delay of 20 micro seconds. The switch begins forwarding a packet 35 microseconds after it recieves 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 _____

Ans



$x = 2$.

$B = 10^7$ bit/sec

$Pd = 20\mu sec$.

Packet size = 5000 bit

No. of packet : $(N) = \frac{\cancel{10000}\ \text{bit}}{5000\ \text{bit}} = 2$

$Td(pkt) = \frac{\text{pkt size}}{\text{bandwidth}} = \frac{5000\ \text{bit}}{10^7\ \text{bit/sec}}$

$= 500\times10^{-6}$ sec

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

For 'x' hop & 'N' packet.

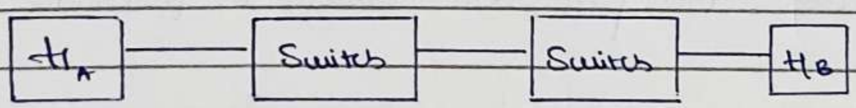
Total time $= x[Td+Pd] + x-1[Qd+Pd]$
$+ (n-1)\ Td$

$= 2(500+20) + 1\times35 + 1\times500$

$= 1000+40+35+500$

$= \underline{\underline{1575\ \mu sec}}$

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 reciever. (Consider for processing overhead at switch is negligible) is __116 msec__.

Ans $P_d = 20\,msec$, $B = 1\,mbps = 10^6\,bits/sec$ No. of packets $(N) = \frac{\cancel{5000}\,B}{\cancel{1000}\,B} = 5$

Packet size = 1000 Byte = 8000 bits

File size = 5000 Byte

$T_d(pkt) = \frac{pkt\ size}{bandwidth} = \frac{8000\,bits}{10^6\,bits/sec}$

$= 8 \times 10^{-3}\,sec$

$= \underline{\underline{8\,msec}}$

Total time $= x(T_d + P_d) + x-1(Q_d + P_{rd}) + (N-1)T_d$

$= 3(8 + 20) + 4 \times 8$

$= 24 + 60 + 32$

$= 84 + 32$

$= \underline{\underline{116\,msec}}$.

Q6. Consider two hosts A and B are connected through two Routers R_1 and R_2

$A \to R_1 \to R_2 \to B$ No. of hops $(x) = 3$

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 Bytes from host A to host B, using packet size 1000 Bytes is $\underline{176\,msec}$.

Ans $P_d = 20\,msec$, $B = 1\,mbps = 10^6\,bits/sec$

$P_{rd} = 2\,msec$

File size = 12000 Byte

Packet size = 1000 Byte

No. of packets $(N) = \frac{12\cancel{000}\,B}{1\cancel{000}\,B} = 12$

$T_d(pkt) = \frac{pkt.\ size}{bandwidth}$

$= \frac{8000\,bits}{10^6\,bits/sec} = 8 \times 10^{-3}\,sec$

$= \underline{\underline{8\,msec}}$

Total time $= x(T_d + P_d) + x-1(\cancel{Q_d}^{0} + P_{rd}) + (N-1)T_d$

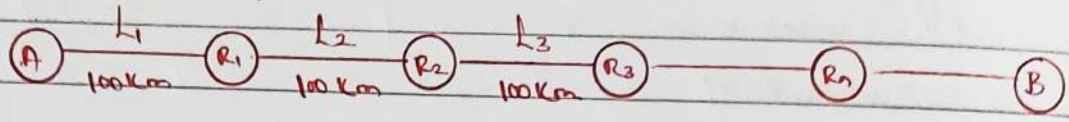
$= 3(8 + 20) + 2(2) + 11 \times 8$

$= 24 + 60 + 4 + 88$

$= \underline{\underline{176\,msec}}$

Q7 Consider a host computer (A) transmitting a file of size 10^5 bits to a host computer (B) over a network of routers $(R_1, R_2 \ldots R_n)$ and links $(L_1, L_2, \ldots L_n)$. L_1 connects A to R_1, L_2 connects R_1 to R_2. L_3 connects R_2 to R_3 and L_n connects R_{n-1} to B. Let each link be of length 100 km. Assume signals 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 bandwidth on each links is 1Mbps. The total sum of Td and Pd in transmitting the file from A to B is 119 msec. Assume y is the no. of routers betw. A and B and x is number of minimum links between A and B then find x+y?

Ans.



$v = 10^8 m/sec = 10^5 km/sec$

No. of packets (N) = 100

Packet size = 1000 bits

$B = 1Mbps = 10^6 bits/sec$

Total time = 119msec.

$Pd = \frac{d}{v} = \frac{100 Km}{10^5 km/sec} = 10^{-3} sec = \underline{1msec}$

$Td(pkt) = \frac{pkt\ size}{bandwidth} = \frac{1000 bits}{10^6 bits/sec} = 10^{-3} sec = \underline{\underline{1msec}}$

For 'x' hops and 'N' packets

$$\text{Total time} = x[Td+Pd] + x-1(Qd+Prd) + (N-1)(Td)$$

$119 = x(1+1) + 99\times1$

$119 = 2x + 99$

$119 - 99 = 2x$

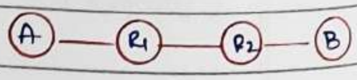
$20 = 2x$

$\boxed{x = 10}$ → 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 = $\underline{x-1}$.

* Substituting $G=1$ in the above equation we get maximum throughput of pure aloha $= 1 \times e^{-1}$

$$= \frac{1}{e} = 0.368$$

$\therefore$ max. throughput of slotted aloha = 36.8%.

Note:

1. If 1000 frames are generated by n/w in one frame transmission time then maximum 368 frames delivered successfully.
2. One frame should be generated in one time slot (one frame transmission time) to achieve maximum throughput.

$$S_{max} \longrightarrow G = 1.$$

3. Vulnerable time t_f is basically representing if one frame is generated by the n/w in one slot time (one frame transmission time) then there will be no collision. So if there is no collision so we will achieve maximum throughput.

eg: A slotted aloha network transmits 200 bit frames on a shared channel of 200 kbps. What is the throughput if the system (all station together) produces:

(i) 1000 Frames generated by n/w in one sec

(ii) 500 " " " "

(iii) 250 " " " "

} thw

Note: Throughput is defined as average no. of frames successfully transmitted per second.

Frame size = 200 bits

$B = 200\text{Kbps} = 200 \times 10^{3}$ bits/sec

Transmission time = $\frac{200 \text{ bit}}{200 \times 10^{-3} \text{ bit/sec}}$

$= 10^{-3}$ sec

$= 1$ msec.

Sol^n (i) 1 sec $\longrightarrow$ 1000 frames

1 msec $\longrightarrow$ 1000×10^{-3} frames

$G = 1$ frame

Throughput $S = G \times e^{-G}$
$S = 1 \times e^{-1}$
$= \frac{1}{e} = 0.368$
$= 36.8\%$

Avg no of frames successfully transmitted per sec = 1000×0.368
$= \underline{368}$

	Pure Aloha	Slotted Aloha.
1.	Any station transmit the data at any time.	Any station can transmit the data at the beginning of any time slot.
2.	Vulnerable time in which collision may occur = $2 \times T_f$.	Vulnerable time in which collision may occur
3.	Throughput of pure aloha = $G \times e^{-2G}$	Throughput of slotted aloha = $G \times e^{-G}$
4.	Max. Throughput $S_{max} = 18.4\%$. (when $G = 1/2$)	Max throughput $S_{max} = 36.8\%$. (when $G = 1$)
5.	The main advantage of pure aloha is simplicity in implementation.	The main advantage is that it reduce the no. of collisions to half and double the throughput of pure aloha.

<u>Random Access Protocols:</u>

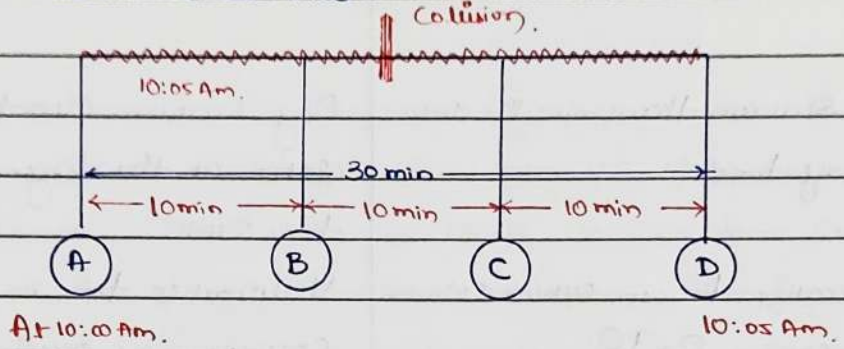
1. Pure Aloha
2. Slotted Aloha
3. CSMA
4. CSMA/CD
5. CSMA/CA

<u>CSMA (Carrier Sense Multiple Access)</u>

* To minimise the chance of collision CSMA method was developed.
* Chances of collision can be reduced if station sense the medium or carrier before trying to use it.
* CSMA requires that each station must sense the carrier before

transmit the data.

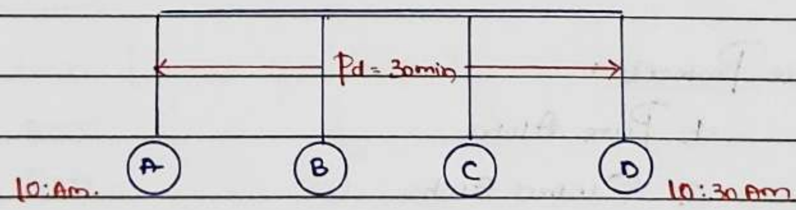
* Each Station Station Can Sense the Carrier Only at its point of contact with Carrier.
* It is not Possible for any Station to sense the entire data Carrier.
* Thus, there is a huge possibility Station might Sense the Carrier free when it is not.



* The possibility of Collision still exists because of propogation delay.
* When a Station Send a frame, it still takes Small amount of time for 1^{st} bit to reach every Station So that Station may Sense the medium and find it idle.

Vulnerable time in CSMA.

Vulnerable time for CSMA = Propogation time.



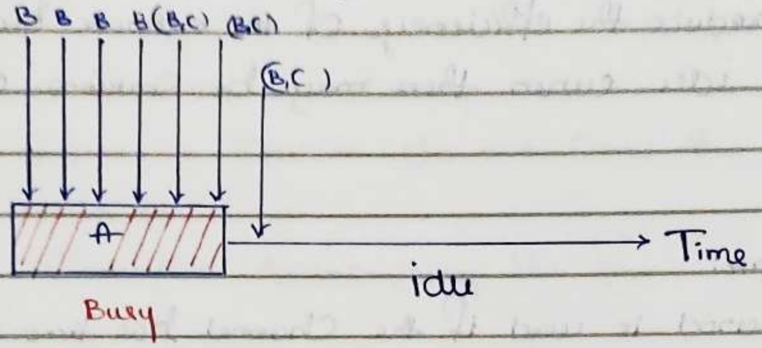
$\boxed{\text{Vulnerable time for CSMA} = Pd}$

* When a Station Send a frame and any other Station try to send a frame during this time, a collision will result.
* But if the first bit of frame reaches the end of medium, every Station will already have heard the bit then Stations will understand that medium is busy.

Persistent Methode In CSMA:

(1.) Persistent CSMA

In case of 1-percistent CSMA station will Continously Sense the Channel and once the Channel is idle. It send it's frame immediately (with probability 1).



* Probability of collision is high for example, if two Station become ready in the middle of the third transmission, both will wait politely until the transmission ends, and then both will begin transmitting exactly Simultaneously then Collision will occur.
* Ethernet LAN uses 1-persistent method.

(2.) Non-persistent CSMA:

In non Persistent CSMA, once the Station is ready with the data It will Sense the Channel, if Channel is busy then it will wait for random amount of time and again Sense the Channel