Computer Networks

Computer Networks(Marks 7 to 9)

- Concept of Layering
  - OSI/TCP Layer
- Physical Layer
  - Encoding, Transmission media(Guided and Unguided) and Modes, Network types & Topologies
- Data link Layer
  - Logical Link(LLC) sublayer
    - Flow control methods(Stop & Wait, Sliding Window:(Go back N, Selective Repeat))
    - Error Control Methods(Parity Check, CRC, Checksum, Hamming Code)
  - Medium Access control(MAC) sublayer
    - Framing (Fixed and Variable length), Bit Stuffing
    - LAN protocols
      - Token Ring
      - Aloha(Pure/Slotted Aloha)
      - CSMA/CD & Exponential Back-off Algorithm
      - Ethernet[IEEE 802.3]
    - Networking Devices (Bridges, Switches, Routers etc.) + Collision/Broadcast domain
- Network Layer
  - IPv4 Addressing
  - IPv4 header
  - Fragmentation
  - IP support protocols (ARP, RARP, BOOTP, DHCP, ICMP)
  - Routing & its protocols
    - Non-Adaptive(Static): Flooding
    - Adaptive: Distance Vector Routing & Link State Routing
  - Switching: (Types -Circuit, Packet(types:Datagram, Virtual Circuit) and Message Switching)
- Transport Layer
  - TCP Header
  - TCP Flow Control
  - TCP Congestion control
    - TCP Timer Management
    - Quality of Service (Traffic Shaping)
  - UDP Header
- Application Layers protocols
  - DNS, E-mail, SMTP, FTP, HTTP

Calculate the sequence no. Properly. Minute difference can change the answer & read the question for no. Of sequence numbers or max sequence number

Use arrows to eliminate silly mistake in CRC and start after 0(Gate 2017 mistake)

Used at University of Hawaii

Use 1/1+6.44a formula for CSMA/CD OR Ethernet Not 1/1+2a to find efficiency

Write Decimal and binary number together to avoid confusion like 224 = 1110 0000

Read MTU properly and check if data segment is divisible by 8 for the OFFSET to work properly

In Token Bucket, I do calculation mistake like 5/3 = 2.66 | 8/5 = 2.66

Top Notorious Topics (Recent/Frequent)

★ Switching PYQ'S Question ★

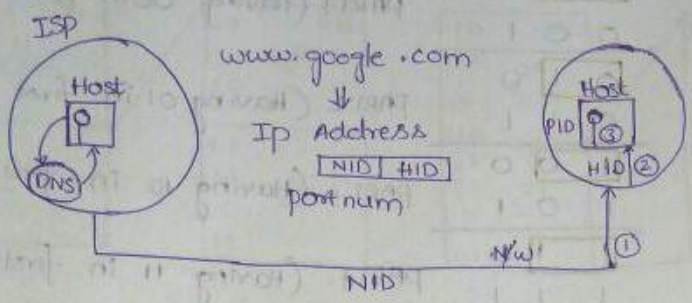
★ IP addressing - Subnets ★

★ Sequence numbers : Read properly ★

★ Token Bucket: Read slowly and understand it ★

COMPUTER NETWORKS

INTRODUCTION TO CN AND IP ADDRESS



⇒ The service that is used to convert the Domain name to Ip Address is called **Domain Name service**

⇒ port number is used to identify a particular process in the host, for well known services the port num are already predefined and fixed

http -> port num = 80 **SMTP port num = 25**

Ftp -> port num = 21

⇒ Eventhough your intention is to reach gogle.com you are visiting DNS first and then getting the Ip Address of google.com and then visiting the google home page. This is actually a overhed which is also called "DNS overhead" so this problem of overhead can be rectified by, when you get the Ip Address of google.com you store it actually on your computer for some time, and if you again want to visit google you can directly get Ip Address from your computer. If your Ip Address in computer expires, there is no another alternative, you have to go to DNS.

Unary = 0

Binary = 0,1

octal = 0,1,2 --- 7

Decimal = 0,1,2 -- 9

Hexa decimal = 0,1,2,--9

A B -- F

10 11 15

$2^1 = 2$

$2^2 = 4$

$2^{10} = 1024 = K$

$M = 2^{20}$

$G = 2^{30}$

$T = 2^{40}$

$K = 2^{10}$

$M = 2^{20}$

$G = 2^{30}$

$T = 2^{40}$

Now, the possible Binary numbers with 1 Bit, 2 Bits, 3 Bits are

1 Bit

0
1

2 Bits

0 0
0 1
1 0
1 1

3 Bits

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

PART 1 (Having 00 in first 2 digits)

PART 2 (Having 01 in first 2 digits)

PART 3 (Having 10 in first 2 digits)

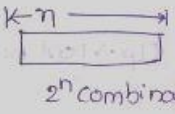
PART 4. (Having 11 in first 2 digits)

⇒ If i choose 1 bit I am going to divide the number space into 2 parts $= 2^1$

⇒ If i choose 2 bits I am going to get 4 parts. $= 2^2$

⇒ If i choose K bits the number space / Address space will be divided into 2^K parts

⇒ So, if i have 'n' bits the no of possible ways are 2^n

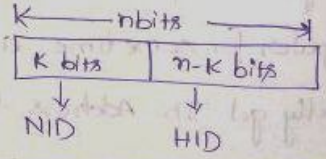


Now, if i choose 'K' bits the entire space will be divided into 2^K parts

⇒ 2^K parts $= 2^n$ numbers

⇒ 1 part $= 2^n / 2^K$ numbers

⇒ 1 part $= 2^{n-K}$ numbers ⇒



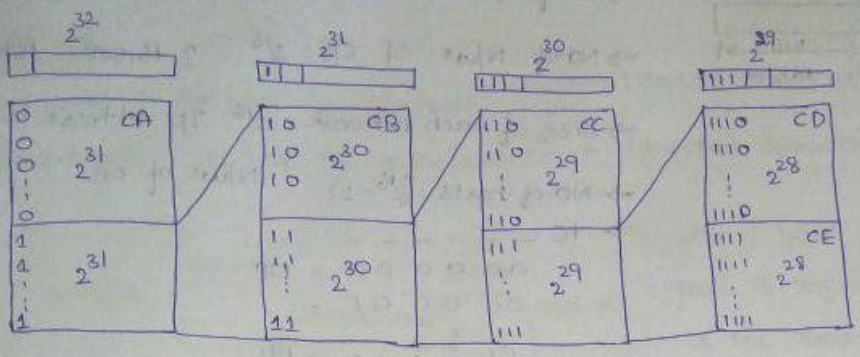
⇒ Size of Each N/w $= 2^{n-K}$

⇒ In operating system 'n' bits = Address, K = page offset / Blk no / Segment no

⇒ In computer Organization 'K' = TAG (n-K) = Block SIZE.

⇒ Ip Address size = 32 bits in CN. ⇒ 2^{32} Ip Address are possible

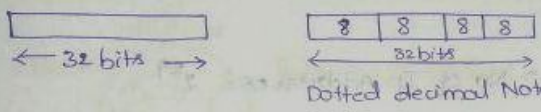
CLASSFULL IP ADDRESS CLASSIFICATION



The no. of Ip Addresses possible in a N/w of class A = 2^{31} class C = 2^{29}

class B = 2^{30} class D = 2^{28}

Now, the popular Representation of Ip Address = Binary Notation, Dotted decimal Notation (4 octets)

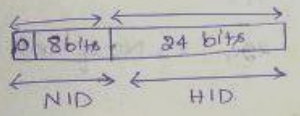


CA = start with '0' CD = starts with 1110

CB = start with 10 CE = start with 1111

CC = start with 110

CLASS A



⇒ The No. of possible N/ws of classA = $2^7 = 128$

⇒ Size of each Network = 2^{24} = 16M (NASA, PENTAGON USES CA)

⇒ No. of hosts = $(2^{24} - 2)$

⇒ But practically 126 N/ws are possible in CA

0 _ _ _ _ _ _ _

0 0 0 0 0 0 0 0 = 0

0 0 0 0 0 0 0 1 = 1

⋮

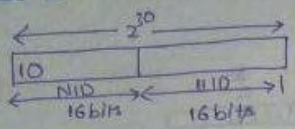
1 1 1 1 1 1 1 = 127

⇒ we donts use the starting Address (All 0's) and Last Address (all ones)

⇒ ∴ No. of N/w's in CA = 128 - 2 = 126 practically.

∴ RANGE = 0-126

CLASS B



⇒ No of Ip Addresses = 2^{30}

⇒ No of N/ws of CB = 2^{14} ≅ 16,000 = 16K N/ws

⇒ Size of each network = 2^{16} Ip Address in one N/ws of CB.

⇒ No of hosts = $(2^{16} - 2)$

⇒ 10 _ _ _ _ _ _

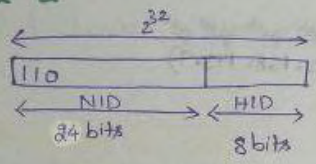
00 0 0 0 0 0 = 128

0 0 0 0 0 0 1 =

1 1 1 1 1 1 1 = 191

⇒ **RANGE = 128 - 191**

CLASS C



⇒ No of Ip Addresses = 2^{29}

⇒ No of N/ws of CC = 2^{21} N/ws = 2million

⇒ Size of Each N/w = 2^8 Ip Address are in one N/w of CC

⇒ 110 _ _ _ _ _

0 0 0 0 0 = 192

0 0 0 0 1 = 193

1 1 1 1 1 = 223 ⇒ No of hosts = $(2^8 - 2)$

⇒ **RANGE = 192 - 223**

CLASS D

There is nothing called as N/w ID and HID in CD and CE

CD

1110 _ _ _ _

0 0 0 0 = 224

1 1 1 1 = 239

RANGE = 224 - 239

1) Used for Multicasting

2) Group Emailing, Group Broadcasting

CE

1111 _ _ _ _

0 0 0 0 =

1 1 1 1 = 255

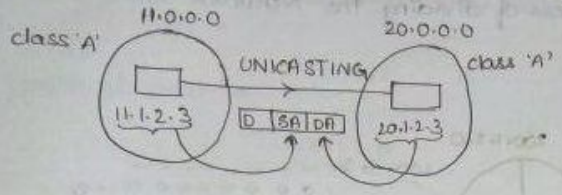
RANGE = 240 - 255

1) Used for Military Applications

2. TYPES OF CASTING - UNICAST, LIMITED BROADCAST, DIRECTED BROADCAST

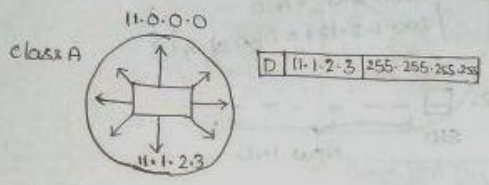
CASTING

1. Unicast - one host to one host
2. Broadcast - one host to many hosts → Limited Broadcasting / Directed Broadcasting



⇒ when i have All 0s in the HID part it represents NID that is the reason we don't use 1st Ip Address as the valid Ip Address to any host

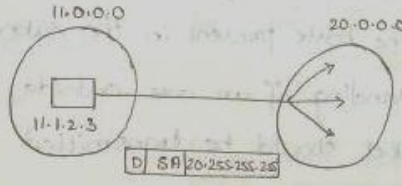
LIMITED BROADCASTING



⇒ If Destination Address = DA = 255.255.255.255 then the packet will be sent to all the hosts in the N/w

LBA = 255.255.255.255

DIRECTED BROADCASTING

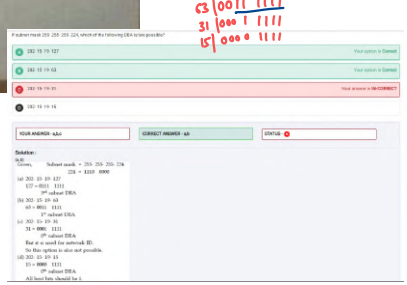


⇒ we are not going to use the Ip Address containing all 1's in HID part, it is used for Direct BROADCASTING (DBA)

DBA : NID , HID = all 1's

Ip Address	NID	DBA	LBA
1.2.3.4	1.0.0.0	1.255.255.255	255.255.255.255
10.15.20.60	10.0.0.0	10.255.255.255	255.255.255.255
130.1.2.3	130.1.0.0	130.1.255.255	255.255.255.255
150.0.150.150	150.0.0.0	150.0.255.255	255.255.255.255
200.1.10.100	200.1.10.0	200.1.10.255	255.255.255.255
220.15.1.10	200.15.1.0	200.15.1.255	255.255.255.255
250.0.1.2	X	X	X
300.1.2.3	X	X	X

NID HID
FF:FF:FF: 1110 0000
127/0111 1111
63/0011 1111
31/0001 1111
15/0000 1111



Q.13
What is the purpose of a subnet mask in an IP address and mask combination?

Time taken to answer this question 00:00:12 hrs

Hide Answer | Add Notes | View Notes | Show Comments

A. To indicate the default gateway IP address. — Your answer is Wrong

B. To dictate the physical location of the address.

C. To save on the possible addresses that you can use in the network.

D. To delineate the network portion of the address from the host portion. — Correct Option

Solution:

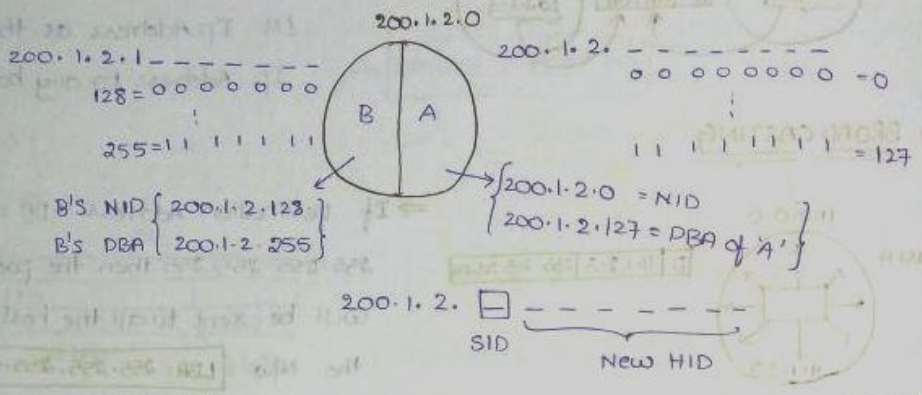
Yes mask separate the host bits with the network bits.

3SUBNETS, SUBNET MASK, ROUTING

⇒ when the size of the N/w is Big then the maintainence will be difficult.

⇒ Lack of security when the size of N/w is Big, so we divide the Network into small parts and this process is called Subnetting.

⇒ "SUBNETTING" is the process of dividing the Network into Smaller Networks



Now, ambiguity arises in the above subnetting, if is say 200.1.2.0 i mean the whole network or only the first subnet and if i say 200.1.2.255 then there is a dilema whether to transfer the packet to all the hosts in the Network or only to the hosts present in the subnet A. so this depens upon where we are standing if we are outside the network then we assume that the packet should be transmitted to all the hosts in the network, if I am standing inside the packet will be transmited to the hosts in subnet'A'.

Q.7
Negative Marks: 0.66 | MCQ | Subject: Computer Networks | Max Marks: 2

Consider a router that interconnects three subnets:
Subnet 1, Subnet 2 and Subnet 3. Suppose all of the interfaces in each of these three subnets are required to have the prefix 223.1.17/24. Also, suppose that Subnet 1 is required to support at least 60 interfaces, Subnet 2 is to support at least 90 interfaces, and Subnet 3 is to support at least 12 interfaces. Provide three network addresses (of the form A.B.C.D/X) that satisfy these constraints.

Time taken to answer this question 00:03:23 hrs

Hide Answer | Add Notes | View Notes | Show Comments

A. Subnet 1 = 223.1.17.0/27, Subnet 2 = 223.1.17.128/25 Subnet 3 = 223.1.17.192/28

B. Subnet 1= 223.1.17.0/26, Subnet 2 = 223.1.17.64/26, Subnet 3 = 223.1.17.128/26

C. Subnet 1 =223.1.17.0/25, Subnet 2=223.1.17.128/25, Subnet 3 = 223.1.17.192/28 — Your answer is Wrong

D. Subnet 1= 223.1.17.0/26, Subnet 2= 223.1.17.128/25, Subnet 3 = 223.1.17.64/26 — Correct Option

Solution:

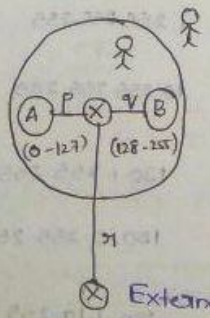
Prefix = 223.1.17/24

First subnet = 6 host bits (64>at least 60), net bits = 24 fixed, subnet bits= 2
So mask = 24 +2 = 26
Hence, 223.1.17.00 000000 = 223.1.17.0/26

Second subnet = 7 host bits(128>at least 90), net bits = 24 fixed, subnet bits = 1
So mask = 24 +1 = 25
Hence, 223.1.17. 1 0000000 = 223.1.17.128/25

The third subnet = 6 host bits (64> at least 12), net bits = 24 fixed, subnet bits = 2
Mask =26
Hence, 223.1.17.01 000000 = 223.1.17.64/26

Took My time & also Silly Mistake with Subnet 3



Q.141
MCQ | Subject: Computer Networks | Max Marks: 1

What is the broadcast address of subnet number 32 in the classful addressing scheme, given an ip address 12.1.0.0/12?

Time taken to answer this question 00:02:13 hrs

Hide Answer | Add Notes | View Notes | Show Comments

A. 12.32.0.255

B. 12.33.255.255

C. 12.47.255.255

D. None of the above — Correct Option | Answered

Solution:

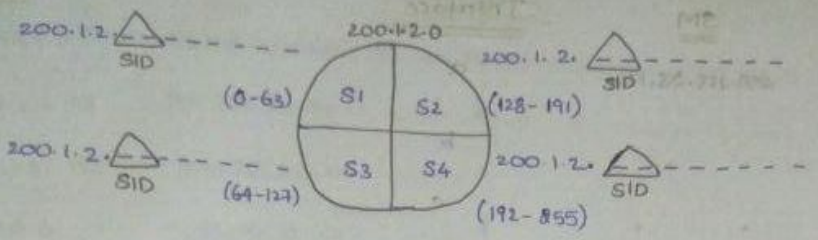
Ans D
Sol: As this IP belongs to class A so network mask is 255.0.0.0
12= Subnet mask is 255.240.0.0

The subnet bits = 4= Total number of subnets possible = (2^4 -2)= 14
So there is no possibility of number 32 subnet because the total number of subnets possible is 14.

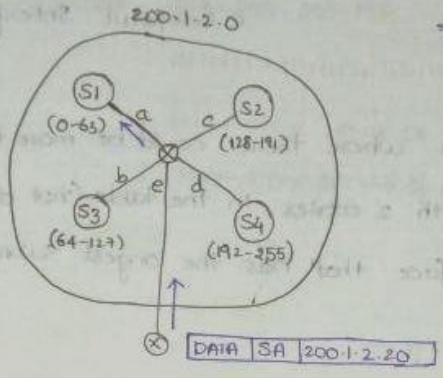
My Mistake: tried to create Subnet

*) There will be loss of ipAddresses due to "SUBNETTING"

FOUR SUBNETS



The, practical view is.



⇒ Here the challenge is you should identify the Nlw or Subnet for which a particular Ip Address belongs to. Here this can be done using "SUBNET MASK"

SUBNET MASK

SM: 32-bit Number

1's: SID, NID part

0's: HID part

Now, the SubNet mask for the above Nlw will be

200.1.2.__ HID
NID.
SID.

⇒ 11111111.11111111.11111111.11000000

SM = 255.255.255.192

⇒ Given an Ip Address, if you bitwise AND with SM you will get NID for which the Ip belongs to

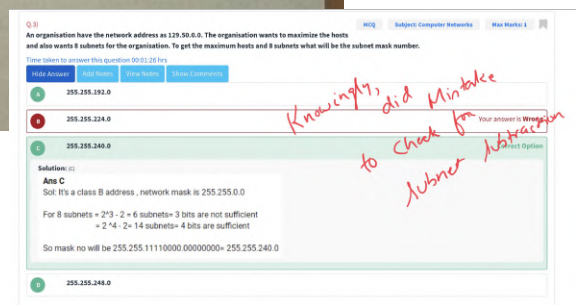
SM && Ip = NID for which the given Ip Belong

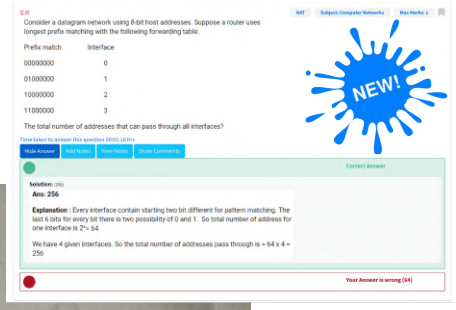
Ip: 11001000.00000001.00000010.10000010 = 200.1.2.130

SM: 11111111.11111111.11111111.11000000 = 255.255.255.192

NID: 11001000.00000001.00000010.10000000

200.1.2.128


Q.9
An organisation have the network address as 129.50.0.0. The organisation wants to maximize the hosts and also wants 8 subnets for the organisation. To get the maximum hosts and 8 subnets what will be the subnet mask number.
MCQ | Subject: Computer Networks | Max Marks: 1
Time taken to answer this question 00:01:26 hrs
Hide Answer | Add Notes | View Notes | Show Comments
A 255.255.192.0
B 255.255.224.0 — Your answer is Wrong
C 255.255.240.0 — Correct Option
Solution:
Ans C
Sol: It's a class B address , network mask is 255.255.0.0
For 8 subnets = 2^3 - 2 = 6 subnets= 3 bits are not sufficient
= 2 ^4 - 2= 14 subnets= 4 bits are sufficient
So mask no will be 255.255.11110000.00000000= 255.255.240.0
D 255.255.248.0
Knowingly, did Mistake to check for Subnet Mask

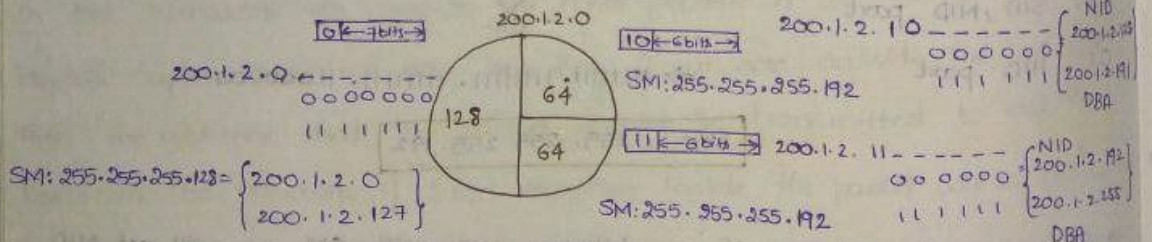


ROUTING TABLE

NID	SM	Interface
200.1.2.0	255.255.255.192	a
200.1.2.64	" "	b
200.1.2.128	" "	c
200.1.2.192	" "	d
0.0.0.0	0.0.0.0	e (default Interface)

⇒ There may be some cases where there could be more than one matches (our packet matches with 2 entries in the table (not default)), in that case choose the interface that has the longest Subnet mask (more ones)

4. VARIABLE LENGTH SUBNET MASKING



Step 1: Divide the entire N|w into 2 parts choosing 1 bit

Step 2: Divide the subnet (your choice) into 2 parts by choosing another bit then you will get 3 subnets

⇒ The N|ws that are having same sizes have the same "subnet mask".

⇒ when the N|w size is Big then the SM will be small
when the N|w size is small then the SM will be Big.

ROUTING TABLE

NID	SM	INTERFACE
200.1.2.0	255.255.255.128	a
200.1.2.128	255.255.255.192	b
200.1.2.192	255.255.255.192	c
0.0.0.0	0.0.0.0	d

Now, Given Subnet mask : 255.255.255.192

: 11111111.11111111.11111111.11000000 = (26 1's, 6 0's)

: NID + SID = No of 1's

: NID + SID = 26 → If classA is subnetted then,

8 + SID = 26 ⇒ SID = 18

= No of Subnets = 2^{18}

→ If CB, NID + SID = 26

SID = 26 − 16 = 10 = 2^{10} Subnets

→ If CC, NID + SID = 26

SID = 26 − 24 = 2 = 2^2 subnets

0 - 00000000

128 - 10000000

192 - 11000000

224 - 11100000

240 - 11110000

248 - 11111000

252 - 11111100

254 - 11111110

255 - 11111111

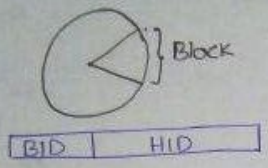
5. SUBNET MASKING QUESTION

	SUBNET MASK	No of HOSTS	SUBNETS IN CA	CB	CC
CA	255.0.0.0	$2^{24}-2$	1	–	–
	255.128.0.0	$2^{23}-2$	2^1	–	–
	255.192.0.0	$2^{22}-2$	2^2	–	–
	255.240.0.0	$2^{20}-2$	2^4	–	–
CB	255.255.0.0	$2^{16}-2$	2^8	1	–
	255.255.254.0	2^9-2	2^{15}	2^7	–
CC	255.255.255.0	2^8-2	2^{16}	2^8	1
	255.255.255.224	2^5-2	2^{19}	2^{11}	2^3
	255.255.255.240	2^4-2	2^{20}	2^{12}	2^4

CLASSLESS INTER DOMAIN ROUTING (L-6)

IANA = Internet Assigned Number Authority

⇒ Generally the Ip Addresses in CIDR Notation is represented as a.b.c.d/(n)



⇒ n = NID bits ⇒ if n=20, NID = 20 bits, HID = 12 bits, 32 bits

⇒ n = Slash Number

FORMATION OF CIDR BLOCKS

These are the Rules for forming CIDR Blocks

1) All the Ip Addresss should be contigious

2) The Block size should be a power of 2

3) The Starting Address should be divisible by size of the Block. evenly

(n-k) bits	k bits

← n-bit → Binary Number

$[n/2^k]$ ⇒ last k bits = Remainder

last (n-k) bits = Quotient

1)

100.1.2.32
100.1.2.33
⋮
100.1.2.47

Whether these Ip Addresses form a CIDR Block?

Rule 1 ✓

Rule 2: No. of Ip Address = 16 = 2^4 ✓ ⇒ HID = 4, BID = 28

Rule 3: 100.1.2.00100000 ÷ 2^4 = LSB (4bits) {Least significant Bits}

= 0000 ✓

∴ They form CIDR Block

2) 20.10.30.32
20.10.30.33
20.10.30.34
⋮
20.10.30.63

Rule 1 = ✓

Rule 2: (63-32)+1 = 32 = 2^5 ✓ (In powers of 2) HID = 5 bits, NID = 27 bits

Rule 3: 20.10.30.001 00000 ÷ 2^5 = last 5 bits

= 00000 ✓

∴ They form CIDR Block

3>

150.10.20.64
150.10.20.65
150.10.20.66
!
150.10.20.127

Rule 1 ✓

Rule 2: $(127-64)+1 = 64 = 2^6$ ✓ ⇒ HID=6, BID=26 Bits

Rule 3: 150.10.20.01000000 ÷ 2^6 = 000000 ✓

FORM CIDR BLOCK ✓

4>

20.10.30.35/27 Derive the Range of CIDR Block?

⇒ BID = 27bits HID= 5bits

BID | HID

20.10.30.00100011

0000 = 32
0001 = 33
!
1111 = 63

⇒ Block = 20.10.30.32
20.10.30.33
!
20.10.30.63

5>

100.1.2.35/28

BID = 27bits HID = 5 bits

BIK NO= BIKID

100.1.2.0010 0011

0000 = 32
!
1111 = 47

100.1.2.32
100.1.2.33
!
100.1.2.47

6> 100.1.2.35/20

BID

100.1.0000 0010.00100011

0000.00000000 = 0 ⇒ 100.1.0.0

1111.11111111 ⇒ 100.1.15.255

15

7. SUBNETTING IN CIDR, VLSM IN CIDR

20.30.40.10/25

BID | SID | HID

20.30.40.0 0 001010

000000 = 0
!
111111 = 63

20.30.40.0/26
20.30.40.63/26

BID | SID | HID

20.30.40.0 1 001010

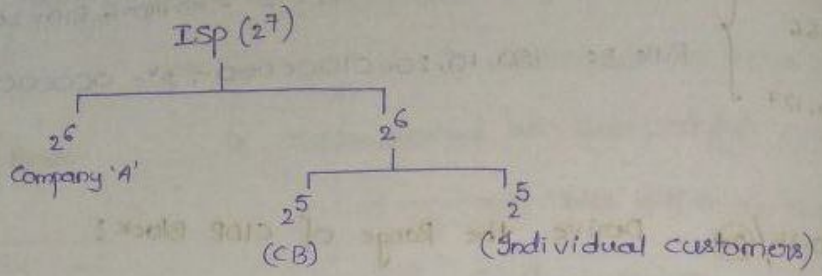
000000 = 64
!
111111 = 127

20.30.40.64/26
20.30.40.127/26

A B

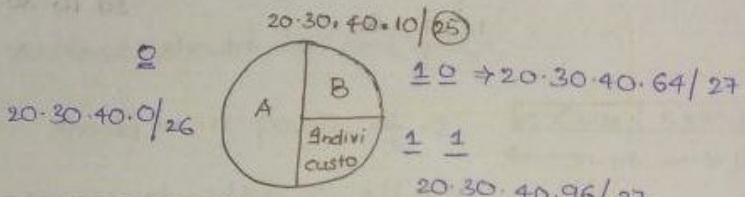
VLSM IN CIDR BLOCKS

1) 20.30.40.10/25



Now, BLK ID
20.30.40.0 0000 1010

000 0000 = 0
111 1111 = 127



∴
CA = 20.30.40.0/26
CB = 20.30.40.64/27
Customers = 20.30.40.96/27

8. SOME INTRESTING PROBLEM ON SUBNET MASK

⇒ subnet mask is sometimes called as "Network mask".

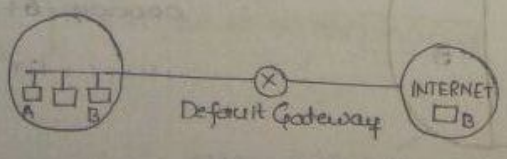
⇒ whenever you open "ipconfig" in your computer you will see these things

1> IpV4 Address: provided by ISp

2> Default Gateway: Default Router connected to your n/w

3> Subnet Mask: Subnet mask which you should use

4) DNS: convertion of Ip addriess




```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:1bca:b119:c62:9117:27bb:2806
   Temporary IPv6 Address. . . . . . : 2401:4900:1bca:b119:f836:e1ad:7553:43c6
   Link-local IPv6 Address . . . . . : fe80::c62:9117:27bb:2806%15
   IPv4 Address. . . . . . . . . . . : 192.168.132.182
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::c4e6:f5ff:fe5b:c769%15
                                       192.168.132.14
```

Let I_A = IpAddress of 'A' I_B = Ip Address of B. (1)

S_A = Subnetmask of 'A' S_B = Subnetmask of B.

⇒ Now if you want send a packet from 'A' to 'B' there are 2 cases possible

1: 'B' may be in different network and you want to send first to DGw and DGw will forward the packet to 'B'

2. 'B' may be in same Network so that you can send the packet directly

Now what 'A' does is A: I_A I_B

Bitwise AND = $\frac{I_A \quad S_A}{((NID)A)}$ Acc to A $\frac{I_B \quad S_A}{((NID)B)}$ Acc to A

If $((NID)A)_{Acc\,to\,A} = ((NID)B)_{Acc\,to\,A}$ then A&B are in same N/w

If

I_A: 200.1.2.10 I_B: 200.1.2.130

S_A = 255.255.255.128

Now, I_A: 11001000.00000001.00000010.00001010

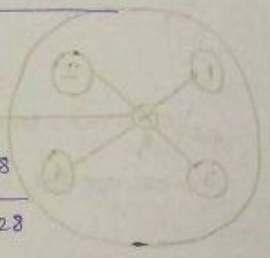
S_A: 11111111.11111111.11111111.10000000

200 . 1 . 2 . 0

$((NID)A)_{Acc\,to\,A}$ = 200.1.2.0 I_B: 200.1.2.130

S_A: 255.255.255.128

$((NID)B)_{Acc\,to\,A}$: 200.1.2.128



$((NID)A)_{Acc\,to\,A} \neq ((NID)B)_{Acc\,to\,A}$ ∴ 'A' assumes that 'B' is in diff Network.

② I_A: 200.1.2.10 I_B: 200.1.[illegible].69

S_A: 255.255.255.128 S_B: 255.255.255.192

I_A I_B

S_A S_A

200.1.2.0 ← $((NID)A)_{Acc\,to\,A}$ $((NID)B)_{Acc\,to\,A}$ → 200.1.2.0

I_B I_A

S_B S_B

$((NID)B)_{Acc\,to\,B}$ = 200.1.2.64 $((NID)A)_{Acc\,to\,B}$ = 200.1.2.0

If $((NID)A)_{Acc\,to\,A} = ((NID)B)_{Acc\,to\,A}$ ⇒ 'A' think B is in same N/w.

⇒ 'B' think 'A' is in another N/w

9. SUPERNETTING OR AGGREGATION

⇒ If we look at the Routing table, it contains a single entry for each and every N/w, now if the networks are large then the size of the routing table may grow exponentially, so that router takes lot of time to process the Routing table, hence we need to Aggregate / combine / supernet the Networks.

RULES FOR AGGREGATION

1) All the N/ws should be contigious. (N/w Id's)

2) Size of each N/w should be same and inturn they should be in powers of 2.

3) 1st Address should be divisible by size of Block

Aggregate the following N/w's

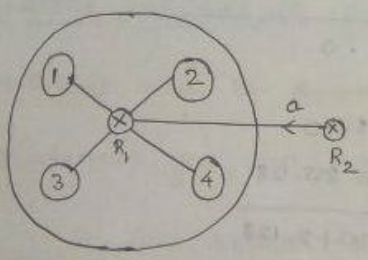
1) 200.1.0.0/24
2) 200.1.1.0/24
3) 200.1.2.0/24
4) 200.1.3.0/24

Total size of N/w = 4×2^8
$= 2^{10}$

Rule 1 ✓

Rule 2 : ✓

Rule 3 ✓ 200.1.00000000.00000000 ÷ 2^{10}
= Divisible



The Routing table at R_2 looks like

NID	SM	INTERFACE
200.1.0.0	255.255.255.0	a
200.1.1.0	255.256.255.0	a
200.1.2.0	255.255.255.0	a
200.1.3.0	255.255.255.0	a

SUPERNET MASK

Supernet mask : 32 bits

: No of 1's = Fixed part

: No of 0's = Variable part

FIXED PART	VARIABLE PART
200.1.000000	00.00000000
200.1.000000	01.00000000
200.1.000000	10.00000000
200.1.000000	11.00000000
255.255.111111	00.00000000

Supernet mask = 255.255.252.0

⇒ Now, the N/w id of the Aggregated N/w is same as the starting IpAddress
= 200.1.0.0/(24) (8)

SHORTCUT TO FIND FIXED AND VARIABLE PARTS

⇒ Size of all N/ws = $2^8 + 2^8 + 2^8 + 2^8 = 2^{10}$ ⇒ Host id part should contain 10 bits

⇒ BID part contain '22' bits

⇒ Now, the Routing table at R_2 look like

	NID	SM	INTERFACE
	200.1.0.0	255.255.252.0	a

2)

100.1.2.0/(25)
100.1.2.128/(26)
100.1.2.192/(26)
} Aggregate them!

⇒ All the Addresss are contigious ✓, but of diff sizes

⇒ The N/ws 100.1.2.128/26, 100.1.2.192/26 } These can be Aggregated first ← Rule 1 ✓, Rule 2 ✓, Rule 3 ✓

⇒ Total size of N/w = $2^6 \times 2 = 2^7$ // ⇒ HID = 7 ⇒ NID = 25 bits

⇒ The N/w of the above Aggregated N/w = 100.1.2.128/25 and now Combine with 1st N/w 100.1.2.0/25

⇒ 100.1.2.0/25, 100.1.2.128/25 } Rule 1 ✓, Rule 2 ✓, Rule 3 ✓

N/w id of Supernet = 100.1.2.0/24

Supernet mask = 255.255.255.0

Now size of N/w = 2×2^7

$= 2^8$ ⇒ NID = 24, HID = 8

174.17.2.1

mask → 0000 0010 . 0000 0000

NID → 1111 1110 . 0000 0000

The router interface has the following IP address on Ethernet0: 174.17.2.1/23. Which of the following can be valid host Ids on the LAN interface attached to the router?

A 174.17.1.100

B 174.17.1.198

C 174.17.2.255 Correct Option

D 174.17.3.0 Your option is Correct

YOUR ANSWER - d | CORRECT ANSWER - c,d | STATUS - ✗

Solution :

(c, d)

174.17.2.1/23

174.17.00000010.00000001

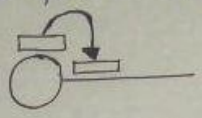
Therefore the host id range is 174.17.2.1 to 174.17.3.254 and thus only option (c) and option (d) are valid.

2. FLOW CONTROL METHODS

DELAYS IN CN (L-1)

TRANSMISSION DELAY (T_t):

The time taken to transmit the packet from a host to the outgoing line is called "transmission delay"



Bandwidth = 1bps (In one second we can transmit 1bit to the outgoing delay)

Data = 10bits

$\Rightarrow$ Transmission delay = 10sec (for 10bits)

So, If size of datapacket is 'L' bits and Bandwidth is 'B' bps then the

Transmission delay = L/B sec

$$T_t = L/B \text{ sec}$$

1) L = 1000 bits, Bw = 1Kbps $\Rightarrow T_t = L/B = \frac{1000}{1000} = 1$ sec

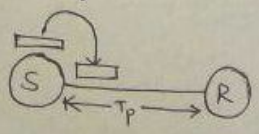
2) L = 1Kb, Bw = 1Kbps $\Rightarrow T_t = L/B = \frac{1024}{1000} = 1.024$ sec

DATA	BANDWIDTH
K = 1024 bits	K = 1000
M = 1024 x 1024	M = 1000 x 1000 = 10^6
G = 1024 x 1024 x 1024	G = 1000 x 1000 x 1000 = 10^9

LEARN FROM THIS MISTAKE

PROPOGATION DELAY (T_p):

The time taken by a bit to reach from one end of the link to other end of the link is called "propogation delay"



The propogation delay depends upon 1) distance

2) velocity

$$T_p = d/v$$

⇒ In case of optical fibers the speed of the signal is approximately 70% of speed of Light ⇒ $v = \frac{70}{100} \times 3\times10^8$ m/s

$\Rightarrow \boxed{v = 2.1\times10^8 \text{ m/s}}$

1) d = 2.1Km

$v = 2.1\times10^8$ m/s

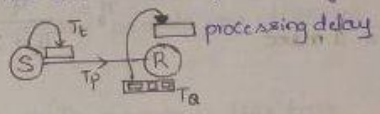
$T_p = d/v = \frac{2.1\times10^3 \text{ m}}{2.1\times10^8 \text{ m/s}} = 10^{-5}$ sec $= \frac{10^{-5}\times10^{-3}}{10^{-3}}$

$\boxed{T_p = 10^{-2} \text{ msec}}$

Now, the total time taken to send a packet from source to Destination = $T_t + T_p$

QUEUING DELAY (T_Q):

⇒ The amount of time the packet sits in the Queue before it gets processed is called Queuing delay(T_Q).

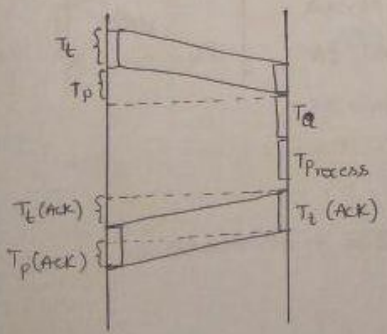


⇒ Whenever the packet is received by the Receiver, it may or may not get immediately processed they are going to sit in Buffer (Queue).

2. FLOW CONTROL STOP AND WAIT

⇒ Stop and wait is the simplest flow control mechanism in which the sender sends a packet and then stop and wait for the acknowledge from the Receiver, before sending the next packet.

Stop and wait uses 1 bit of sequence number 0 and 1 alternatively.



Total time = T_t (data) + T_p (data) + ~~T_Q~~ + ~~$T_{process}$~~ + T_t (Ack) + T_p (Ack)

$= T_t$ (data) + $2*T_p$ + ~~T_t (Ack)~~

Total time = $T_t + 2*T_p$ for sending 1 packet

$$\eta = \frac{\text{useful time}}{\text{Total cycle time}} = \frac{T_t}{T_t + 2*T_p} = \frac{T_t}{T_t(1+2\,T_p/T_t)} = \frac{1}{1+2a} \quad \left(\text{where } \frac{T_p}{T_t} = a\right)$$

$$\eta = \frac{T_t}{RTT}$$

Q. 58

Have any doubt ?

An image is 1024 × 500 pixels with 3 bytes/pixel. Assume the image is uncompressed. How long does it take to transmit it over a 10 Mbps Ethernet?

- 194.6 seconds
- 19.46 seconds
- 1.946 seconds — Your answer is Correct
- 0.1946 seconds

Solution

(d)

Transmission time = $\frac{L}{B}$

for 1. (Data) -

Image = 1024 × 500 pixels

Number of byte = 3 × 1024 × 500

Hence, $TT = \frac{3 \times 1024 \times 500 \times 8}{10 \times 10^6} = 1.9660800$ seconds

Throughput = No. of bits we can send a second using this protocol

$\Rightarrow$ Throughput / Effective Bandwidth / Bandwidth utilisation / Link utilisation $= \frac{L}{T_t + 2*T_p} \Rightarrow \frac{L \times B \times (1/B)}{T_t + 2T_p} = \frac{T_t}{T_t + 2T_p} * Bw$

$\Rightarrow \frac{1}{1 + 2a} * Bw = \eta \times Bw$

$\therefore$ **Throughput = $\eta \times Bw$**

1>

T_t = 1 msec

T_p = 1 msec

Efficiency $(\eta) = \frac{T_t}{T_t + 2*T_p} = \frac{1}{1+2} = 1/3$

2>

T_t = 2 msec

T_p = 1 msec

$\eta = \frac{T_t}{T_t + 2*T_p} = \frac{2}{2 + 2(1)} = 2/4 = 1/2 = 0.5 = 50\%$

3> Now if the efficiency has to be 50% what is the relation between T_t & T_p?

$\eta = 50\% = 1/2 \Rightarrow \frac{T_t}{T_t + 2T_p} \geq 1/2$

$\Rightarrow 2T_t \geq T_t + 2T_p$

$\Rightarrow$ **$T_t \geq 2T_p$** $\Rightarrow L/B \geq 2T_p$

$\Rightarrow$ **$L \geq 2*T_p*B$**

4> Bw = 4 Mbps

T_p = 1 msec

L = ? so that η = atleast 50% ?

$L \geq 2*T_p*Bw$

$L \geq 2 \times 1 \times 10^{-3} \times 4 \times 10^6$

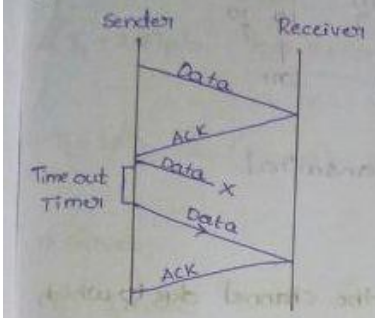
$L \geq 8 \times 10^3$ bits

⇒ NOW, $\eta = \frac{1}{1+2a} = \frac{1}{2+2(T_p/T_t)} = \frac{1}{1+2*\frac{d}{v}*\frac{B}{L}}$ ⇒ $\boxed{\eta \propto 1/d}$. SAW is best for LANS

⇒ $\boxed{\eta \propto L}$

(10)

5)

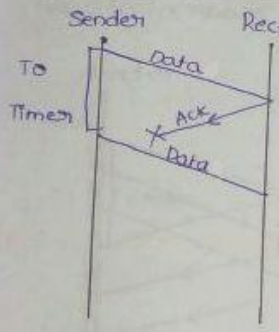


∴ STOP AND WAIT + TIMEOUT TIMER

⇒ STOP AND WAIT ARQ {Automatic Repeat Request}

DATA PACKET LOSS PROBLEM ⇒ {overcome by TO timer}

6) ACK LOST PROBLEM

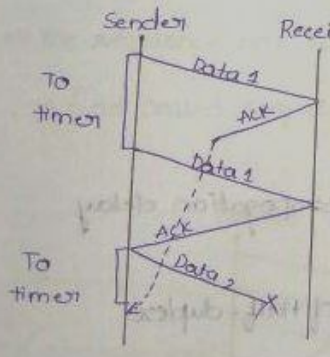


⇒ Acc to sender both the data packets are same but Acc to Receiver both the packets are different

DUPLICATE PACKET PROBLEM ⇒ {To overcome this have sequence numbers}

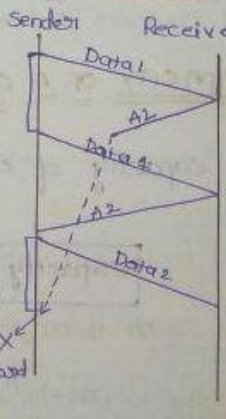
SAW + TO + SEQ. NO TO DATA PACKET

7) DELAYED ACKNOWLEDGEMENT



⇒ This problem can be overcomed by having seqno on Ack also.

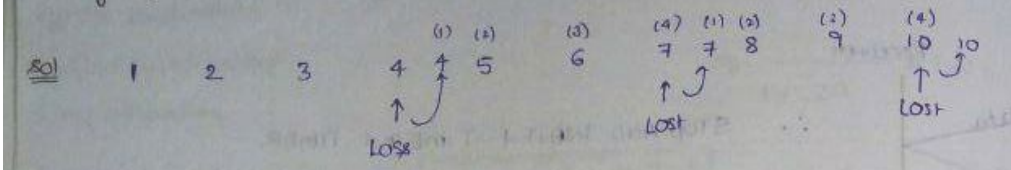
⇒ If the Receiver receives 'D1' sucessfully then it sends Ack A2 which means {"I have sucessfully received D1, please send D2}



⇒ SAW + TO + SEQ NO TO DATA AND ACK

8> Using SAW we have to send 10 packets from sender to Receiver out of which every 4th packet is lost then how many packets are we going to send totally?

Sol



∴ Total = 13 ; (4,7,8) ⇒ packets are Retransmited

9> (S) ——— (R) , Now there are some problems in the channel due to which some of bits are lost, Let us say error probability of channel is 0.2 = 20%, Now if i send 400 packets, then how many packets are transmited totally

Sol ⇒ $400 + 400(0.2) + \{400(0.2)\}(0.2) + \cdots$

⇒ $n + np + np^2 + \cdots$ ⇒ $n(1+p+p^2+p^3+\cdots)$

⇒ $n\left(\frac{1}{1-p}\right) = \frac{n}{1-p}$

here $n = 400$, $\frac{400}{1-0.2} = \frac{400}{0.8} = \frac{4000}{8} = \underline{500}$ packets totally.

3. CAPACITY OF PIPE AND PIPELINING

CAPACITY OF A CHANNEL / WIRE / LINK

The capacity of channel depends on Bandwidth and propogation delay

Capacity of the channel = BW * Tp ⇒ Incase of half-duplex

Capacity = 2 × BW × Tp ⇒ Incase of full duplex

PIPELINING

T_t sec – 1 packet
1 sec – $1/T_t$ packets

Now time taken to transmit one packet of data in stop and wait protocol is $T_t + 2*T_p$. Now,

$\Rightarrow (T_t + 2*T_p) = \frac{T_t + 2*T_p}{T_t}$ packets

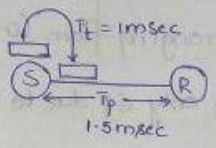
$\Rightarrow T_t + 2*T_p = (1 + 2a)$ packets $\left(a = T_p/T_t\right)$

WINDOW OF PACKETS

1) Given,

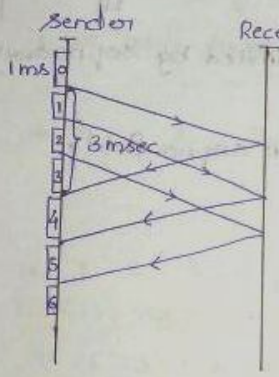
T_t = 1 msec

T_p = 1.5 msec



$\Rightarrow \eta = \frac{T_t}{T_t + 2*T_p} = \frac{1}{1+2(1.5)} = \frac{1}{4} = 25\%$

Now to increase the efficiency of stop and wait protocol,



Round trip time = $2*T_p$

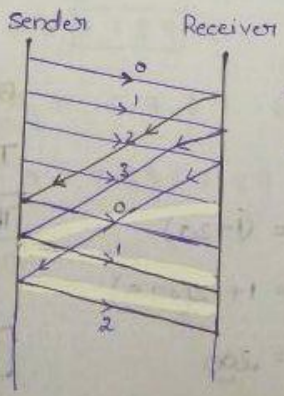
9 8 7 | 6 5 4 3 | 2 1 0

9 8 7 – Yet to be Transmitted

2 1 0 – Already Transmitted and Acknowledged

$\Rightarrow$ The sender window size in sliding window protocol = $w_s = 1 + 2a$

$\Rightarrow$ The sequence nos have to be stored in the header field of packets in a field called sequence no of field.



$\Rightarrow$ Min no of sequence nos = $1 + 2a$

$\Rightarrow$ Min no of bits in seq no fields = n

$2^n = 1 + 2a$

$\Rightarrow n \log 2 = \log(1 + 2a)$

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

2) $T_t = 1\,ms$, $T_p = 49.5\,ms$ } what is the sender window size to get max efficiency?

Sol $\quad w_s = 1+2a \Rightarrow 1 + 2\left(T_p/T_t\right) = 1+2(49.5) = 100$

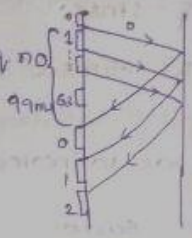
Min. no. of sequence no's $= 100 = (1+2a)$

Min no. of bits in seq no field $= \lceil \log_2(1+2a) \rceil = \lceil \log_2(100) \rceil = 7$

⇒ Now, in the above problem if the min. no. of bits in seq no field is "6", then we can get 64 seq. no (2^6) ranging from (0-63)

⇒ $\eta = \frac{64}{100} = 0.64$ → But I am sending only 64 due to lack of seq no

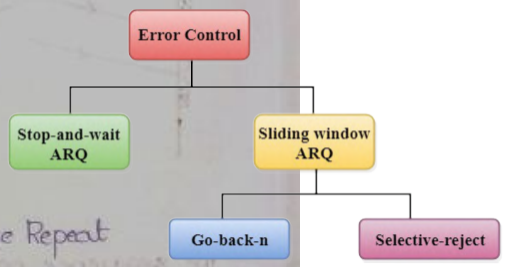
↳ I can send 100 packets in the time available



∴ The window size in the stop and wait protocol is limited by seq. no available

$\therefore w_s = \min(1+2a, 2^n)$ {n = no. of bits in seq no field}

GO BACK -N (1-4)



Sliding window protocol

Go-Back N (cumulative ACK) | Selective Repeat

GOBACK - N (N>1)

1) Sender window size in GBN is "N"

T_t = 1msec

T_p = 49.5msec } η = ?

GOBACK - 10

Max window size $= (1+2a)$

$= 1 + 2(49.5)$

$= 100$

BW = 40mbps

Throughput = ?

Th ⇒ $\eta \times BW$

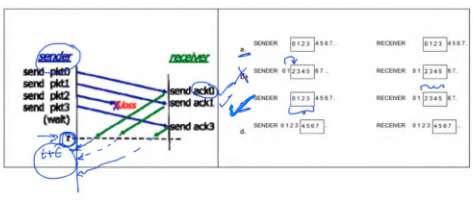
$= 40 \times \frac{10}{100}$

Th = 4mbps

$\eta = \frac{10}{100} = 10\%$

[Medium]

Que: 3 Consider the given figure. Suppose the sender and receiver windows are of size N = 4 and suppose the sequence numbers go from 0 to 15. What are the positions of the sender and receiver windows at time t.



Minute Difference

Consider a selective repeat sliding window protocol, the window size of the sender is 64. What will be the sequence number for the 500th frame?

Hide Answer | Add Notes | View Notes | Show Comments

Correct Answer

Solution:

Window size of selective repeat 2^(n-1) = 64.

So, n = 7 bits
In 7 bits possible sequence number = 128 = 0 to 127
For First 128 frames= 0 to 127
For next 128 frames= 0 to 127
For next 128 frames= 0 to 127
Upto then 384 frames completed transmission
Left 116 frames out of 350 = 0 to 115
Hence 115 is the sequence number for the 500th frame.

Your Answer is wrong (116)

I saw 500 as frame and thought of 115 frame. But, Marked 116

If the Sender Window size is 128 using selective repeat ARQ. Then the sequence number of frame to be sent after sending 400 th frame is ?

Hide Answer | Add Notes | View Notes | Show Comments

Correct Answer

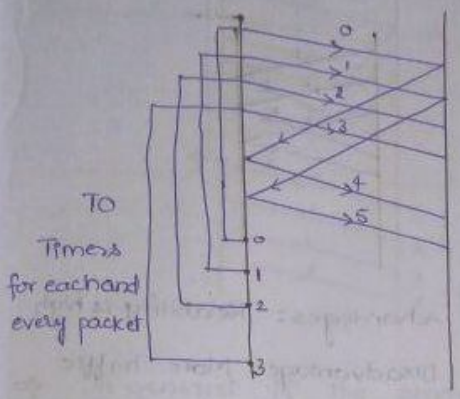
Solution:

For selective repeat ARQ, we know that sender window size=receiver window size and total no number of sequence numbers=2N (where N is the sender window size)
Total sequence number = 2^N = 256
Hence 0-255 would be consumed for sending 256 frames.
0-143 = 144 frames
400 frames completed.
After 400 the frame the sequence number would be 144

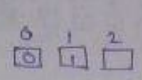
Your Answer is wrong (144)

I forgot to double the window size for SR.

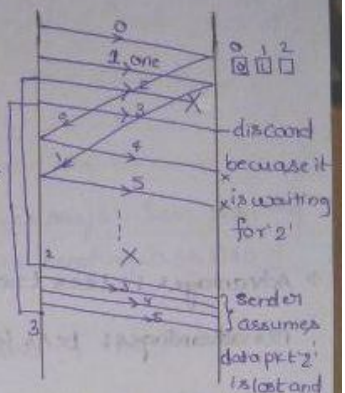
2) Receiver window size:



To Timers for each and every packet



Suppose if Data pkt 2 ⟹ is lost, then what happens at Receiver side is ⟹



Sender retransmit all the frames before the next timeout.

3) In GoBack-3 if every 5th packet that is being transmitted is lost and if we have to send 10 packets, then how many transmissions are Required?

⇒ 1 2 3 4 [5 6 7] 8 9 10
↑ is lost

⇒ 1 2 3 4 [5 6 7] 5 6 [7 8 9] 10
1 2 5 6 7 8 9

= 1 2 3 4 5 6 7 5 6 7 8 9 7 8 9 [9 10]

= 1 2 3 4 5 6 7 5 6 7 8 9 7 8 9 10 9 10 = 18 packets are Transmited

4) GB-4, Every 6th packet is lost, I should send 10 packets, How many transmissions

Sol = 1 2 3 4 5 [6 7 8 9] 10

= 1 2 3 4 5 6 7 8 9 6 7 [8 9 10]

= 1 2 3 4 5 6 7 8 9 6 7 8 9 10 8 9 10

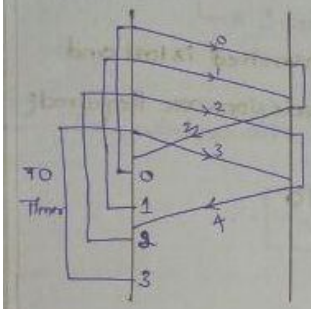
= 17 transmissions

5) Acknowledgements: There are 2 kinds of Ack 1) Cumulative Ack
2) Independent Ack

1) Advantages: Less traffic
Disadvantages: Less Reliability

2) Advantages: Reliability is high
Disadvantage: More Traffic

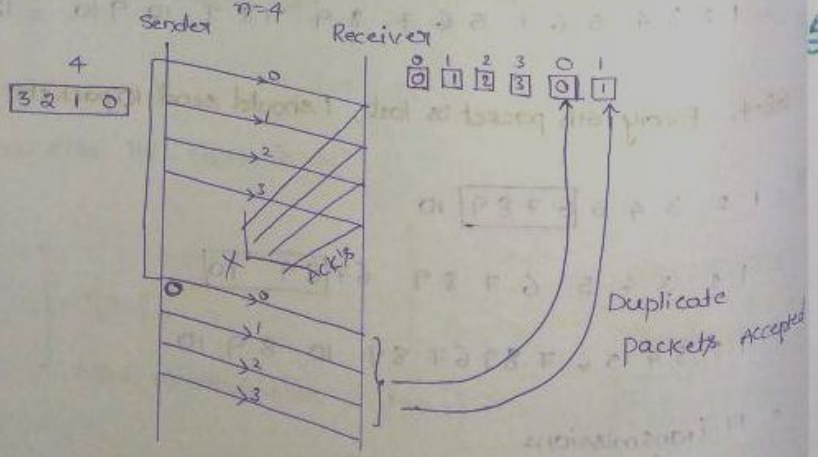
⇒ GoBack - N uses cumulative Acknowledgements.



⇒ TO Timers > Ack Timers

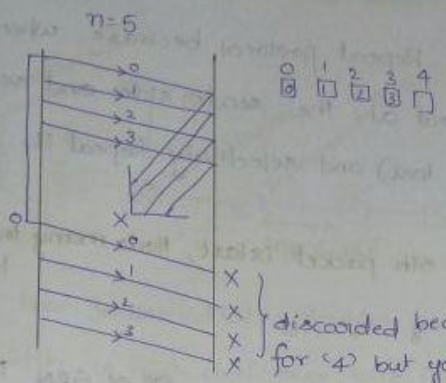
RELATIONSHIP BETWEEN WINDOW SIZES AND SEQUENCE NO's IN GBN

GB-4 ⇒ Sender window size = 4 ⇒ No of sequence no.



∴ This scenario ⇒ (having the sequence nos = window size) don't work

2) GB-4 , N=5 (Seq. No's)



⇒ In general if the sender window size = 'N' and if the Receiver window size = 1 then to detect the Duplicate packets in GBN the No. of Seq nos should be (N+1).

⇒ In any sliding window protocol if it has to work without any problem the condition is $(w_s + w_R) \leq$ ASN (Available Sequence nos)

⇒ If $w_s = N$, $w_R = 1$ ⇒ Seq Nos = N+1 ⇒ No. of bits in Seq no field = $\lceil \log_2(N+1) \rceil$

⇒ If Seq Nos = N then wat is the max value of $w_s = N-1$ $w_R = 1$

⇒ No. of bits in Seq no field = K then $w_s = 2^K - 1$, $w_R = 1$, No. of Seq Nos = 2^K

5. SELECTIVE REPEAT AND COMPARISION BETWEEN ALL SLIDING WINDOW PROTOCOLS

1) $w_s > 1$

$T_t = 1$ ms $T_p = 49.5$ msec, $w_s = 50$, In SR-protocol $\eta = ?$

Sol) $\eta = \frac{50}{100}$ ⇒ $\boxed{\eta = 50\%}$

Max window size of sender = 1+2a
= 1+2(49.5)
= 100

Bw = 4mbps ⇒ Throughput = $\eta \times Bw$
$= 1/2 \times 4 = 2$ mbps

2) $W_R = W_S$

⇒ This protocol is called selective Repeat protocol, because whenever a packet is lost there will be a timeout at the sender side and sender is going to select that packet (which is lost) and selectively Repeat it.

$W_S = 3$, 10 packets are sent, every 5th packet is lost, How many transmissions in SR protocol

Seq: = 1 2 3 4 5 6 7 8 9 10

= 1 2 3 4 5 5 6 7 8 9 9 10

= 1 2 3 4 5 5 6 7 8 9 9 10

= 12 transmissions

Properties	Stop and Wait	Go Back N	Selective Repeat
Sender window size	1	N	N
Receiver Window size	1	1	N
Minimum Sequence number	2	N+1	2N
Efficiency	1/(1+2*a)	N/(1+2*a)	N/(1+2*a)
Type of Acknowledgement	Individual	Cumulative	Individual
Supported order at Receiving end	–	In-order delivery only	Out-of-order delivery as well
Number of retransmissions in case of packet drop	1	N	1

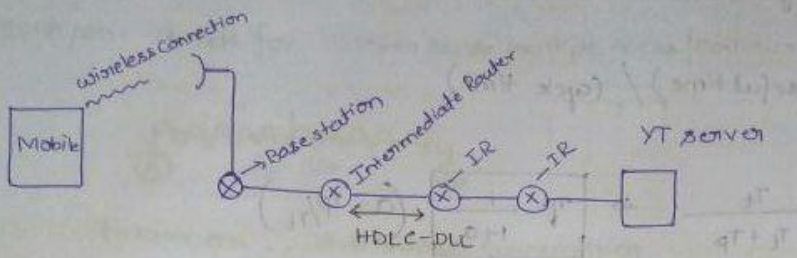
3) The Ack are independents in SR-protocol

⇒ In case of packet loss both GBN and SR protocol behaves same way but in case of corrupted Data packets SR is going to send "NACK" (Negative Acknowledgement)

	SAW	GBN	SR
Efficiency	$\frac{1}{(1+2a)}$	$\frac{N}{(1+2a)}$	$\frac{N \rightarrow \text{Sender window size}}{(1+2a)}$
Buffers	1+1 = 2	N+1	N+N = 2N
Sequence Numbers	1+1 = 2	(N+1)	(N+N) = 2N
Retransmissions (1 packet is lost)	1	N	1
Bandwidth	Low	High (More Retrans)	Moderate
cpu	Low	Moderate	High
Implementation	Easy	Moderate	Difficult/complex

⇒ The maximum window size for data transmission using Selective Reject protocol with n-bit frame sequence numbers is 2^{n-1}

PRACTICAL SCENARIO WHERE SR AND GBN ARE USED



⇒ Generally the Intermediate Routers are connected with Thick wires.

⇒ Bandwidth is high and error rate is low, out of order are not possible, cpu's are powerful and there are always Busy in processing the pkts

∴ The availability of cpu is very less.

⇒ For all the above scenarios GBN is used.

⇒ When we consider near our mobile phone / Laptop, Error rate ↑, Bw↓ and out of order packets are possible, cpu is available ∴ cpu ↑

⇒ SR protocol is used.

∴ Link to Link protocols like HDLC -(DLL) uses "GBN"

End to End protocols like Tcp - uses - "SR" Tcp-(Transport Layer)

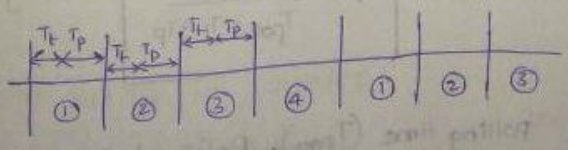
6. INTRODUCTION TO ACESS CONTROL METHODS, TDM, POLLING

The are two types of Links
- Broad cast Link
- point - point Link

TDM

⇒ TDM stands for Time Division Multiplexing.

⇒ Divide the timeline into slots and allot a station to each slot in Round Robin manner.



η = (cycle time)$^{-1}$ × (use ful time)

η = (useful time) / (cycle time)

$$\eta = \frac{T_t}{T_t + T_p} \Rightarrow \boxed{\eta = \frac{1}{1+a}} \quad \left(a = T_p/T_t\right)$$

If T_t = 1msec, T_p = 1ms and η of TDM? $\eta = \frac{1}{1+a} = \frac{1}{1+1} = \frac{1}{2} = 50\%$

Bw = 4mbps Throughput = $\eta \times Bw = \frac{1}{2} \times 4 = 2$mbps

Now, if 'N' stations are connected to the channel and each station Require 2kbps Bw then what is the max value of N?

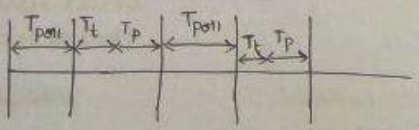
$\Rightarrow N * 2\text{kbps} = 2\text{mbps}$

$\Rightarrow \boxed{N = 1000}$

Disadvantages

1. The problem with Reservation method in TDM is, whenever you reserve a slot for a station, the station might not use it completely the reason is it is not always true that every station might have data to transmit then the slot alloted will be wasted.

POLLING



η = (useful time) / cycle time

$$\eta = \frac{T_t}{T_{poll} + T_t + T_p}$$

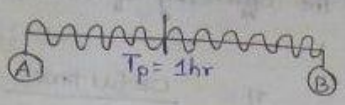
$$\boxed{\eta = \frac{T_t}{T_{poll} + T_t + T_p}}$$

Throughput = $\eta \times Bw$

⇒ The disadvantage is the polling time (T_{poll}). Before transmiting we should actually construct polling.

1. CSMA/CD

⇒ The CSMA/CD stands for carrier sense multiple Access/collision Detection.



t = 10:00 Am , A & B starts transmitting

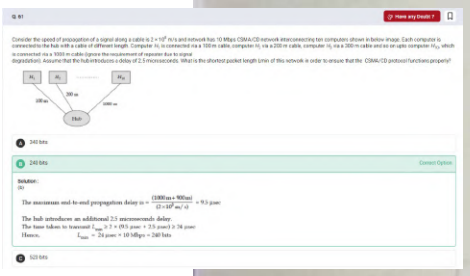
t = 10:30 Am, collision

t = 11:00 AM , collision signals observed by A & B

⇒ Now, if A & B must be sure about their data (i mean whether the data that they are transmitting, got collided or others data) the condition is

$$T_t > T_p$$

⇒ At worst case, if A starts transmiting at 10:00 Am after how much time will 'A' get the collision signal back.


Q. 61

Consider the speed of propagation of a signal along a cable is 2×10^8 m/s and network has 10 Mbps CSMA/CD network interconnecting ten computers shown in below image. Each computer is connected to the hub with a cable of different length. Computer H_1 is connected via a 100 m cable, computer H_2 via a 200 m cable, computer H_3 via a 300 m cable and so on upto computer H_{10}, which is connected via a 1000 m cable (ignore the requirement of repeater due to signal degradation). Assume that the hub introduces a delay of 2.5 microseconds. What is the shortest packet length (min of this network in order to ensure that the CSMA/CD protocol functions properly?

Have any Doubt ?

A 240 bits

B 240 bits — Correct Option

Solution:

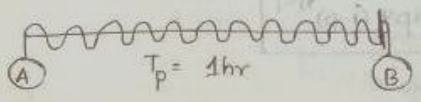
(i) The maximum end-to-end propagation delay is $= \frac{(1000 m + 900 m)}{(2 \times 10^8 m/s)} + 9.5\ \mu sec$

The hub introduces an additional 2.5 microseconds delay.

The time taken to transmit L_{min} is $7 \times (9.5\ \mu sec + 2.5\ \mu sec) \geq 34\ \mu sec$

Hence, $L_{min} = 24\ \mu sec \times 10\ Mbps = 240$ bits

C 320 bits



10:00:00 Am, A start transmitting

10:59:59 Am, B starts transmiting

11:00:00 Am, collision

12:00:00 Am, 'A' sees the collision signal.

Consider a 10 Mbps Ethernet LAN that has stations attached to a 2.5 km long coaxial cable.Given that the transmission speed is 2.3*10^8 m/s, the packet size is 128 bytes out of which 30 bytes are overhead, the 'A' effective transmission rate and 'B' maximum rate at which the network can send data. Find A +B in Mbps?

Time taken to answer this question 00:05:10 hrs

Hide Answer | Add Notes | View Notes | Show Comments

Solution: (11.44)

Ans : 10.44

Sol: In effective Transmission you can consider the overhead , as it is explicitly given otherwise it will be given as negligible.

And in the Maximum Transmission Rate just discard that overhead and take the Ideal Situation.

Prop.Delay =length/ speed= (2.5 x 10^3 m)/(2.3 x 10^8)= 10.8 μsec

Trans.Delay= data size/ Bandwidth= 128 B/ 10Mbps = 102.4 μsec

a = T_p / T_t = 10.8 μsec / 102.4 μsec = 0.105

Efficiency(η) = 1 / (1 + 6.44 x a) = 0.59 = 59%

Maximum rate or Throughput = Efficiency x Bandwidth= 0.59 x 10 Mbps= 5.9 Mbps= B

Effective transmission rate= Throughput x (128-30 / 128)= 5.9 Mbps x (98 / 128)

= 0.77 x 5.9 Mbps= 4.54 Mbps = A

A+ B= 10.44

∴ The time at which 'A' sees the collision signal is 2hrs = $2*T_p$

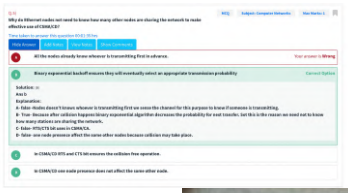
∴ If 'A' has to detect collision (be sure about whether its own data) got collided or others data) it should still be transmiting the data in worst case also

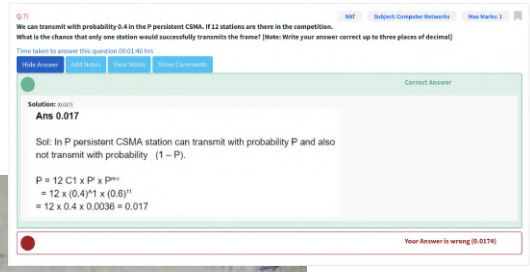
⇒ $T_t \geq 2*T_p$ ⇒ $L/B \geq 2*T_p$

⇒ $L \geq 2*T_p*B$ = This is the min size of packet to detect collision

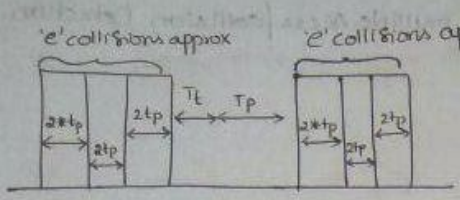
⇒ There are NO Ack in CSMA/CD.

⇒ CSMA/CD is used in Ethernet & IEEE 802.11 Wireless LAN





EFFICIENCY OF CSMA/CD/ETHERNET



The efficiency of CSMA/CD is

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

$$\eta = \frac{Tt}{[e * 2 * tp] + Tt + Tp} \Rightarrow \eta = \frac{\text{Trans mission delay}}{[(\text{No. of contention slots}) * 2 * pD] + TD + PD}$$

1> If there are 'n' stations connected to CSMA/CD and every station wants to send the data with probability 'p'.

Now, There will be a successful trans mission if only one station transmits the data and other stations Refrain = ploty for successful trans =

$$P_{sucess} = {}^{n}C_1\, p * (1-p)^{n-1}$$

$$\boxed{P_{sucess} = np * (1-p)^{n-1}}$$

Throughput of Aloha = $p.(1-p)^{n-1}$

Now, $\frac{dP_{sucess}}{dp} = 0 \Rightarrow \boxed{p = 1/n}$ At value of $p = 1/n$ the sucess probability will be maximum.

$$\Rightarrow \boxed{P_{max} = (1 - 1/n)^{n-1}} \quad \text{Now,} \boxed{\lim_{n \to \infty} (1 - 1/n)^{n-1} = 1/e}$$

2> No. of tries (or) times we should try before getting first sucess = $1/P_{max} = e$

$$\eta = \frac{Tt}{e * 2 * Tp + Tt + Tp}$$

$$\boxed{\eta = \frac{1}{1 + 6.44a}} \quad \left(a = Tp/Tt\right) \Rightarrow \eta = \frac{1}{1 + 6.44\left(\frac{d}{v} \times \frac{B}{L}\right)}$$

⚠ CAUTION SILLY MISTAKES

↑ in this in CSMA/CD or Ethernet not $\left(\frac{1}{1+2a}\right)$

⇒ The max amount of data that can be sent through Ethernet = 1500 Bytes

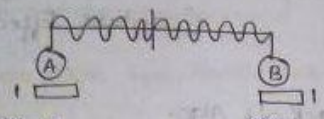
⇒ $\eta \downarrow$ as $d \uparrow$ {CSMA/CD NOT SUITABLE FOR WANS}

⇒ $\eta \uparrow$ as $L \uparrow$ {send Bigger pkts for good efficiency}

8. BACK OFF ALGORITHM FOR CSMA-CD

⇒ The Back-off Algorithm is used to give waiting time of a station before it starts Retransmiting after involved in a collision. This waiting time is called Backoff time

1)



n = 1 n = 1

⇒ $(0, 2^n - 1)$ ⇒ $(0, 2^n - 1)$

⇒ (0,1) ⇒ (0,1)

n = Collision Number

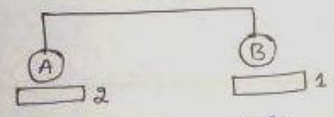
⇒ This Algo says both the stations 'A' and 'B' should randomly choose a no between $(0 \to 2^n - 1)$

∴

A	B	
0	1	⇒ A's waiting time = 0 * T_{slot} = 0 } A' won Backoff race
1	0	B's waiting time = 1 * T_{slot} = T_{slot} }
0	0	} - collisions
1	1	

p(A) = 1/4 p(B) = 1/4 p(collision) = 1/2

Now, Suppose let us Assume 'A' wins the Backoff Race ⇒ 'A' has successfully transmited its 1st Data packet and is ready with 2nd Data packet



n = 1 n = 2

$= (0, 2^n - 1)$ $= 0(0, 2^n - 1)$

$= (0,1)$ $(0,3)$

$= (0,1)$ $(0,1,2,3)$

A	B	
0	0	⇒ collision
0	1	⇒ 'A' win
0	2	⇒ 'A' win
0	3	⇒ 'A' win
1	0	⇒ 'B' win
1	1	⇒ collision
1	2	⇒ 'A' win
1	3	⇒ 'A' win

p(A) = 5/8 p(B) = 1/8 p(collision) = 2/8

⇒ Waiting Time = K × T_{slot} $K \in (0, 2^n - 1)$ n: collision number

⇒ collision probability is decreasing exponentially.

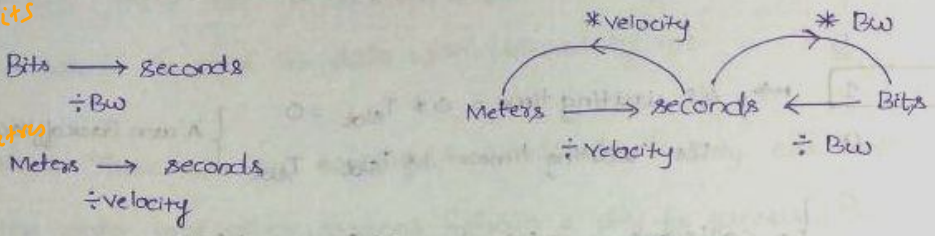
⇒ If 'A' has won first collision the pbty that it wins 2nd collision is high (Capture Effect)

⇒ Applicable only for 2 stations.

⇒ Binary Backoff Algo or Binary exponential Backoff Algo.

9. TOKEN PASSING ACESS CONTROL METHOD

- When Time is given in Bits
- When Time is given in Meters



How many meters 10bits Equalent to, given that Bw 4mbps, $V = 2 \times 10^8$ m/s

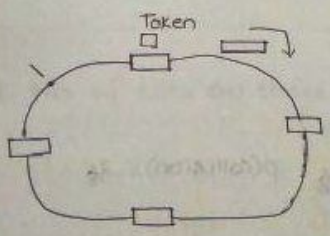
Sol

Bits = 10bits

$$\frac{Bits}{Bw} = \frac{10}{4} = \frac{2.5 \text{ sec}}{10^6} * 2 \times 10^8 \text{ m/s}$$

$$= \frac{5 \times 10^8 \text{ m}}{10^6}$$

Ans = 500 m



1. Unidirectional flow of data
2. only one station can transmit at a time
3. If i leave a bit at some point in the ring the time taken by it to take one complete Rotation is called "RING LATENCY"

Ring latency = $\left(\frac{d}{v}\right)_{sec} + (N * b)_{Bits}$ → delay

N → No. of Stations

d = length of Ring
V = Velocity

$$\text{Ring Latency} = \frac{d}{v} + \frac{(N*b)}{Bw} \text{ seconds}$$ (or)

$$RL = \frac{d}{v} * Bw + N*b \text{ Bits}$$

THT = Token Holding time → THT is time for which each station holds the token

(17)

Cycle time = $\frac{d}{v} + (N * THT) = T_p + (N * THT)$

$$\eta = \frac{N * T_t}{T_p + (N * THT)}$$

There are two strategies that are present in token passing mechanism they are

1) Delayed Token Reinsertion ⇒ $THT = T_t + T_p$ ⇒ $\eta = \frac{1}{1 + \frac{(N+1)}{N} a}$ $\left(a = T_p/T_t\right)$

2) Early token Reinsertion ⇒ $THT = T_t$ ⇒ $\eta = \frac{1}{1 + (a/N)}$

Used at University of Hawaii

10. ALOHA AND DIFFERENCES BETWEEN FLOW AND ACESS CONTROL

1) Any station could transmit data at any time - No carrier sensing.

2) collisions are possible, Acknowledgements are there ⇒ Collision detection ✗

3) Retransmissions ✓ after some time (Backoff time)

ALOHA
- pure Aloha
- Slotted Alha

Q.2)
Groups of user stations(N) share a 56Kbps pure aloha channel. Each station outputs a 1000 bits frame on an average of once every 100sec(stations are buffered). What is the max value of N?

NAT | Subject: Computer Networks | Max Marks: 1

Hide Answer | Add Notes | View Notes | Show Comments

Correct Answer

Solution:

Ans: 1030

Sol: With pure ALOHA, the usable bandwidth is 0.184 x 56 = 10.3 kbps.
Each station send= 1000bits
So in 1 sec each station sends= 1000/100= 10bps
, so Max number of stations possible = 10.3Kbps/10bps = 1030 stations.= N

pure Aloha

1) Vulnerable time = $2T_t$

2) $\eta = G * e^{-2G}$ (G = No. of stations who wants to transmit in T_t slot)

$\Rightarrow \frac{d\eta}{dG} = 0 \Rightarrow G = 1/2$

if $G = 1/2$, η = max

$\Rightarrow \eta_{max} = 1/2 \times e^{-1}$

$\eta_{max} = 0.184$

$\eta_{max} = 18.4\%$

Slotted Aloha

1) Vulnerable time = T_t

2) $\eta = G * e^{-G} \Rightarrow \frac{d\eta}{dG} = 0 \Rightarrow G = 1$

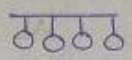
$\Rightarrow \eta = 0.368$

$\eta_{max} = 36.8\%$

FC	AC
SAW = $\frac{1}{(1+2a)}$, SWP: $\frac{N}{(1+2a)}$	TDM = $\frac{1}{1+a}$, polling: $\frac{T_t}{T_t + T_{poll}}$
GBN: $\frac{N}{(1+2a)}$	CSMA/CD = $\frac{1}{1+6.44a}$
SR: $\frac{N}{(1+2a)}$	Aloha → Pure $G \times e^{-2G} = 18.4\%$; Slotted $G * e^{-G} = 36.8\%$

5. LAN - TECHNOLOGIES

ETHERNET (IEE 802.3)

1> Topology: Bus topology 

2> Access control method: CSMA/CD

3> NO Acknowledgement

4> Data Rates (Bandwidth): 10mbps — 100mbps — 1Gbps
(Fast Ethernet) (Gigabit Ethernet)

5> Encoding technique: Manchester Encoding (Baud Rate = 2 * Bit Rate)

6> "Ethernet" operates at Data Link Layer. (LAN technologies are dealt at DLL)

AL = Message

TL = Segment

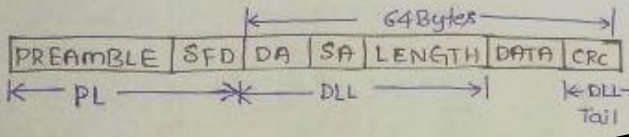
NL = Datagram

DLL = Frame

PL = Single protocol Data unit. (I-PDU)

Gate 2006

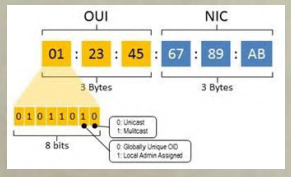
FRAME FORMAT OF ETHERNET (OR) IEEE 802.3 FRAME FORMAT



PREAMBLE: 7bytes : 10 10 1010 10 ----- 10 → Syn. clock of sender's & Receiver's.
⇒ used to alert all the stations
⇒ Indicate Start of frame, Synchronization.

SFD: [Start frame Delimeter]: 1Byte : 10101011

DA: 6Bytes } MAC Address
SA: 6Bytes }
CRC: 4Bytes



TYPES OF MAC ADDRESS

Ex: 1A:2B:34:48:56:6F

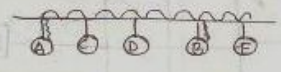
1. UNICAST MAC ADDRESS: [LSB of 1st byte is 0] 00011010 : 00101011 :
↑

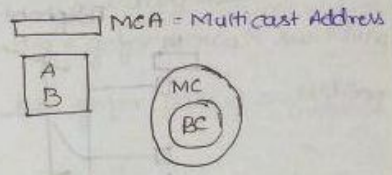
2. MULTICAST MAC ADDRESS: [1st Byte's LSB is 1]

3. BROADCAST MAC ADDRESS: [All the bits are ones in MAC Address] FF:FF:FF:FF:FF:FF

⇒ The multicasting MAC Address is implemented in this way (24)

⇒ Consider a LAN containing many stations, Now, i want to send a message to two stations A and B (or) Repeatedly i want to send messages to some set of stations inside my LAN, Let us Assume that A, B are my stations and if I send a message both of them should Receive it. Then it is always better that you create a group for them and for that group you are giving a Group ID and that ID should be a multicast Address, and inform A and B that see you both are present in a Multicast Group with some Address then Both A&B will configure their NIC's in such a way that whenever any packet is sent to that particular Multicast Address both of them will automatically Read and others will discard it.





LENGTH : 2Bytes = 16bits

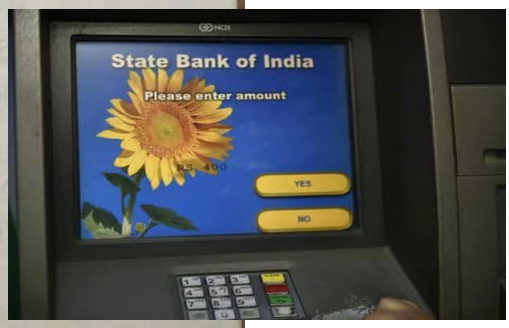
: The main reason for including Length field is ETHERNET follows variable length frames

: In CSMA/CD : $L \geq 2 * T_p * BW$ substituting the standard values of T_p, BW for Ethernet we get

$L \geq 64$ Bytes

: Max Length : 1500 Bytes

	MIN	MAX
DATA	46B	1500B
FRAME	64B	1518B



like in ATM Machine

DISADVANTAGES

1) Not applicable to Real time Applications

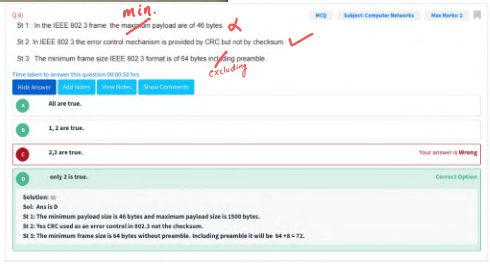
2) Not Applicable to Interactive Applications [chatting].

3) No priorities so not suitable for client Server Applications.

∵ PREABLE = 7B LENGTH = 2B

SFB = 1B CRC = 4B

SA = DA = 6B



3. ERROR CONTROL METHODS

1. ERROR CONTROL AND CRC

⇒ The main reason for packet loss is "Congestion"

⇒ Error handling is mainly of 2 types → Error Detection → (D+D), parity check, CRC, Checksum
→ Error Correction → Hamming code

CRC (CYCLIC REDUNDANCY CHECK)

⇒ CRC is mainly used at Hardware Level.

Sender: 1011011 CRCG: 1101 Receiver:

⇒ If CRC Generator is 'n' bits we are going to append (n-1) bits (All 0s) to the data.

Appended Bits

Appended data = 1011011 000

⇒ ⊕ = Exclusive OR (or) modulo 2 sum

1⊕1 = 0 1⊕0 = 1
0⊕0 = 0 0⊕1 = 1

Now,

```
1101) 1011011000 (...
      1101
      0110011000
       1101
      0001111000
         1101
      0011100
          1101
      0010
```

⇒ If CRC G = n bits then CRC = (n-1) bits

⇒ Always start Applying XOR from the Leading 1 (Starting 1)

Now the least significant 3 bits will be the "CRC" = 001

∴ The Zeros that you appended at the begining will be replaced by the CRC and gets transmited.

∴ The data that will be sent to Receiver is = Actual data + CRC

= 1011011 001
AD CRC

At Receiver side, Whether the data that is transmited is Right or wrong

```
1101)10111011001(
     1101
     ----
     01100
      1101
      ----
      00011
       1101
       ----
       00110
        1101
        ----
        0011
        =CRC
```

If you get all zeros as CRC then the data that is transfered is error free

2. CRC EXAMPLE

CRC: $x^3+x+1 = 1\cdot x^3+0\cdot x^2+1\cdot x+1\cdot x^0$ = 1011 is the CRC

If the degree of the polynomial = 3 the no.of bits in CRC Generator are 4 and we append '3' 0's ∴ Degree of the CRC polynomial = Size of CRC generated.

At Sender

Data: 11010

CRC: x^3+x+1 = 1011

∴ Appended data = 11010 000

```
1011)11010000(
     1011
     ----
     01100
      1011
      ----
      0111
       1011
       ----
       0100
        1011
        ----
        0010
```

CRC = 010

At Receiver side

```
1011)11010010(
     1011
     ----
     01100
      1011
      ----
      0111
       1011
       ----
       0110
        1011
        ----
        0000   = All 0's ✓
```

3. CHECKSUM

⇒ Tcp, Ip, UDP uses 16 bit checksum, and checksum is used at Software level.

⇒ The entire stream of data (bits) are divided into many parts of equal sizes which is equal to the size of checksum that you need i,e If you are using 8 bit checksum then divide the entire stream of data into equal parts and size of each part should be 8.

Q. 30

? FAQ Have any Doubt ?

If we have to send 7 bits of data then the number of redundant bits need to be added before send the data is _____

4 — Correct Option

Solution :
4
We need to satisfy the condition $2r >= m + r + 1$ where r is number of redundant bits and m is number of data bits that needs to be send.
The smallest value for $r = 4$ is satisfying the condition.
Hence the answer is 4.

Your Answer is 1

⇒ Now encode the decimal values of all the parts and add them all, finally than ans you get must be Negotiated (if we get 34 you should write -34) and add this value (-34) to the checksum field.

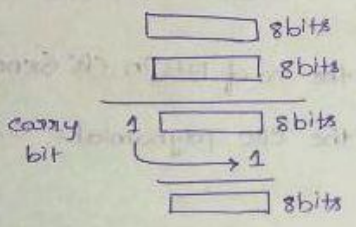
8 bits	8bits	8bits	8bits	8bits	8bits	8bits	CS −31

10 1 2 3 4 5 6 = 10+1+2+3+4+5+6

= 31 ⇒ CS = −31

Ones Compliment

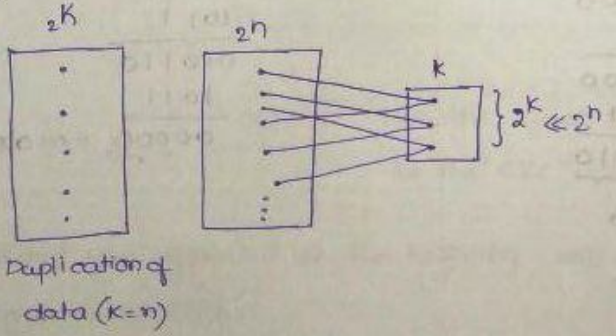
⇒ Suppose if i add two 8 bit no's in the above checksum then i may get a 9 digit Binary number then you take the LSB and add it to the obtained number, This is called "wrap Around."



4. CN - SUMMARY

⇒ No method is actually Reliable, the data may be corrupted (or) the Error handling bits may be corrupted.

⇒ Meaningful errors are nothing but, data is being corrupted in such a way that no one is able to detect it because error handling bits are also changed.



Q.11)

MCQ Subject: Computer Networks Max Marks: 2

Which of the following are true:

(1.) A CRC of length R is calculated over a message of length M bits. The CRC will detect all errors in the message.

(2.) The strings 10001 and 11001 have a Hamming distance of one.

(3.) If a single parity bit is added to a message, the resulting code set has a minimum Hamming distance of two.

(4.) A larger Hamming distance is needed to detect errors than to correct errors.

Time taken to answer this question 00:01:12 hrs

Hide Answer Add Notes View Notes Show Comments

A. All are true

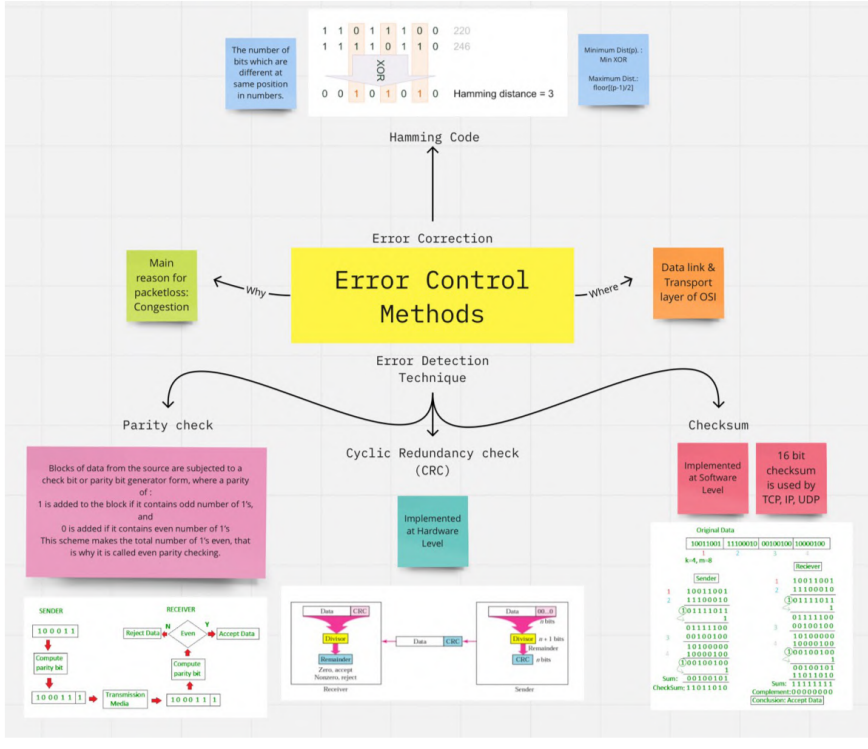
B. 2 and 3 are true — Correct Option

Solution:
Ans: b
Explanation: 1. Detects only single and double bit errors
2. Yes, only one bit change so hamming distance is only one.
3. True, To detect d errors the minimum hamming distance needed is d+1
Single parity-check codes can detect all single-bit errors.
So hamming distance will be d+1 =2
4. To detect errors d =1 code and to correct errors 2d+1 code

New Info.

C. 2 and 4 are true — Your answer is **Wrong**

D. 1 and 4 are true

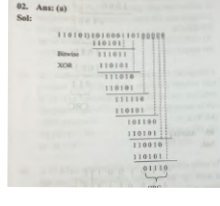


QUESTION

Error Control Questions from GATE

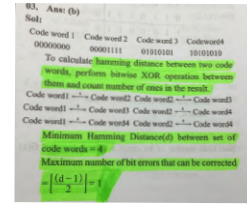
02. Consider the following message M = 1010001101. The cyclic redundancy check (CRC) for this message using the divisor polynomial $x^5 + x^4 + x^2 + 1$ is **(GATE-05)**

(a) 01110 (b) 01011
(c) 10101 (d) 10110



03. An error correcting code has the following code words:
00000000, 00001111, 01010101, 10101010, 11110000.
What is the maximum number of bit errors that can be corrected ? **(GATE-07)**

(a) 0 (b) 1
(c) 2 (d) 3



ANSWER

4. ISO/OSI STACK

1. ISO - OSI LAYERS

Functions

- Mandatory
  1. Error Control
  2. Flow control
  3. Access control
  4. Multiplexing and Demultiplexing
  5. Addressing
  ⋮
- optional
  1. Encryption and Decryption
  2. Checkpointing
  3. Routing
  ⋮

⇒ To implement all the above functionalities there are various Reference models which classify all the above functionalities and define what functions are carried out at a particular layer. One of the Reference model is "ISO-OSI STACK".

1) ISO - OSI
2) TCP/IP
3) ATM
4) X.25
5) IEEE (Mainly deals with LAN Technologies)

} various Reference models

⇒ ISO - OSI stands for "International standard organisation - open system interconnection".

⇒ The various layers in the OSI model are:

User Interactiveness
- ← 1) Application Layer
- ← 2) Presentation layer
- ← 3) Session Layer

Thick layer ← 4) Transport Layer

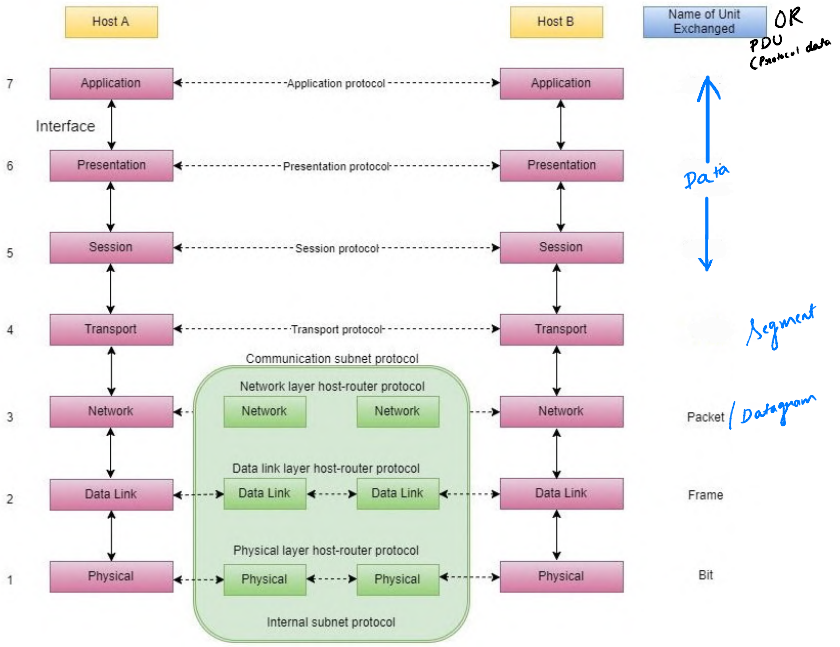
Complex ← 5) Network layer

Both hw/sw ← 6) DataLink layer

h/w ← 7) physical layer

1) 1 Advantage of Layering is
   1. Divide and conquer
   2. Encapsulation is possible
   3. Abstraction.
   4. Testing is made easy

{ Google out: RFC (Request for comments) for learning CN }



OSI Layer	Purpose
Application	Application Program
Presentation	Data Interpretation
Session	Remote Actions
Transport	End-to-End Reliability
Network	Destination Addressing
Data Link	Media Access & Framing
Phvsical	Electrical Interconnect

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP	Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

BGP
(Border Gateway Protocol)
→ State full Protocol

2. PHYSICAL LAYER

⇒ physical layer deals with Electrical, Mechanical, Functional, procedural charectaristics of physical Links.

⇒ Transmission modes: (S) ⟶ (R) (simplex / half duplex)

(S) ⇄ (R) (walkie talkies)

(S) ⇄ (R) (Full duplex)

No. of duplex/simplex link is independent of Topologies

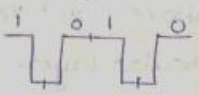
⇒ Deals with Topologies.

⇒ Deals with Encoding (Bits → Signals, waves) 1010

MANCHESTER ENCODING

1 - Represented by ⌐¬

0 - Represented by ¬⌐

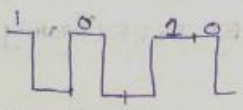


DIFFERENTIAL MANCHESTER ENCODING

0 - Represented by ⊓ ⊔

1 - Represented by ⌐ ⌐

1010

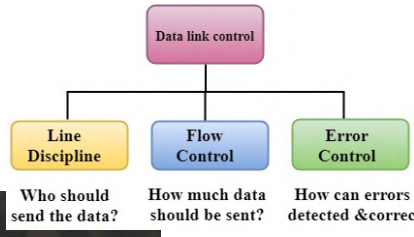


In both the Encodings (Manchester and Differential manchestor)

Baud Rate = 2* Bit rate { Baud = a letter with 4 letters
Bit = a letter with 3 letters }

Baud Rate = No. of voltages that are being sent per second

Bit Rate = No of Bits that are sent per second.



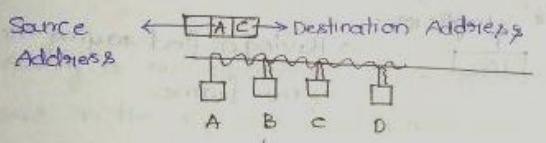
3. INTRODUCTION TO DATA LINK LAYER

The main functions of DLL are
1> Flow control (SAW, GBN, SR)
2> Error control (CRC, checksum)
DLL — Tcp/IP
3> Framing
4> physical Addressing
5> Access control (CSMA/CD, Token passing..)

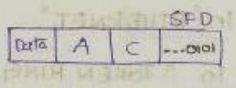
4. FRAMING AT DLL

⇒ At DLL we are mainly talking about LANS and all the LANS are multiaccess channels (All the stations are connected to a single Broadcast medium)

⇒ Framing is nothing but taking the data from the above layer (NL) and putting it in a frame and sending it



⇒ The starting of the packet is seen by B and it will discard it as the destination Address is 'C', so every station should know that a frame is Begining so it has a special field called "SFD" (Starting Frame Delimiter)



⇒ Now, SFD Represents that the frame is comming and Alerts all the stations, generally "SFD" is a sequence of bits that is entirely different from the data

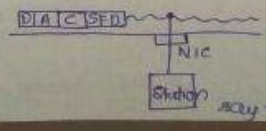
The bits in the "SFD" can be represented with the help of Regular Expression

$(10101010\cdots11)(0+1)^*$

SFD — The data that is present

Now we can convert Regular Expression → DFA → Sequential Circuit (Built using Flipflops)

Now, this sequential circuit has the capability of Recognising the Bits/RE ie $(10101010\cdots11)(0+1)^*$ so,



At this point the sequential circuit alerts the station and say that see a frame is going if it is for

⇒ It is not just enough that you identify the start of the frame (SFD) it is important to find where the frame ends.

⇒ Traditionally framing has been divided into two types — Fixed Length, Variable Length

⇒ The disadvantage of Fixed Length framing is It has Internal Fragmentation

Ex: L = 1000 Bytes ⇒ The min and max amount of data that can be sent is 1000 Bytes, if i have to send 100B then ??

100B + [900 Bytes] Dummy bits Added [This procedure is called padding].

⇒ To identify the ending of frame there are two methods they are,

1. Having a field saying the Length of the frame
2. Having an Ending Delimiter

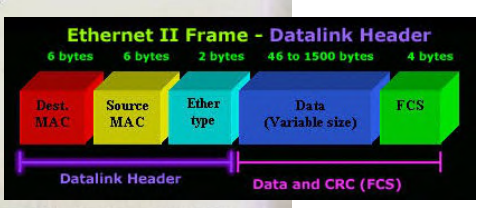
a) Length = 10 | length = 1000 | Length = 100

[10] [1000] [100]

⇒ Having a field saying the length of the frame.

b) Having the End Delimeter: [ED | D | A | C | SFD]

ED: End of the frame transmited — D: Data — A: Source Address — C: Destiny Address — SFD: Starting of frame

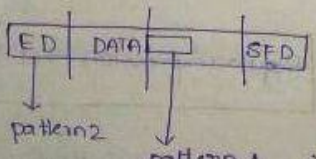


⇒ Fixed Length frames are used in "ETHERNET."

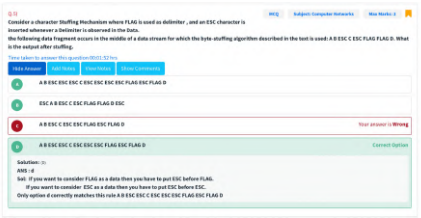
⇒ Variable Length frames are used in "TOKEN RING."

⇒ The problem with having the length field is, if it gets corrupted then Receiver reads only the data upto the modified value of Length field.

⇒ The problem with End delimeter is if ED pattern matches with Data(part) then the receiver cannot scan the entire data available



if p1 = p2 then Receiver scans only a part of data


Q.11 MCQ Subject: Computer Networks Max Marks: 2

Consider a character Stuffing Mechanism where FLAG is used as delimiter , and an ESC character is inserted whenever a Delimiter is observed in the Data.
the following data fragment occurs in the middle of a data stream for which the byte-stuffing algorithm described in the text is used: A B ESC C ESC FLAG FLAG D. What is the output after stuffing.

Time taken to answer this question:00:01:32 Sec

Hide Answer | Add Note | Flag Note | Show Comments

a) A B ESC ESC C ESC ESC ESC ESC FLAG ESC FLAG D

b) ESC A B ESC C ESC FLAG FLAG D ESC

c) A B ESC C ESC ESC FLAG ESC FLAG D — Your answer is Wrong

d) A B ESC ESC C ESC ESC ESC FLAG ESC FLAG D — Correct Option

Solution:

ANS : d

Sol: If you want to consider FLAG as a data then you have to put ESC before FLAG.

If you want to consider ESC as a data then you have to put ESC before ESC.

Only option d correctly matches this rule A B ESC ESC C ESC ESC ESC FLAG ESC FLAG D

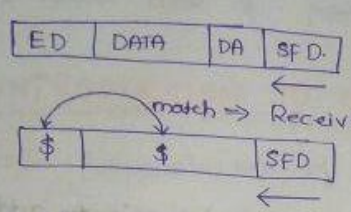
⇒ End Delimeter can be dealt in 2 ways they are : charecter stuffing

Bit stuffing.

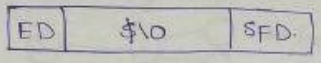
(21)

CHARECTAR STUFFING

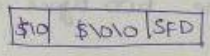
⇒ OBSELETE TECHNOLOGY



⇒ so, add a null charectar after $ so that the Receiver thinks /sees a '\0' followed by a '$ then it assumes it is not the end of data and it discard the Null charectar and scans the entire data.

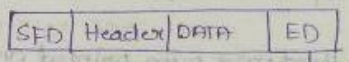


Now, if ED = $\0 and the data is $\0 then there is problem so add again null charectar $\0\0 to the data. ⇒



⇒ so Adding a Null charectar for each and every match with the charectar present in the ED is called "charecter stuffing."

BIT STUFFING (V. Imp FOR GATE)



↳ 01111

Sender

D: 01111

⇓

D: 011101 ⟶ 0111 ⊗ 1

D: 011101 ⟶ 0111 0 1 ⇒ 01111

(0 inserted after four consecutive 1s)

→ The rule at sender side is when you see 0,3 1's add an zero

If ED = 011111

Sender side

D: 011110

SD: 0111100 (After four ones add a zero)

D: 011111

SD: 0111101

Receiver side

D: 0111100

01110

SD = Stuffed Data

1) ED = 01111
D = 0111 000 11110 } Now, what is the data after Bit stuffing?

Sol Data = 0 111 000 11110

Stuffed Data = 0111 0 000 111010

2) ED = 0111111

Data ⇒ At the sender after the Run of 6 ones im going to add zero

= 0111111 0 1

⇒ At the Receiver side after a '0' followed by 6 ones im going to delete a zero.

4. PHYSICAL ADDRESSING

There are two types of Adresses { physical address - static, constant; Logical Address. }

⇒ Now, physical Address should be unique within the Network

⇒ Logical Address should be unique in the entire World wide web.

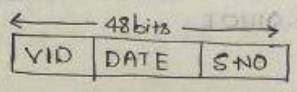
⇒ Ip Address = 32bit Number, software num.

⇒ MAC Address = 48bit Number, Hardware num printed on our "NIC" → ROM → MAC

The MAC Address is divided into three parts (unequal lengths) theyare

1. The Manufacturer ID or VendorID
2. What is the date of manufactoring
3. Serial NO. of the device on that day

} UNIQUE GLOBALLY



⇒ Conceptually Both Ip, MAC Addresses can be logical but only Ip Addresses is used for Logical Address because the info in the Ip Address (NID, HID) are sufficient for Routing the packets. where as this is not the case in MAC Addressing.

⇒ MAC is a physical Address.

⇒ "APPLE TALK" is the N/w in the world that doesnot use the MAC Address it artificially generates a random Number and assign to the users.

⇒ Data Link Layer is divided into two parts they are: 1> Logical Link Control
2> Medium Access control

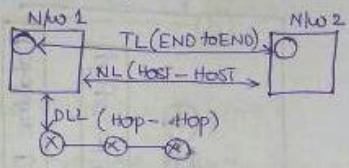
⇒ LLC takes care of Error control, Flow control, (12)

⇒ MAC takes care of Framing, Access control, Error control, physical Address

L-6: INTRODUCTION TO NETWORK LAYER

The main Responsibilities of Network layers is

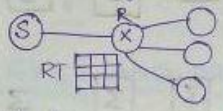
1> Host to Host connectivity



2> Logical Addressing

3> Switching (connecting various Networks together)

4> Routing



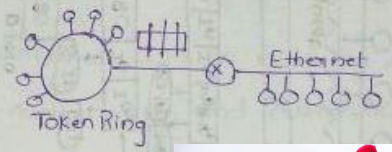
⇒ Building the Routing table = Routing

⇒ Using the Routing table = Switching

Not in Syllabus

5> Congestion Control

6> Fragmentation.



Max frame size = 1500B

7. TRASPORT LAYER

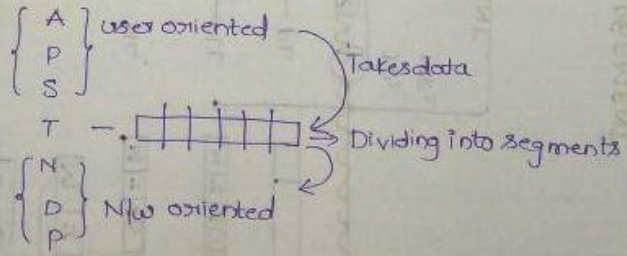
The main Responsibilities are

1> End to End communication using port numbers (port nos are also called Service point Addressing)

2> Flow control (SR)

3> Error control (checksum)

4> Segmentation ⇒



5> Multiplexing and Demultiplexing.

6> Congestion control

8. HOW ALL THE LAYERS WORK TOGETHER

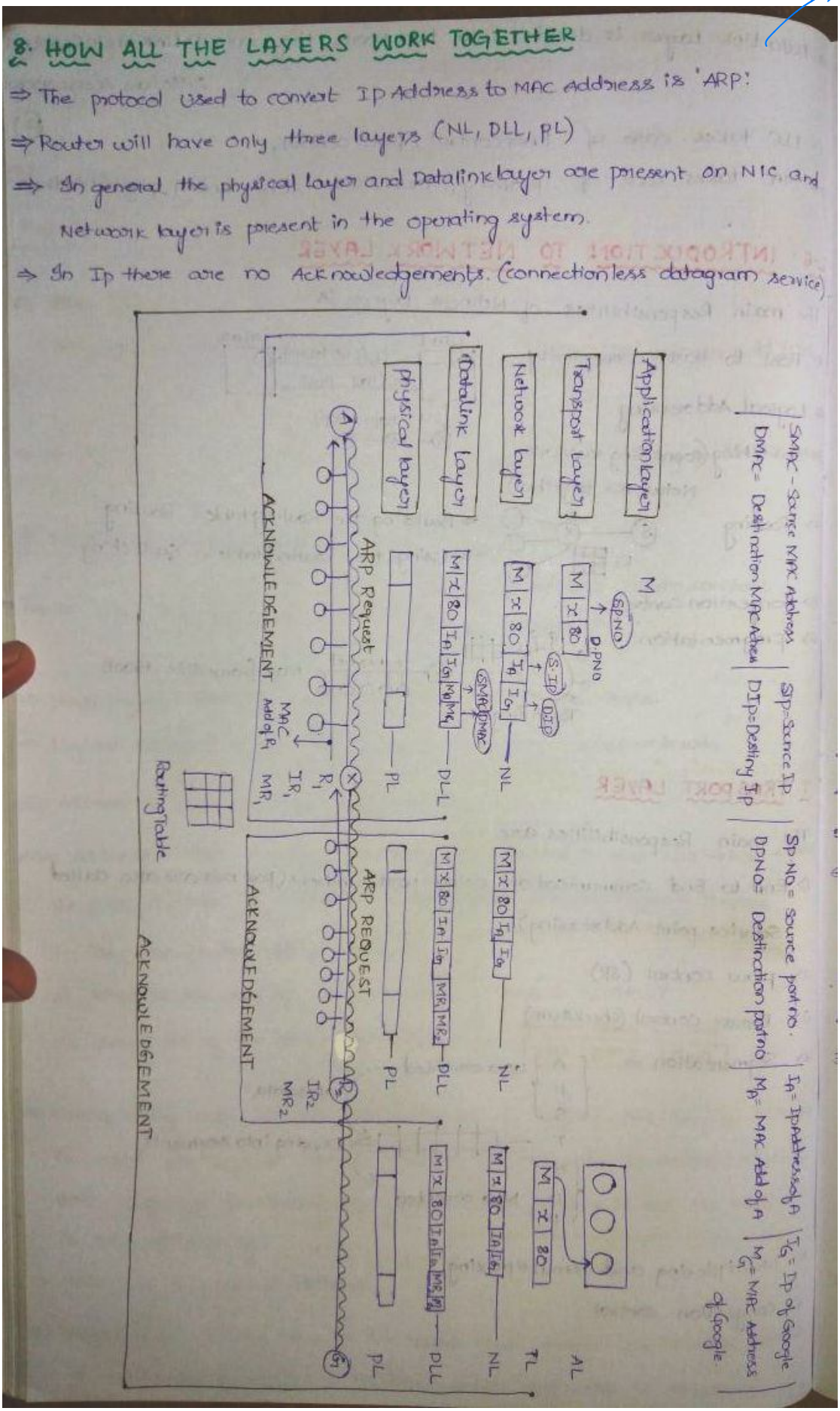
⇒ The protocol used to convert IP Address to MAC address is 'ARP'.

⇒ Router will have only three layers (NL, DLL, PL)

⇒ In general the physical layer and Datalink layer are present on NIC, and Network layer is present in the operating system.

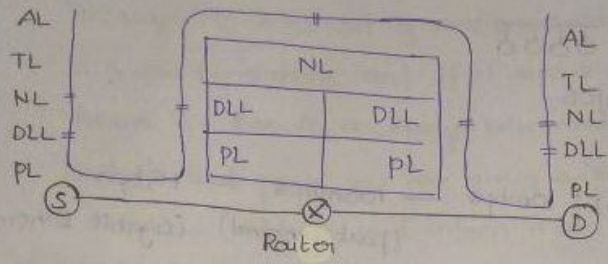
⇒ In IP there are no Acknowledgements. (Connectionless datagram service)

Refer Video for Detail Explanation



Imp points for Gate

⇒ Routers have only 3 layers 1.PL 2.DL 3.NL



= The no of times a packet hit the DataLink layer = 4

= The no of times a packet hit the Network Layer = 3.

= Depending on No of Routers we have the no of time each layer hits depend.

9. SESSION LAYER AND PRESENTATION LAYER

SESSION LAYER

1) passwords and usernames will be dealt by session layer

2) Main Responsibility Authorization and Authentication (using Digital signatures)

3) check pointing (Torrentz example).

4) Synchronization.

5) Dialog control

6) Logical Grouping of operations

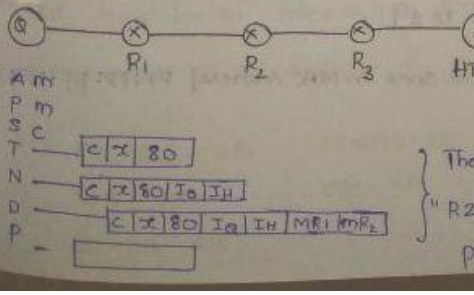
PRESENTATION LAYER

1) character translation

2) Encryption and Decryption.

3) Compression (.zip)

GATE - 2014



} These are the situations when the packet reaches "R2." ⇒ Intruder could find Ip's of S,H and port numbers of S,H

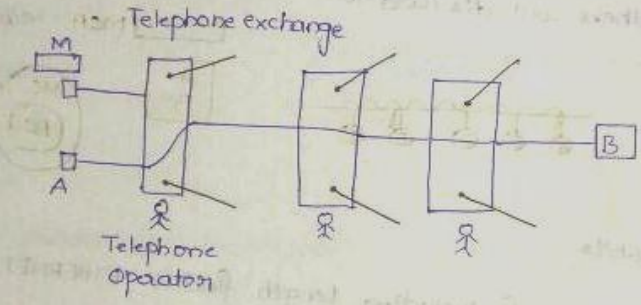
6. SWITCHING

1. INTRODUCTION TO SWITCHING

Switching
- Circuit switching ⇒ Applied at physical Layer, Obsolete technology.
- Message switching
- Packet switching
  - Virtual circuits switching
  - Datagram switching.

⇒ Switching is done at Network Layer

2. COMPARISION BETWEEN CIRCUIT SWITCHING AND PACKET SWITCHING



Let M = size of total message that 'A' wants to send to 'B'.

B = Bandwidth of the entire channel

X = No. of Hops

d = Length of Each hop

V = Velocity of signal

Total time taken to send message 'm' to 'B' is = Setup time (connection establish time) $+ T_t + \frac{xd}{V}$

$= \text{Setuptime} + \frac{M}{B} + \frac{xd}{V} + TD$ { T_p btn two hops $= d/V$ ∴ In btn x hops $= x \cdot \frac{d}{V}$ }

→ Teardown the link

$$TT = \text{Setuptime} + M/B + \frac{xd}{V} + TD$$

∴ packetization is the process of dividing the data into packets and transmitting.

⇒ The packetisation process helps in reducing the total transmission time and the size of the packet should not be so small if it is the case the total time taken to transmit the data will increase. so the packet size must be choosen Appropriately.

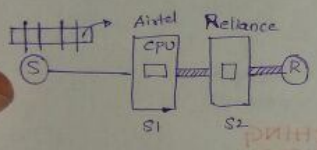
4. VIRTUAL CIRCUITS AND DATAGRAMS

There are two types of packet switching they are Virtual circuits, Datagrams

⇒ our phone call is going through Virtual circuit.

⇒ our Data usage is going through Datagram circuit

Virtual circuit



1> Headers are not Required

2> for the 1st packet, Global Header for other packets, local header

3> Connection oriented (Resource Reservation) if Resources are Reserved then it is connection Oriented. (Buffer, CPU, Bw)

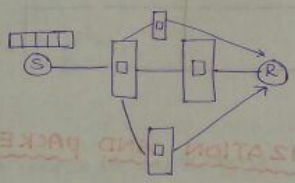
4> Same path → In order packets

5> Highly Reliable

6> Costly

7> ATM (Asynchronous Transfer mode) Network uses ATM. VC.

Datagram Circuit



1> Headers are Rd for all packets

2> Connectionless oriented

3> NoGuarantee, they may follow diff path, they may appear out of order.

4> Not Reliable

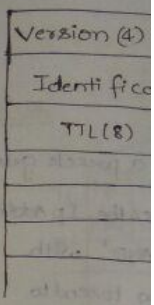
5> Not very costly.

6> Viber, whatsapp call have VoIp (VOICE OVER INTERNET PROTOCOL)

7> Ip Network uses Datagram

1. INTRODUCTIO

IpV4 Header



TTL:

Here the min
HLF is of 4
so we use th
∴ If

VERSION: The
if version=
appropriately.

2. IDENTIFICA

⇒ Identification
Out of a host.
we do fragm
number.

Circuit Switching	Packet Switching	
	Virtual Circuit Switching	Datagram Switching
Connection oriented service	Connection oriented service	Connection less service
Ensures in order delivery	Ensures in order delivery	Packets may be delivered out of order
No reordering is required	No reordering is required	Reordering is required
A dedicated path exists for data transfer	A dedicated path exists for data transfer	No dedicated path exists for data transfer
All the packets take the same path	All the packets take the same path	All the packets may not take the same path
Resources are allocated before data transfer	Resources are allocated on demand using 1st packet	No resources are allocated
Stream oriented	Packet oriented	Packet oriented
Fixed bandwidth	Dynamic Bandwidth	Dynamic bandwidth
Reliable	Reliable	Unreliable
No header overheads	Only label overheads	Higher overheads
Implemented at physical layer	Implemented at data link layer	Implemented at network layer
Inefficient in terms of resource utilization	Provides better efficiency than circuit switched systems	Provides better efficiency than message switched systems
Example- Telephone systems	Examples- X.25, Frame relay	Example- Internet

Circuit Switching	Packet Switching
In circuit switching there are 3 phases: i) Connection Establishment. ii) Data Transfer. iii) Connection Released.	In Packet switching directly data transfer takes place .
In circuit switching, each data unit know the entire path address which is provided by the source.	In Packet switching, each data unit just know the final destination address intermediate path is decided by the routers.
In Circuit switching, data is processed at source system only	In Packet switching, data is processed at all intermediate node including source system.
Delay between data units in circuit switching is uniform.	Delay between data units in packet switching is not uniform.
Resource reservation is the feature of circuit switching because path is fixed for data transmission.	There is no resource reservation because bandwidth is shared among users.
Circuit switching is more reliable.	Packet switching is less reliable.
Wastage of resources are more in Circuit Switching	Less wastage of resources as compared to Circuit Switching
It is not a store and forward technique.	It is a store and forward technique.
Transmission of the data is done by the source.	Transmission of the data is done not only by the source, but also by the intermediate routers.
Congestion can occur during connection establishment time, there might be a case will requesting for channel the channel is already occupied.	Congestion can occur during data transfer phase, large number of packets comes in no time.
Circuit switching is not convenient for handling bilateral traffic.	Packet switching is suitable for handling bilateral traffic.

[NAT, Easy]
Que: 1: Consider a circuit-switched network with a bandwidth of 10 Mbps. How many users can the network support if half of the users want 50 Kbps and half of them want 450 Kbps ?

$\frac{x}{2} \cdot 50 + \frac{x}{2} 450 = 10,000$

$500x = 20,000$

$x = 40$

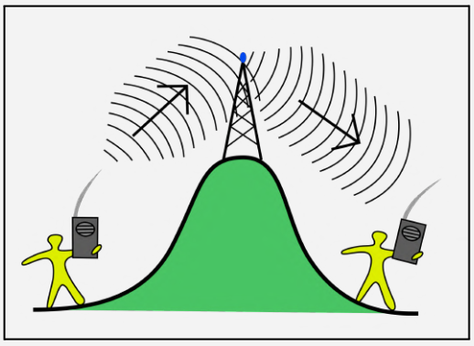
Networking Devices

LAN Wires:

10BaseT(10 Mbps, No Mux, 100m)
10Base2(10 Mbps, No Mux, 200m); BASE stands for baseband signalling, & 2 for a maximum segment length approx 200 m
10Base5(10 Mbps, No Mux, 500m)
100Base(100 Mbps)

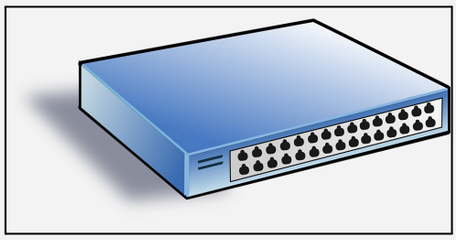
- All operations are physical layer
- Collision is possible

Repeater:



- A repeater operates at the physical layer.
- Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.
- It is a 2 port device and connects 2 same types of Network.

Hub:

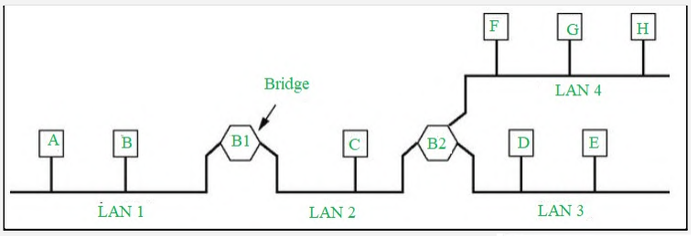


- A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches., eg: the connector in star topology which connects different stations.
- Hubs cannot filter data, so data packets are sent to all connected devices.
- They do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

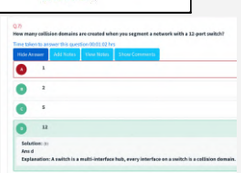
Traffic - ↑

Bridge:

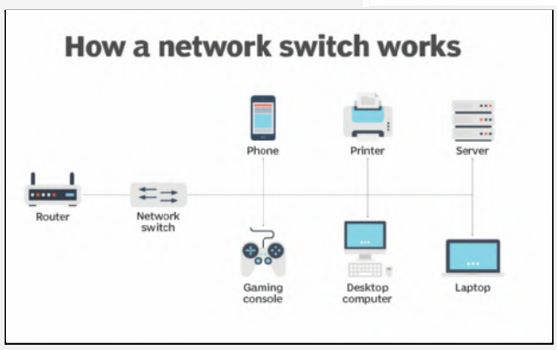
[GATE-2004]



- A bridge operates at the data link layer.
- A bridge is a repeater, which adds on the functionality of filtering content by reading the MAC addresses of source and destination.
- It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.
- Reduces Collision domain.
- Bridges uses Spanning tree Algorithms to avoid looping. As they can't use TTL at DLL.



Switch:



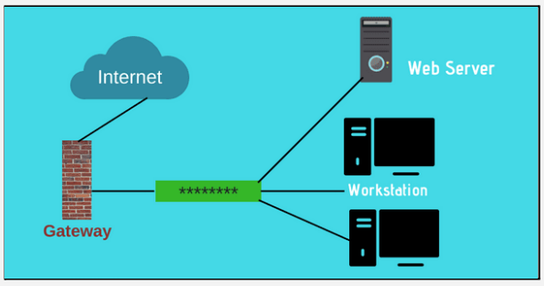
- A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance.
- A switch is a data link layer device.
- The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

Routers:

- The router is mainly a Network Layer device that connects two networks of the same type.
- A router is a device like a switch that routes data packets based on their IP addresses.
- Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Routers divide broadcast domains of hosts connected through it.
- There are two types of routings
    - Router routing, where the router decides the outgoing route of the packet.
    - Source Routing, where sources can decide the route.

[GATE-2003]

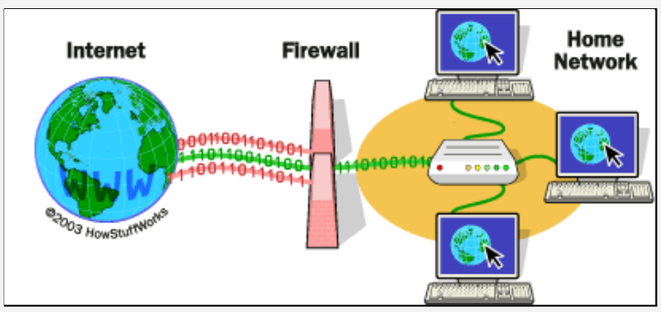
Gateway:



- A gateway is a passage to connect two networks together that may work upon different networking protocols. It basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system.
- It works from Layers 1 through 7 of the OSI Model.
- Gateways are also called protocol converters and can operate at any network layer.
- Gateways are generally more complex than switches or routers.
- Proxy ✔
- Caching ✔
- NAT(Network address Translation) ✔
- Deep Packet Inspection ✔

Firewall

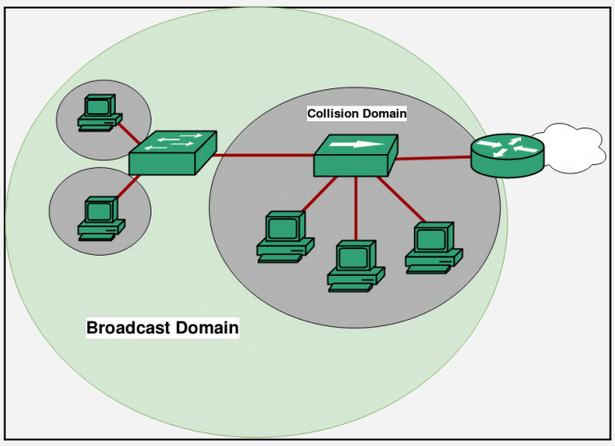
- A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.
  Accept : allow the traffic
  Reject : block the traffic but reply with an "unreachable error"
  Drop : block the traffic with no reply



- A firewall establishes a barrier between secured internal networks and outside untrusted networks, such as the Internet.
- Layer 3 firewalls (i.e. packet filtering firewalls) filter traffic based solely on source/destination IP, port, and protocol.
- Layer 4 firewalls do the above, plus add the ability to track active network connections, and allow/deny traffic based on the state of those sessions (i.e. stateful packet inspection).
- Layer 7 firewalls (i.e. application gateways) can do all of the above, plus include the ability to intelligently inspect the contents of those network packets. For instance, a Layer 7 firewall could deny all HTTP POST requests from Chinese IP addresses. This level of granularity comes at a performance cost, though.
  For Story of (Verizon, 2009) where the attacks came from inside the Firewall, read Tanenbaum-CN : 8.6.2 Firewall

Collision Domain

A Collision Domain is a scenario in which when a device sends out a message to the network, all other devices which are included in its collision domain have to pay attention to it, no matter if it was destined for them or not. This causes a problem because, in a situation where two devices send out their messages simultaneously, a collision will occur leading them to wait and re-transmit their respective messages, one at a time.
Remember, it happens only in case of a half-duplex mode.



Broadcast Domain

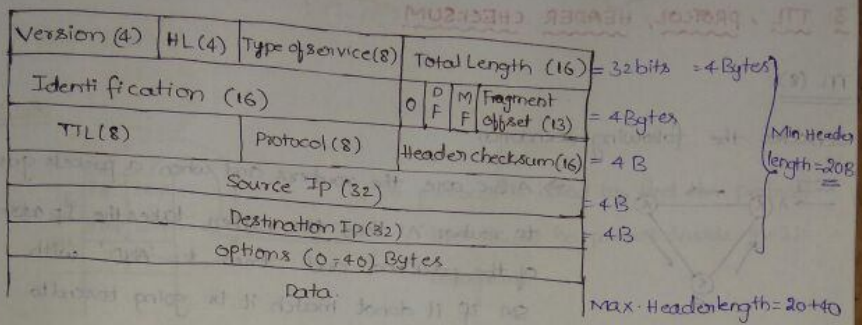
A Broadcast Domain is a scenario in which when a device sends out a broadcast message, all the devices present in its broadcast domain have to pay attention to it. This creates a lot of congestion in the network, commonly called LAN congestion, which affects the bandwidth of the users present in that network.

Networking Devices	Broadcast Domain	Collision Domain
Repeater	Same	Same
Hub	Same	Same
Bridge	Same	Reduces
Switch	Same	Reduces
Routers	Reduces	Reduces
Gateway	Reduces	Reduces

7. INTERNET PROTOCOL

1. INTRODUCTION TO IP HEADER

IpV4 Header



HL:

Here the min size of the Header is 20B but the Header Length field HLF is of 4 bits ∴ only the numbers ranging from (0-15) can be represented so we use the process called scaled Arithematic (divide by 4)

∴ If Header Length = 20B ⇒ HLF contain (5)

HL	HLF
20B ⟶	5
32B ⟶	8
40B ⟵	10

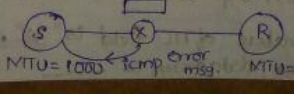
⇒ In exam if a number is given, and if you want to identify it whether it is a Header Length or Header Length field the process is convert it to decimal and check the Ranges HL (20B - 60B)
HLF (5 - 15).

VERSION : The version (of the Ip Address IPv4 / IPv6) If version = 0100 = IPv_4
if version = 0110 ⇒ IpV_6 ⇒ the packet must be parsed by the parsers appropiately.

2. IDENTIFICATION, MF, DF AND FRAGMENT OFFSET

⇒ Identification number is used to number every datagram that is going out of a host. This field is mainly used when we do Fragmentation, when we do fragmentation all the fragments are going to get same identification number.

⇒ DF: Donot priagment



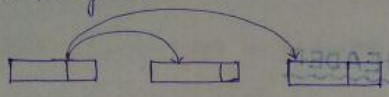
Purpose of Running NAT(Network address translation)
To connect to internet and your host don't have a global unique IP address.
if you change to a new ISP that requires you to re-number your network.
You require two intranets with duplicate addresses to merge

Fields in IP header for fragmentation –

- **Identification (16 bits)** – use to identify fragments of the same frame.
- **Fragment offset (13 bits)** – use to identify the sequence of fragments in the frame. It generally indicates a number of data bytes preceding or ahead of the fragment.
  Maximum fragment offset possible = (65535 − 20) = 65515
  (where 65535 is the maximum size of datagram and 20 is the minimum size of IP header)
  So, we need ceil($\log_2 65515$) = 16 bits for a fragment offset but the fragment offset field has only 13 bits. So, to represent efficiently we need to scale down the fragment offset field by $2^{16-13} = 8$ which acts as a scaling factor. Hence, all fragments except the last fragment should have data in multiples of 8 so that fragment offset ∈ N.

⇒ Fragment offset is no.of data Bytes ahead of this particular Fragment in this particular Datagram.

Ans: 26



Q. 14 — Have any Doubt ?

Consider a very large network of 5000 routers. Sender and receiver are connected with this network. Sender sends data to receiver and after some unit of time sender receives ICMP time exceeded message for the same transmitted packet. The maximum number of routers that can be travelled by packets when ICMP message reaches back to sender is _____

509 — Correct Option

Solution :
509
TTL uses 8-bit in IP header which can travel maximum of 255 routers.
Total routers travelled = 255 (going forward) + 254 (time exceeded message coming back)
= 509

NEW!

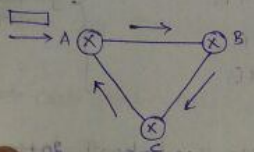
Your Answer is 255

3. TTL, PROTOCOL, HEADER CHECKSUM

TTL (8):

TTL is also used to count the number of routers between host and destination

consider the following scenario,



⇒ A, B, C are the routers and when a packets gets to router 'A' then the router takes the Ip Address of the packend and tries to 'AND' with SM if it donot match it is going to send to default entry.

⇒ Let us say, Router A default entry = Router B and Router B's default entry goes/leads the packet go to Router 'C' and Router 'C' default entry = Router 'A'. then the packet will fall in an infinite loop and will be entirely circulating and there may be some thousands of such packets, then as a results the Buffers are full, Routers will be Busy.

⇒ In order to overcome the above problem there is a Concept called "TTL (TIME TO LIVE)" in which a packet is made to circulate only upto certain no.of hops after that many hops the packet will be discarded.

⇒ The main purpose of TTL is to discard the packet that falls in infinit eloop

⇒ THE TTL VALUE WILL BE DECREMENTED ONLY AT THE INTERMEDIATE ROUTERS AND THE DESTINATION.

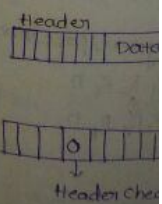
GATE -14 paper 02

In the diagram shown below, L1 is an Ethernet LAN and L2 is a Token Ring LAN. An Ip packet originates from sender 'S' and traverses to 'R', as shown. The Links within each ISP and across the two ISP, are all point-point optical Links. The initial value of TTL field is "32". The max possible value of TTL when R Receives the datagram is ____

PROTOCOL

⇒ Now consider
Buffers at t
at their fu
Buffers are
it is better
packet is T
is a Reliable
instead ch
ICMP, IGM
of more
in which the

HEADER CHECKS



Q. 14 — FAQ — Have any Doubt ?

Which of the following statement is/are correct regarding IPv4 Datagram Header?

A. The minimum value for HLEN field is 5 and the maximum is 20. — Your answer is IN-CORRECT

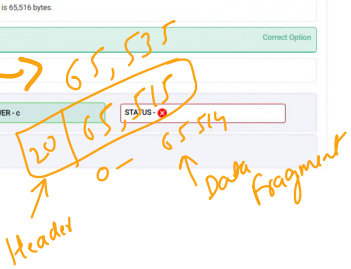
B. Total Length field has a minimum value 20 bytes and the maximum is 65,516 bytes.

C. Fragment Offset is maximum value of 65,514 bytes. — Correct Option

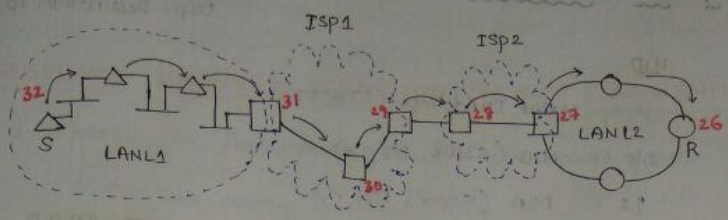
D. None of these

YOUR ANSWER - a | CORRECT ANSWER - c | STATUS -

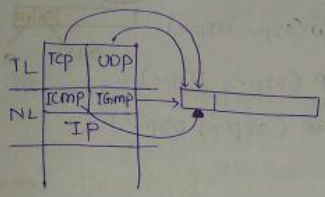
Solution :
(c)



Ans 26

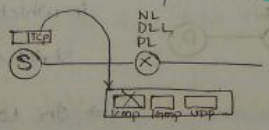


PROTOCOL

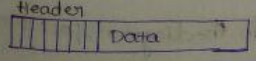


⇒ protocol field is used to find the protocol that could be present inside the IP Datagram.

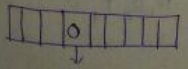
⇒ Now consider the following scenario where Tcp packet is sent, and the Buffers at the Routers are full which means the Buffers are operating at their full capacity. Now if you send a packet to a router whoose Buffers are full, then the router discards it. But before discarding it it is better that what kind of data is present in the datagram, if the packet is Tcp, the sender is going to send the same packet again as Tcp is a Reliable protocol. so if the packet is Tcp dont discard the packet, instead check the Buffers if you find the packets with the protocols ICMP, IGMP discard them and make room for the Tcp packet as it is of more Importance. so that is why we need protocol field. The order in which the router discards the packets is 1) ICMP 2) IGMP 3) UDP 4) Tcp



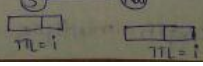
HEADER CHECKSUM(16):



⇒ 16Bit ⇒ 16Bit checksum ⇒ The Header is divided into no of parts each of size = 2Bytes = 16 Bits



Header Checksum (Initially Zero)

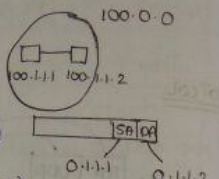


1) FO, MF, TTL
2) Options.
3) HL

SOURCE IP AND DESTINATION IP

SIp = Source Ip Add
DIp = Destination Ip Add

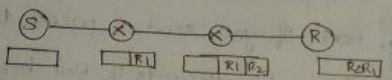
NID	HID	
✓	✓	Valid IpAddress (SIp, DIp)
✓	0's	NID (SIpx, DIpx)
✓	1's	DBA (SIpx, DIp✓)
1's	1's	LBA (SIpx, DIp✓)
1's	0's	SM or NM (SIpx, DIpx)
0's	✓	Host within a N|w (SIp✓, DIp✓)
0's	0's	I dont have Ip (SIp✓, DIpx)
127	✓	Loop back Address (SIpx, DIp✓)



5. OPTIONS

⇒ This field is optinal

Record Route:



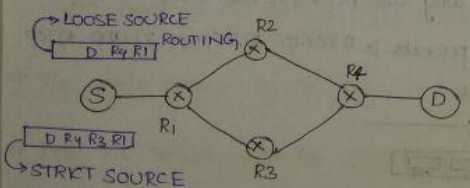
The max no of Ip Address that could be recorded ona packet is "9".

⇒ Ip Address length = 4B

⇒ optional field max length = 40B ⇒ Max no of Ip Add = 10 Ips

But one field is used to indicate the type of option: 10 − 1 = 9

SOURCE ROUTING



⇒ You will specify the entire path in which a packet must go in Strict source Routing

⇒ In Loose source routing you will indicate the Routers from which your packet must definitely go

⇒ In the diagram, packet may go as $R_1 R_2 R_4 D$ or $R_1 R_3 R_4 D$.

⇒ In addition padding is also done at "options" inorder to make Header Length multiple of '2'.

1. DIFFERENCE

MTU = Maxi
frame

⇒ The next field

∴ The max s

Sol: Record Route option in the IP header is used to record the path taken by the Echo Request message and corresponding Echo Reply message (available on IPv4 only). Each hop in the path uses an entry in the Record Route option. If possible, specify a *Count* that is equal to or greater than the number of hops between the source and destination. The *Count* must be a minimum of 1 and a maximum of 9.

The **maximum number** of addresses or names in the host list is 9

⇒ Ip is a protoc
the max size o

⇒ If we remov
payload/ datap

⇒ Here we are c
at each and eve
= 20B

⇒ Now Applicatio
now it is the
given by AL int
the process of

⇒ Now the data f
the problem is
Ethernet then

8. FRAGMENTATION

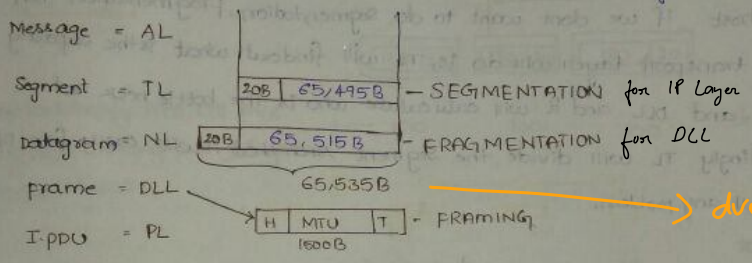
1. DIFFERENCE BETWEEN SEGMENTATION AND FRAGMENTATION

MTU = Maximum Transmitable Unit (The max amount of data that DLL frame can carry is called MTU)

⇒ The next field in the Header format = Total Length = 16b

∴ The max possible number with 16bits = $2^{16}-1$
= 65,535

∴ The max size of datagram that could be present in Ethernet in these days = 65,535



due to 16 bit only in Identification section of IP Header

⇒ Ip is a protocol that operates at Network layer. And now, at N/w layer the max size of datagram is 65,535 ⇒ Total amount of data + Header = 65,535

⇒ If we remove the Header from the data then the remaing data is called payload/ Datapart at that layer.

⇒ Here we are caluculating the max amount of data that can be accomodated at each and every layer, to get max. data the Header Length should be min = 20B

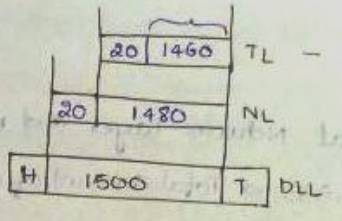
⇒ Now Application Layer could give any amount of data to transport layer, now it is the responsibility of the Transport Layer to divide that packet given by AL into parts so that each part could sit in 65,495B. And the process of dividing the packet into parts is called "Segmentation."

⇒ Now the data from the TL can easily fit into NL but here there is a problem, the problem is DLL has also some limitations, if the underlying LAN is Ethernet then the max size of data that can be fit is only 1500B.

which means NL is going to give you a data of 65,535 B, But DLL c hold a maximum of 1500 Bytes only. Now, NL should divide the datagram into parts, so that each part could go and sit into 1500B and that proce is called "FRAGMENTATION".

⇒ Now, once the Datagram is received by the DLL which is already fragmented, it will add Header and Tail along with preamble, SFD - and this process is called "FRAMING".

⇒ The problem Here is either the Network Layer is going to be Bottleneck or DLL is going to be bottleneck, sometimes DLL can hold the data sent by NL without fragmentation, the Bottleneck will be NL. So at the same host if we dont want to do Segmentation, Fragmentation then what transport layer will do is, TL will find out what is the capacity of NL and DLL and it will calu calate who is the bottle neck and accordingly TL will divide the Segment such that it will easily fit in DLL without any problem.



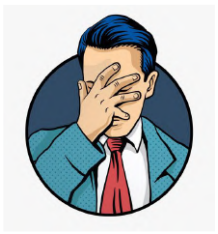
TL – SEGMENTATION ✓

NO FRAGMENTATION.

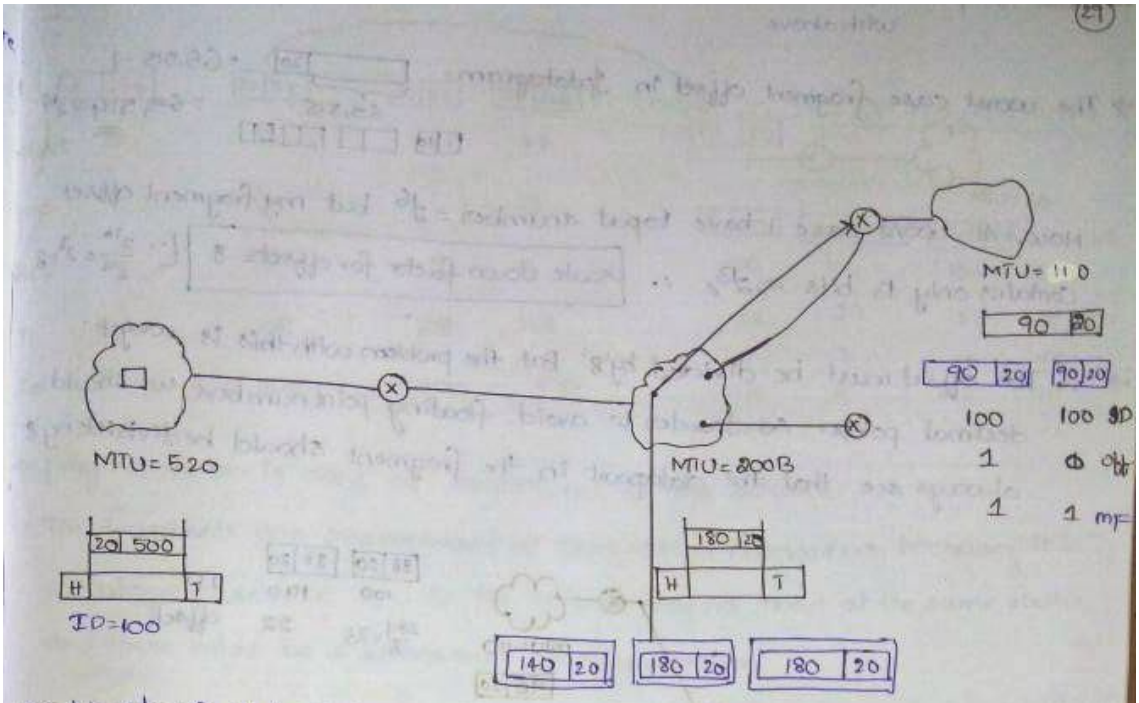
2. FRAGMENTATION EXPLAINED WITH NUMERICAL EXAMPLE

⇒ At source we do only Segmentation in such a way that there is no need of Fragmentation

⇒ MTU = Max amount of data that can sit in DLL frame



Fragment Data Packet only not IP Header.



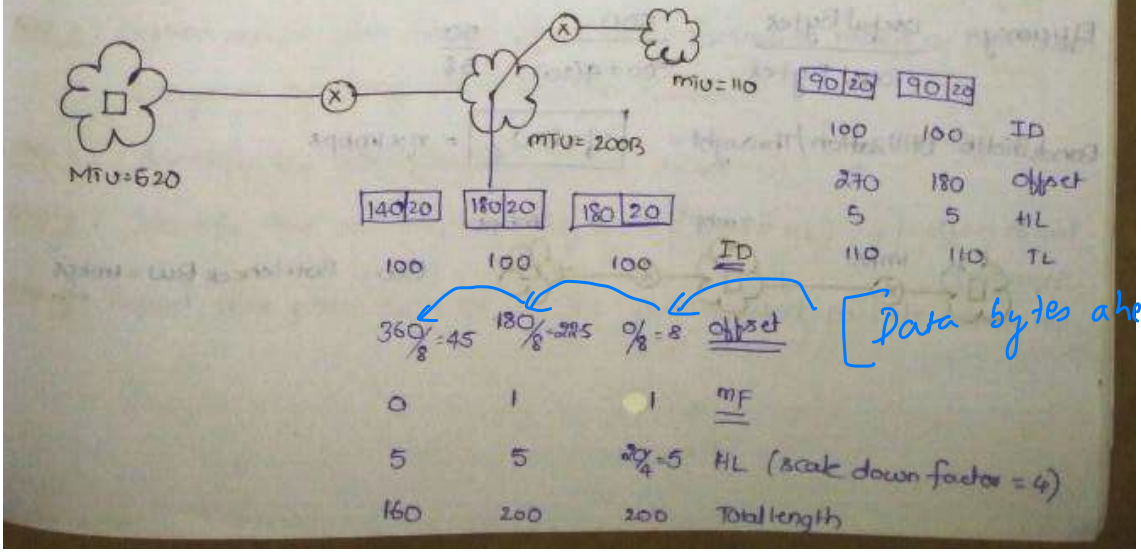
used to identify that all this Fragments belong to a datagram whose id=100

100 100 100 Identification number

2 1 0 offset (used to identify order)

0 1 1 MF (More Fragments following)

⇒ There is a problem with the above type of scenario, the offset is not actually scalable, so the offset is defined this way, offset is nothing but the no of data bytes ahead of particular fragment. so the offset will be



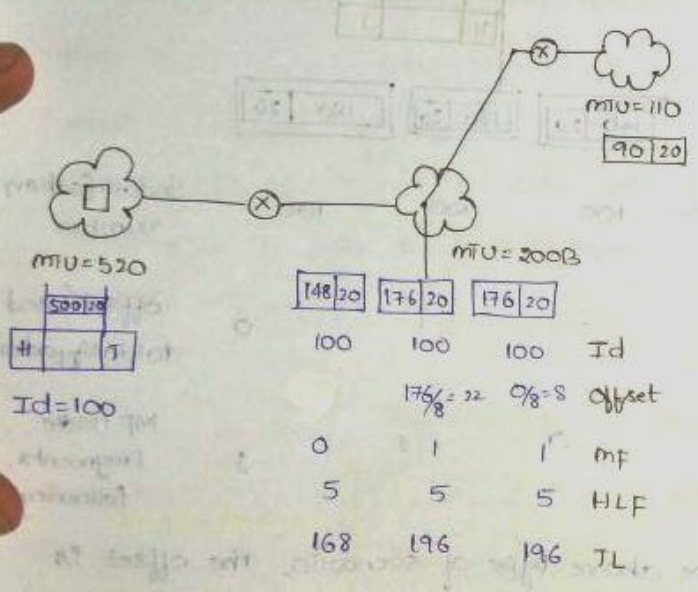
[Data bytes ahead of it.]

⇒ Now the problem scenario with above is, fragment offset = 13 bits ⇒ the max no in offset field = $2^{13}-1 \approx 8000$

⇒ The worst case fragment offset in 1 datagram = 65515 − 1 = 65,514

Now, At worst case i have to put a number = 2^{16} but my fragment offset contains only 13 bits ⇒ 2^{13} ∴ scale down factor for offset = 8 [∵ $\frac{2^{16}}{2^{13}} = 2^3 = 8$]

⇒ ∴ The offset must be divided by '8' But the problem with this is we get decimal points. So inorder to avoid floating point numbers we should always see that the datapart in the fragment should be divisible by 8



100	100	100	Id
	176/8 = 22	0/8 = 0	offset
0	1	1'	mf
5	5	5	HLF
168	196	196	TL

88 20	88 20	
100	100	ID
264/8 = 33	22	offset

∴ The offset for the last fragment can be decimal

⇒ Each fragment size should be divisible by 8

⇒ HLF should be divided with four.

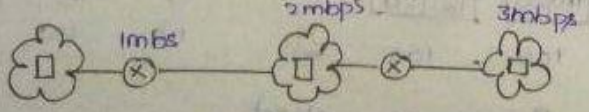
Initial data = (500B + 20B) → Split into 4 packets

Final data = 500B + (4 * 20B) ⇒ overhead = 3 headers [(4*20) − 20] = [3*20]

(Total headers; Initial header)

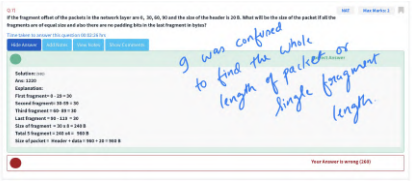
Efficiency = $\frac{\text{Useful Bytes}}{\text{Total Bytes}} = \frac{500}{500 + 4(20)} = \frac{50}{58}$

Bandwidth Utilization / Throughput = $\eta \times BW = \eta \times 1\text{mbps}$



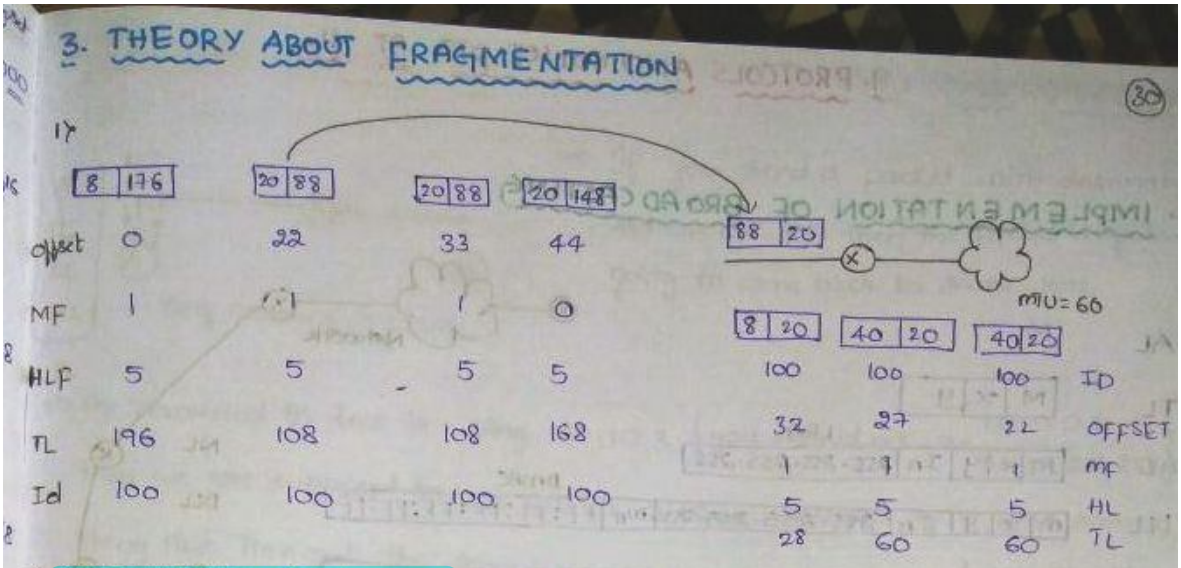
BW = Bottleneck BW = 1mbps

Router can arbitrarily drop the packets due to congestion.



Source is doing Segmentation.

3. THEORY ABOUT FRAGMENTATION



⇒ Fragmentation is done at Router, not at the source

⇒ The fragments are reassembled at Destination not routers because, it is a Datagram service and all the routers may not meet at the same router, and there might be a further need for fragmentation.

4. REASSEMBLY ALGORITHM

⇒ Depending on MF and offset the Receiver will identify that the Datagram is fragmented.

MF	offset		
1	0	⇒ Ist fragment	FRAGMENTATION
1	!0	⇒ Intermediate fragment	
0	!0	⇒ Last fragment	
0	0	⇒ only single Datagram = No Fragmentation.	

Step-1 : Destination should identify that DataGram is fragmented (MF, OFSET)

Step-2 : Destion should also identify that what fragments belong a particular datagram by using Identification number.

Step-3 : Identify the first fragment (MF=1, offset = 0)

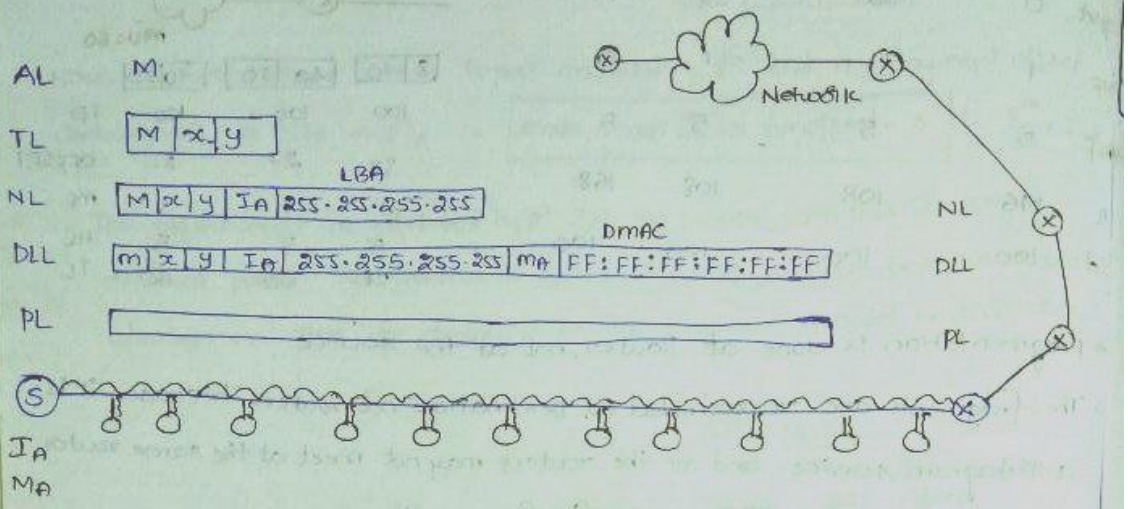
Step-4 : Identify the subsequent fragments $[(\text{Data} \div \text{HL}) \div 8]$ = offset of 2nd fragment

$[TL - (HL * 4)] \div 8$

Step-5 : Repeat this procedure for all the subsequent packets where MF=0

9. PROTOCOLS AND CONCEPTS AT NL

1. IMPLEMENTATION OF BROADCASTING

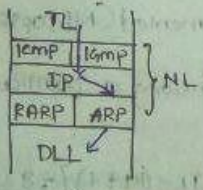


⇒ Even though Broadcasting is done at NL it cannot be done without the Broadcasting features of Data Link layer.

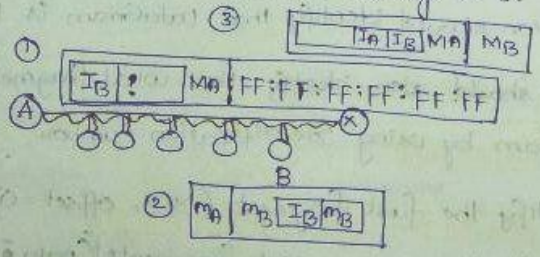
⇒ For Direct Broadcasting the field where LBA is present in above figure will be Replaced by DBA and DMAC will be filled by the next router and then router routes the packet as Unicast message and when the Router forwards to the Network then the DBA will be changed to LBA and DMAC will be all f's.

2. ARP

ARP (IP Address → MAC Address)



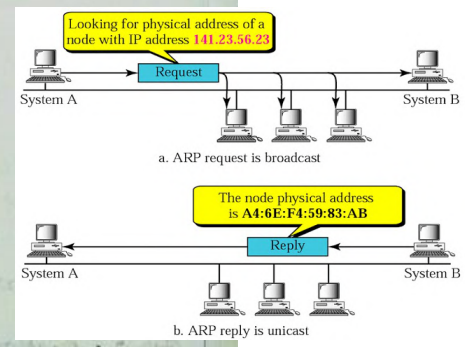
'A' wants to send message to 'B'.



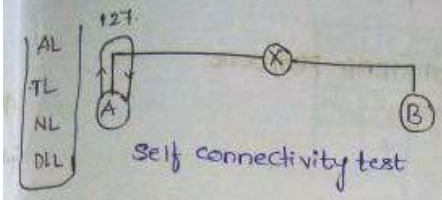
⇒ ARP Request is a Broadcasting packet

⇒ ARP Reply is a unicast packet

⇒ ARP is applied when a Router wants to find MAC Address of another Router (R-R)
host wants to find MAC Address of another host (H-H)
" " " " " router (H-R)
Router " " " " " router (R-R)



3 SPECIAL ADDRESS - 127



⇒ If you send a packet with destination Address as 127 then the packet is again going to come back to same host.

⇒ The command to test is ping 127.1.2.3 {you should not use 127.0.0.0 / 127.255.255.255} then we are supposed to see RTT as ≅ 15ms instead if it sees some thing like Time out the something is wrong in our NIC and you should start troubleshooting.

⇒ It is also called Loop Back Address

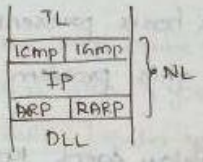
4. RARP

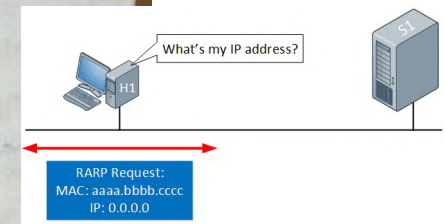
RARP = Reverse ARP (MAC ⟶ Ip)

NFS = Network File Server.

MAC → ROM

IP → RAM



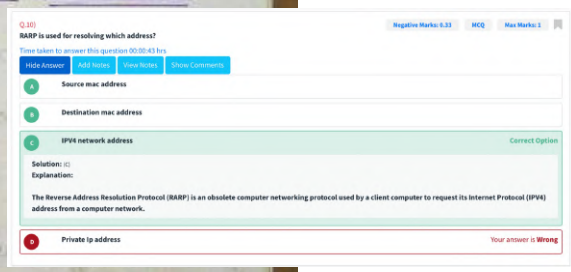


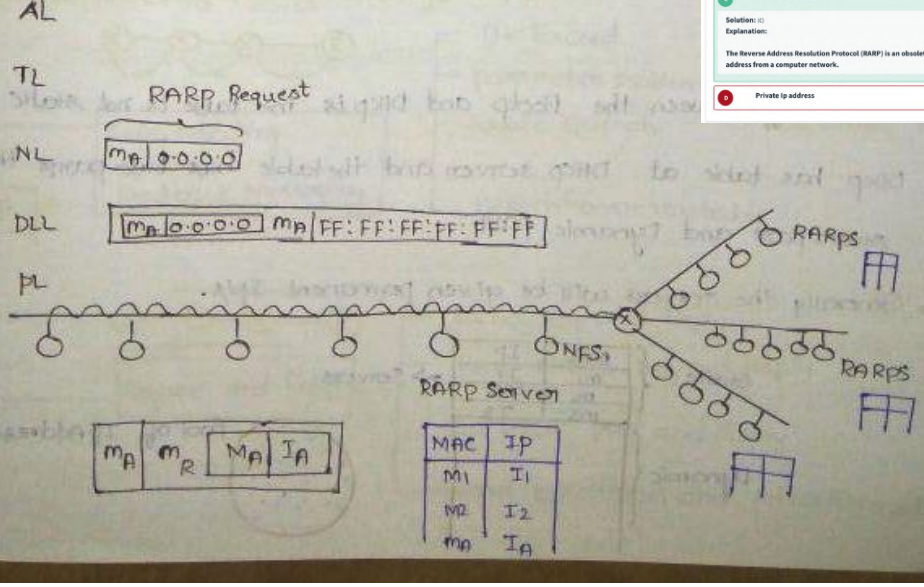
"Host asking Router"

1) The disadvantages of RARP are;

a) Every Nlw should have a RARP server OBSELETE TECHNOLOGY

b) Static mappic (no.IP > no. of Hosts)

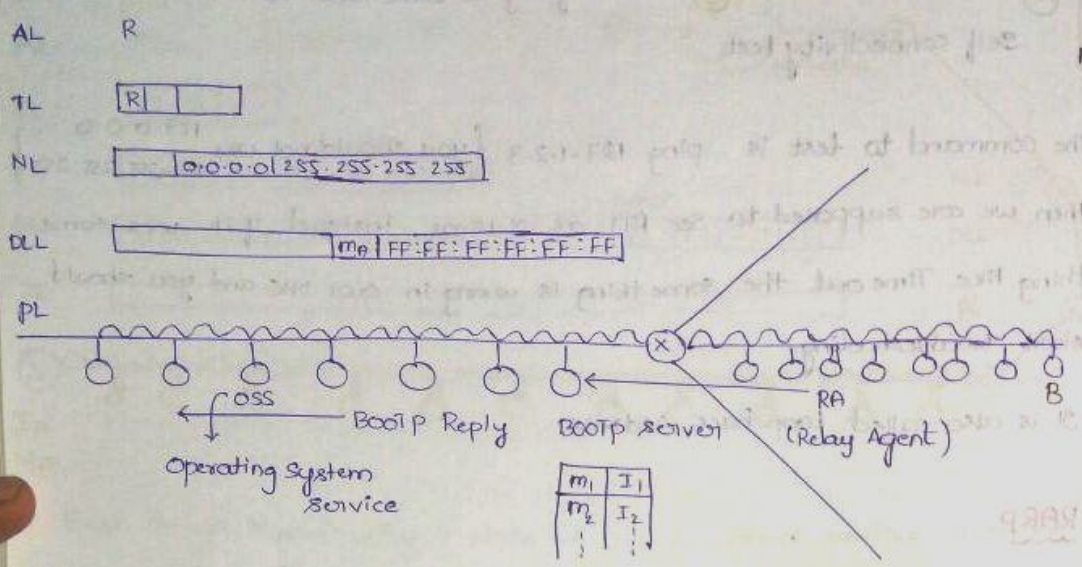




5. BOOTP AND DHCP

⇒ The main difference between Bootp and RARP is, BOOTP works at AL, and RARP works at DLL.

BOOTP = BOOTSTRAP PROTOCOL



⇒ Now the hosts present in other N/w are never going to reach the BOOTP server, this problem is solved by Relay Agent.

⇒ The Relay Agent knows the Ip Address of the BOOTP server and the packet that is Broadcasted by Station B will be Read by RA and RA will ask the Bootp server by sending a Unicast packet.

⇒ Only one Bootp server is Required

⇒ Mapping table is static.

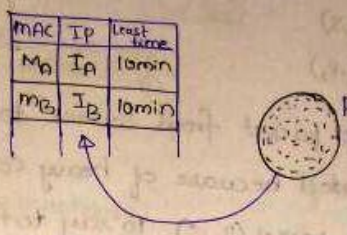
DHCP

The main diff between the Bootp and DHCP is the table is not static in DHCP

⇒ DHCP has table at DHCP server and the table has two parts they are static part and Dynamic part.

⇒ Generally the servers will be given permanent Ip's.

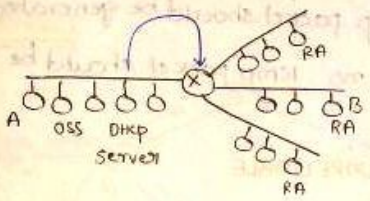
⇒ Let us say, A host M_A wants its Ip Address then the Dynamic port look like this



⇒ only one DHCP server is Enough

⇒ The Stable is a Dynamic table (NO. of Ip Address = NO. of stations online)

⇒ TO make DHCP backward compatable with BOOTP, both DHCP, BOOTP should have same port numbers.



⇒ DHCP is operated at Application layer

⇒ DHCP cannot be implemented on Router as Router has only '3' Layers

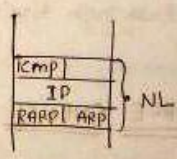
⇒ But practically DHCP can be applied on the routers also, if you Buy cisco's CASR5K Router you are going to be provided with DHCP facility at Router itself.

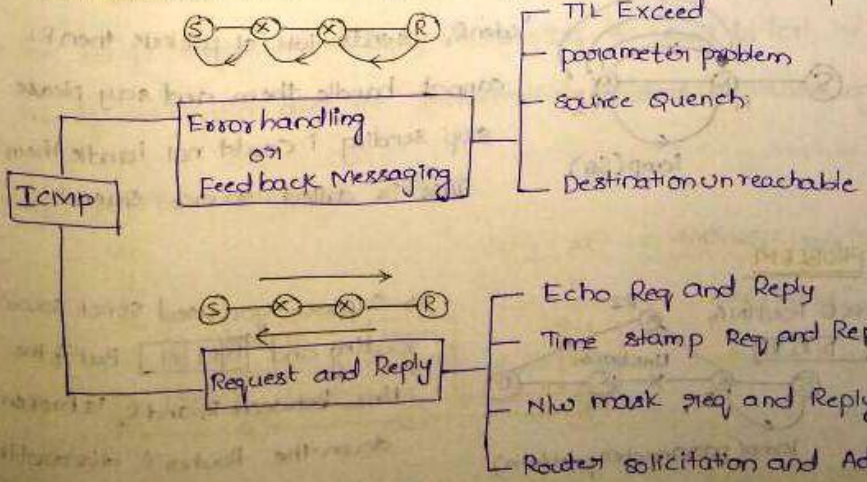
6. INTRODUCTION TO ICMP (v. Imp for GATE)

→ ICMP works at Network Layer

→ ICMP = Internet control message protocol

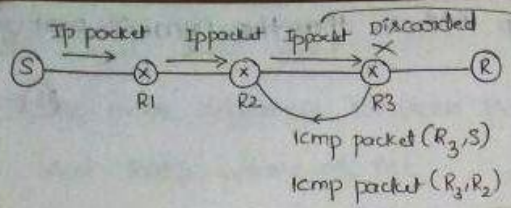
(whenever something is wrong then we get icmp packet)





Q2. When a datagram (using IPV4) is discarded, an error message is sent to the source using ICMP. The error message includes _____?

a. The datagram that had an error.
b. A data section that includes a copy of the entire IPv4 header, plus at least the first eight bytes of data from the IPv4 packet that caused the error message.
c. Only the message that tells there is some error.
d. None of these.



Icmp (R2, R3)
Icmp (R3, R2)
} Infinite loop

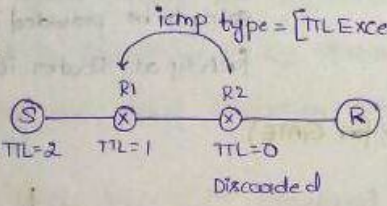
⇒ Suppose you are sending an Ip packet from Source to Receiver but on the way the Ip packet is discarded because of heavy congestion at Router R_3 Now the Router R_3 sends icmp packet (R_3, S) to say to the source that i discarded your packet. Now, the Router R_3 sends "Icmp (R_3, S)" first to Router R2 but because of heavy congestion at R2 the Icmp packet (R_3, S) is discarded at 'R_2' so 'R_2' again sends an Icmp packet to 'R_3' and because of heavy congestion at R_3 again the Icmp packet is discarded this scenario will lead to Infinite loop

⇒ Ip packet is lost the icmp packet should be generated but if ICMP packet is lost then no icmp packet should be generated

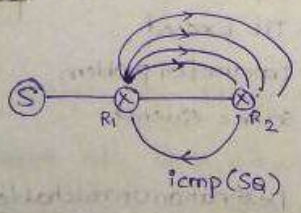
∴ (Icmp + IP) UNRELIABLE

7. ICMP FEEDBACK MESSAGING

TTL EXCEED

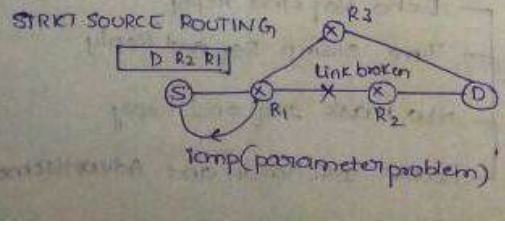


SOURCE QUENCH



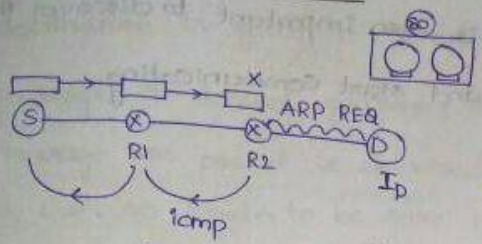
'when R_1 sends lots of packets then R2 cannot handle them and say please stop sending i could not handle them' This is called source quench.

PARAMETER PROBLEM



⇒ Suppose you used strict source routing and [D|R2|R1] But if the link between R_1 and R_2 is broken down the Router 'R_1' discard the packet and sends icmp message

DESTINATION UNREACHABLE

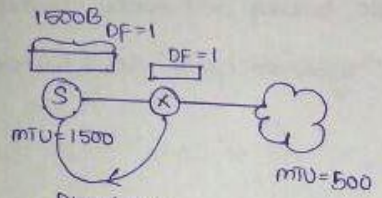


(DH unreachable)

⇒ Destination unreachable is of 2 types they are

1. Destination Host unreachable
2. Destination port unreachable

⇒ R2 send ARP Req for getting MAC Add of the Host if the Host is down then there wont be reply then the Router R2 sends icmp DH unreachable error message").

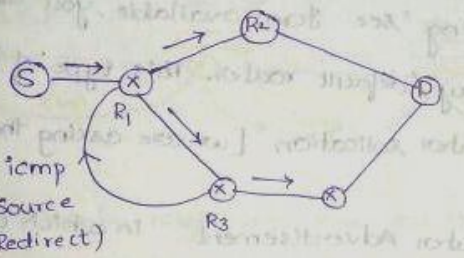


DHU = Destination Host unreachable

DF = Donot fragment = 1

FR = Fragmentation Required.

SOURCE REDIRECT

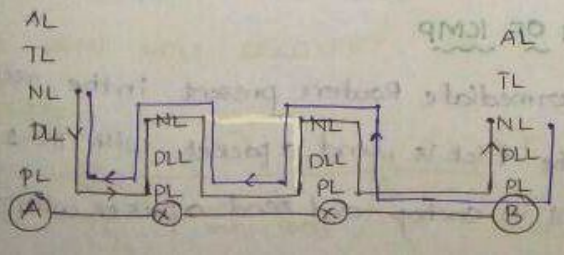


⇒ Now source sends a pacet to R_1 and at R_1 due to some errors in the Routing table if it has choosen Router R_2 (actually the best path is "R_1 R_2 D") then if there is some manual mechanism in R_3 which knows that there is a better path btn 's' and 'D' then 'R_3' sends icmp packet saying "see there is another better path so you please redirect dont send to me next time".

8. ICMP REQUEST AND REPLY MESSAGING

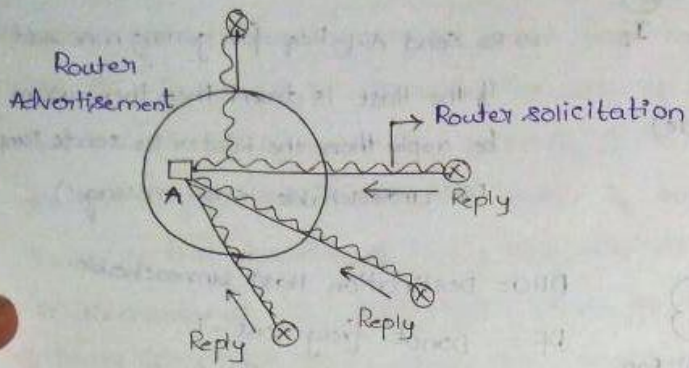
⇒ The Icmp Request and Reply messaging is used to test whether the NL of destination and the Intermediate routers are working or not

PING : PACKET INTERNET GOFER



⇒ PING uses "Icmp echo Req/Reply".

⇒ It is not enough just that you get the Ip Address from DHCP when you are connected to internet, it is also important to discover the default Router for your connection and start communicating.



⇒ The station present in the Network sends a Broadcasting message to all the Routers which are connected to that particular Network then the Routers reply saying "see I am available, you can use me as your default gateway / default router. This type of Broadcasting the message is called "Router solication" [we are asking the Routers]

⇒ The other scenario is "Router Advertisement" in which a router connected to a N|w, says "see I am available you can useme as your default router.

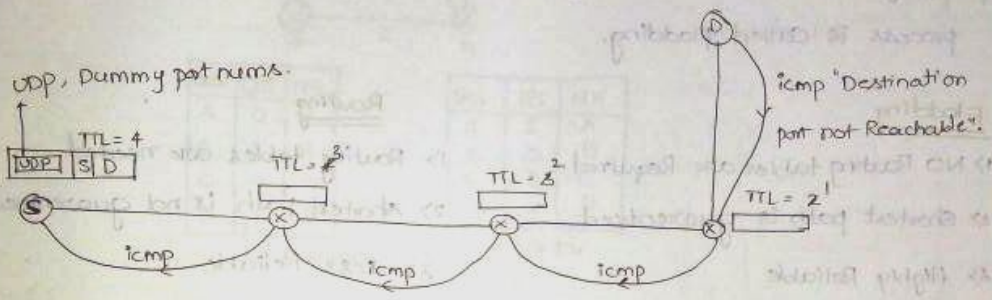
Time Stamp Req and Reply

Generally various Networking devices are placed at different parts of the world. The challenge here is synchronisation which means it is important to check whether they work at same time, inorder to that there is a special type of icmp message called "Time Stamp Req and Reply" message. This is a obselete technology and now we are using "Network time protocol"

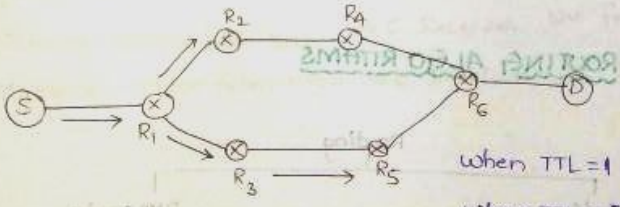
9. TRACE ROUTE APPLICATION OF ICMP

⇒ Inorder to find the intermediate Routers present in the route between source and destination the trick is, send a packet with TTL=1 inorder to get the Router present in one hop, and send a packet with TTL=2 to get the Router present at 2nd hop. when TTL=0 at the router it sends "Icmp TTL exceed" error to the source (send...

=> when the packet reaches the destination TTL will be zero and the destination is going to accept it but it doesn't generate icmp message, it doesnot guarentee that when we dont receive a Icmp message the packet is delivered to the destination, the Icmp may be lost. so inorder to be sure whether the packet reached the destination insert a UDP packet in to the Ip packet and put dummy port numbers so that when the packet reaches destination it is going to accept it and returns an "icmp message" "Destination port unreachable."



=> The Trace route might not give you the actual path, but in almost majority cases we get Actual path. for, example



when TTL = 1 = R_1

when TTL = 2 = R_2

when TTL = 3 = R_5 (This is also a possibility)

when TTL = 4 = R_6

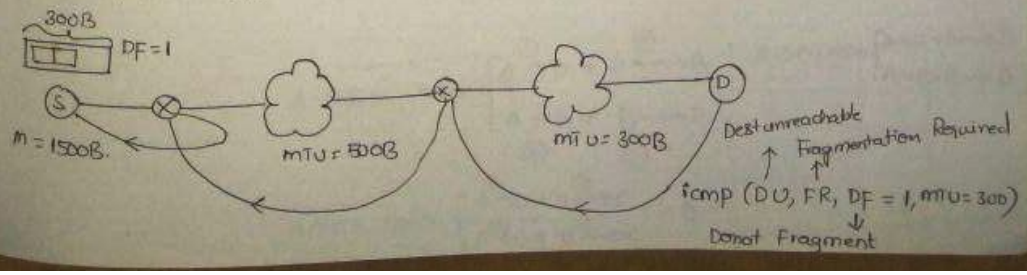
when TTL = 5 = D.

= (R_1 R_2 R_5 R_6 D)

= Not valid path.

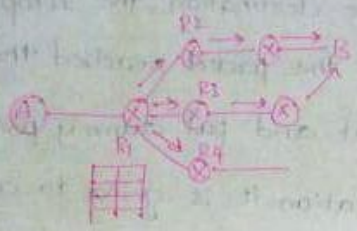
10. PMTDU APPLICATION OF ICMP

PMTDU = PATH MTU DISCOVERY



10. ROUTING

1. DIFFERENCE BETWEEN ROUTING AND FLOODING



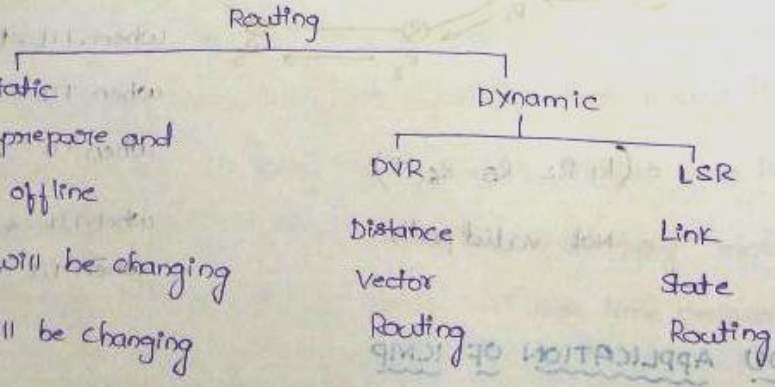
⇒ How does the Router R1 comes to know about the destination, i mean which is the path that it should send the packet so that it will reach destination.

⇒ The process of building the routing table is called "Routing"

⇒ If you dont know which way to send, send it in all possible paths, this process is called flodding.

Flodding	Routing
1> NO Routing tables are Required	1> Routing tables are needed
2> Shortest path is guarenteed.	2> Shortest path is not guarenteed
3> Highly Reliable	3> Less Reliable
Disadv	**Adv**
1> More Traffic	1> Less traffic
2> Duplicate packets are possible	2> No Duplicate packets.

2. TYPES OF ROUTING ALGORITHMS



→ Manually prepare and uploaded offline

→ Topology will be changing

→ Traffic will be changing

3. DISTANCE VECTOR ROUTING

⇒ In the DVR every node is going to know only about its Neighbours.

⇒ The Routing table at a node contain three fields Destination, Distance, Next hop

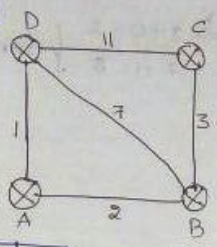
Step 1

Des	Dis	NH
A	1	A
B	7	B
C	11	C
D	0	D

↳ DV

Des	Dis	NH
A	∞	–
B	3	B
C	0	C
D	11	D

↳ DV



⇒ Building Local Routing table with knowledge of Neighbours.

Des	Dis	NH
A	0	A
B	2	B
C	∞	–
D	1	D

↳ Distance vector

Des	Dis	NH
A	2	A
B	0	B
C	3	C
D	7	D

↳ DV

Step-2:

⇒ Every Router will take their distance vectors and exchange with their Neighbours.

⇒ Now at every node the new distance vectors will be newly created.

⇒ 'A' Receives Distance vector from B, D. ⇒ C Receives DV from B, D.

⇒ 'B' Receives Distance vector from A, C, D ⇒ D Receives DV from A, B, C

At A:

DV's from B, D

From B
2
0
3
7

From D
1
7
11
0

⇒ using these two the new DV of Router 'A' will be

A	0	A
B	2	B
C	5	B
D	1	D

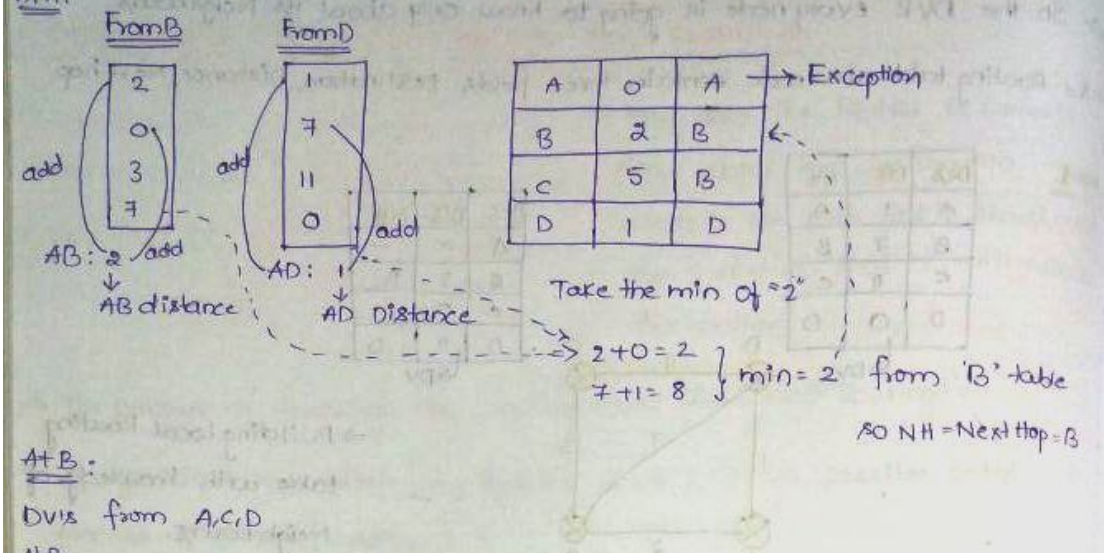
$A \to B = \min \begin{cases} A \xrightarrow{①} D + D \xrightarrow{③} B \\ A \xrightarrow{②} B + B \xrightarrow{⓪} B \end{cases}$

$A \to D = \min \begin{cases} A \to D + D \rightsquigarrow D \\ A \to B + B \rightsquigarrow D \end{cases}$

$A \to C = \min \begin{cases} A \xrightarrow{①} D + D \xrightarrow{④} C \\ A \xrightarrow{②} B + B \xrightarrow{⑤} C \end{cases} = 5$

The shortcut is

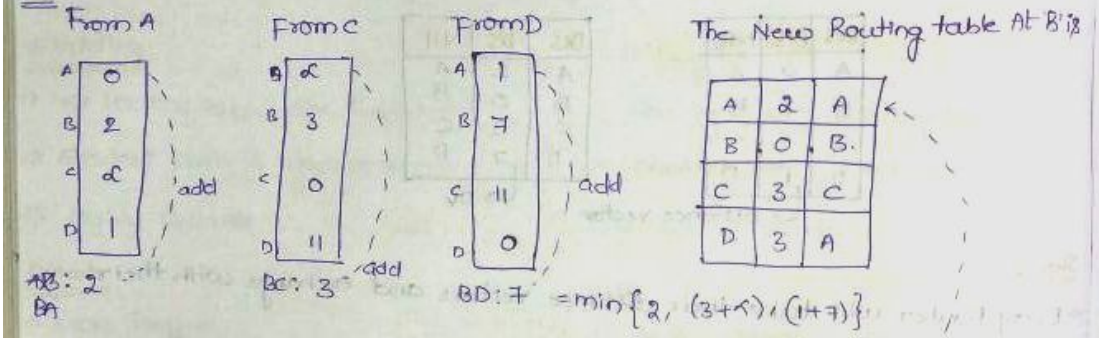
At A:



At B:

DVs from A, C, D

At B



⇒ Repeat this procedure at every node and do it for 3 times (3 Rounds) because the shortest path is of 3 edges. ⇒ no of (nodes − 1). So Repeat the rounds for (n−1) times {n = no of nodes}

The final Routing table is after everything converges is,

At A:

A	0	A
B	2	B
C	5	B
D	1	D

At B

A	2	A
B	0	B
C	3	C
D	3	A

At C

A	5	B
B	3	B
C	0	C
D	6	B,A

At D

A	1	A
B	3	A
C	6	A,B
D	0	D

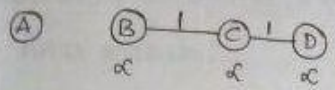
Problem

After the Routing table converges the edges that are unused is D→C, D→B.

4. COUNT TO INFINITY

⇒ There is a problem with DVR the problem is called count to Infinity.

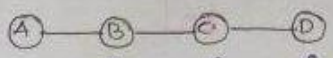
Initially

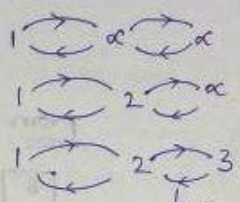


(distances to A)

Step-1

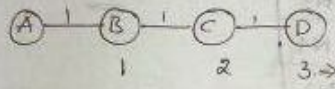
Suppose if 'B' is connected to A





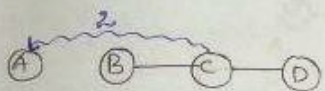
↳ Exchange of DV's

Suppose if Everything is stabilized



→ (distances to A)

Now, suddenly if the link between A,B is down, then it is a Bad news



1 2 3 (Initial values before the link is broken)

∝ 2 3. (Here is the trap, we know that the Routing tables are exchanged in neighbours. Here, B says i cannot reach 'A' but 'C' says dont worry im able to reach 'A' in 2 hops").

Dist. from B→A via C:

3 4 3

5 4 5

5 6 5.

7 6 7

Distances from that node to 'A':

7 8 7

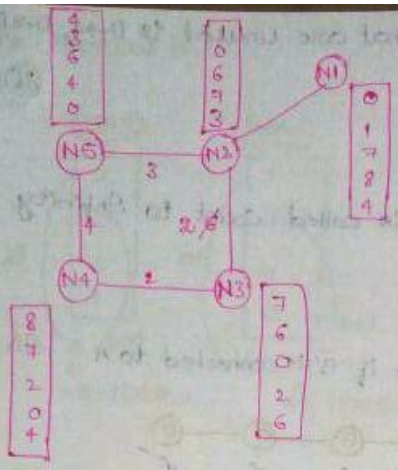
9 8 9

9 10 9

∝ ∝ ∝

⇒ This will execute till the value that you have chosen for Infinity

Now the above explanation can be understood by the explanation given below. This question is asked in GATE



Now suppose the value of distance btn N_3 and N_2 which is '6' falls down to '2' then what is the distance vector at N3? (After 1 round of exchange).

At N3:

From N2

1
0
6
7
3

$N_3N_2 : 2$

From N4

8
7
2
0
4

$N_3N_4 : 2$

New routing table at N3 is

N1	3	N2
N2	2	N2
N3	0	N3
N4	2	N4
N5	5	N2

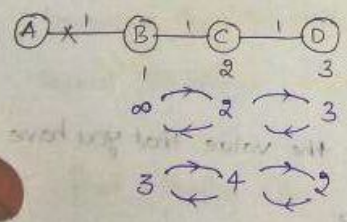
∴ Ans: 32025

Solution ↳

5. SPLIT HORIZON

⇒ The solution to count to infinity is split horizon.

⇒ The count to infinity also creates some loops



The routing tables at A, B and C will be

A	∞	-
:	:	:

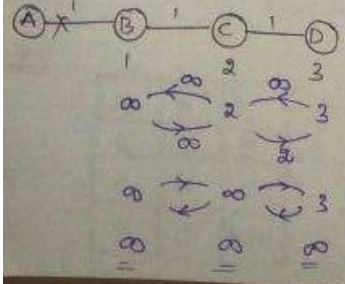
A	2	B
:	:	:

A	3	C
:	:	:

Initially

⇒ This procedure repeats until all the values are stabilized.

So this problem can be solved by sending the Next hops also and this procedure is called split horizon.



⇒ Now, At 'C', c is depending on B' inorder to goto 'A' ∴ when 'C' is already depending on 'B' to goto 'A' it should not say i can take 'u' in some hops", i am already depending on 'y' so please dont

⇒ By using the method of Split horizon convergence is fast, No loops are formed.

⇒ In case of DVR convergence is slow and loops will occur.

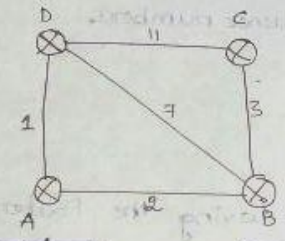
6. LINK STATE ROUTING

⇒ Every Router will create something called as Link state packets.

⇒ In the first round Every node creates a Link state packets with the help of "Hello packets".

D	
Seq	
TTL	
C	11
B	7
A	1

C	
Seq	
TTL	
D	11
B	3



A	
Seq	
TTL	
B	2
D	1

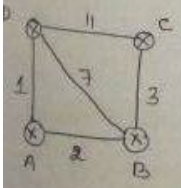
B	
Seq	
TTL	
A	2
D	7
C	3

⇒ In ROUND2 EVERY NODE IS SUPPOSED TO FLOOD THE INFO TO EVERY OTHER NODE. THERFORE WE WILL HAVE GLOBAL DATABASE AT EACH NODE.

DVR- Local knowledge (knows only about the Neighbours)

LSR = Global knowledge (knows about all the nodes.

AA:



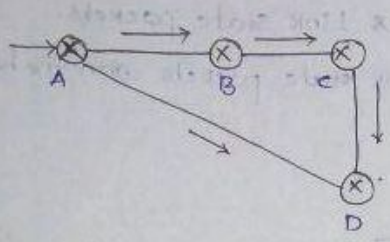
⇒ Then at 'A', 'A' will start applying single source shortest path (Dijkstra Algo) and 'A' comes to know all the shortest path to all nodes and 'A' will construct its Routing table

DES	DIS	NH
A	0	A
B	2	B
C	5	B
D	1	D

⇒ LSR converges faster compared to DVR

⇒ There are some problem in the LSR, since we are flodding, it is going to lead Heavy traffic.

⇒ Now, consider the following scenario,



⇒ Now if a packet is flodded from 'A' to all the nodes then the packet will reach 'D' in less time when compared with the other path (A-B-C-D), so the arrived packet (which has arrived Quickly) is the latest packet but depending on the time of arival we may think that the packet which came late is the latest packet and the packet arrived Quickly is the old packet. so inorder to correct that we have sequence numbers.

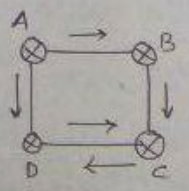
(A, 10) ✓ } Latest packet
(A, 5) × } old packet - discarded.

Therfore At A, it maintains a table having the Router name and latest sequence numbers.

Router	Latest
B	1615
C	20
D	30

(B,8) × - discarded
(B,15) ✓ - Accepted
(B,11) - discarded

Now,



⇒ The packet that is already sent to 'D' from 'A' is going to come again to the same destination via another route (A-B-C-D) so there is a problem of falling in infinite loop. This can be overcomed by having TTL field

7. DIFFERENCE BETWEEN DVR, LSR, RIP AND OSPF

DVR

1) Used in 1980's
2) Bw required is less
3) Local Knowledge
4) Bellman ford Algo
5) Less Traffic
6) periodic updates
7) Converges slowly
8) count to infinity
9) persistent Loops
10) RIP
11) RIP Uses UDP

LSR

1. Used in 1990's
2. High Bandwidth
3. Global Knowledge
4. Dijkstra Algo
5. High Traffic
6. periodic updates
7. Converges fast
8) No count to Infinity
9) Transient Looping
10) OSPF
11) OSPF doesn't use UDP or TCP. It sends directly via IP.

RIP (ROUTING INFORMATION PROTOCOL) 12) Intra-domain routing

⇒ Rip is the implementation of (DVR) simple to Implement

⇒ Metric = Hopcount (weights)

⇒ Infinity cannot be represented in programing language hence the value 16 is used as Infinity.

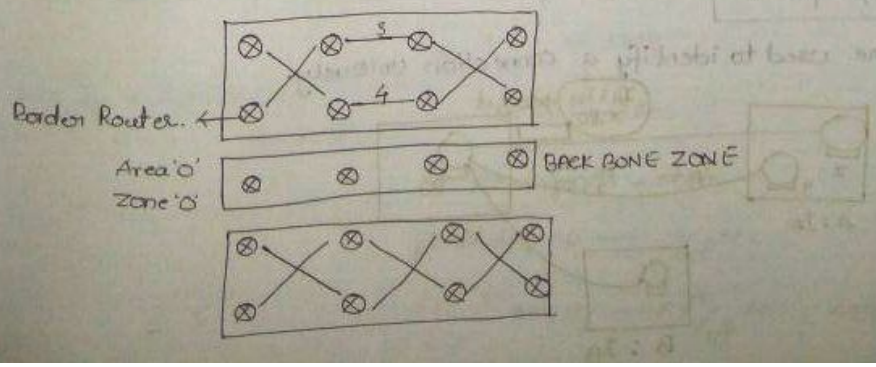
OSPF

⇒ OSPF is the Implementation of the (LSR) → Computation is complex

⇒ OSPF divides all the routers into some Regions and flodding is Restricted to that Region, and there will be one router designated as "Border Router" (It will take all the flodded packet and summarize the Info).

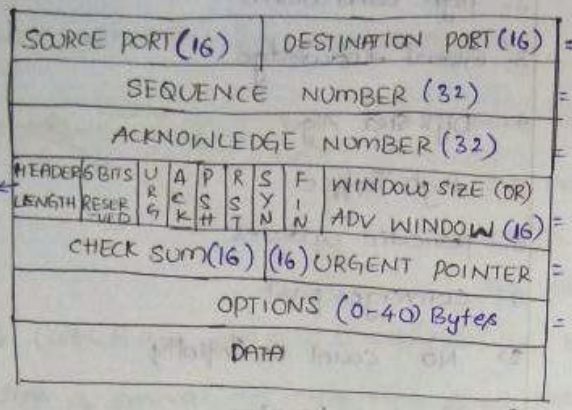
⇒ Border Router is connected to "Area '0'" or "Zone '0'" or "Back Bone Zone".

⇒ "EIGRP" PROTOCOL INVENTED BY CISCO EIGRP = RIP + OSPF



11. TCP

1. TCP HEADER



∴ Max Header Length in Tcp = 60 Bytes

∵ Min. header length in Tcp = 20 Bytes

2. SOURCE PORT, DESTINATION PORT AND SOCKET

⇒ Tcp is End-End protocol because of having port numbers.

⇒ port numbers are used for multiplexing and Demultiplexing.

⇒ SP DP
16 16

[0 to $(2^{16}-1)$] nos can be represented

= (0, 65,535)

Http : 80
FTP : 21
Telnet : 23
Smtp : 25

0 – 1023 } well known services port numbers
1024 – 49,151 } Reserved
49,152 – 65,535 } General public

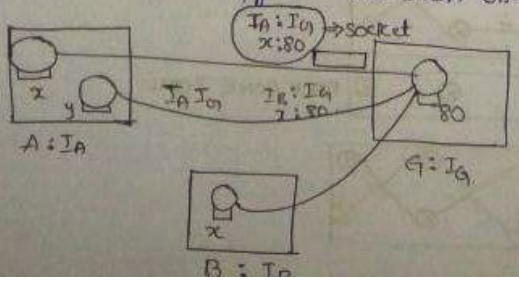
cmd

⇒ open your ~~browser~~ and type "Net stat" to see all the connections, and port numbers (source port number, Destination port number)

⇒ Tcp is connection oriented protocol (Resources are Reserved).

⇒ Socket = Ip + portnum = 32 + 16 = 48 bits

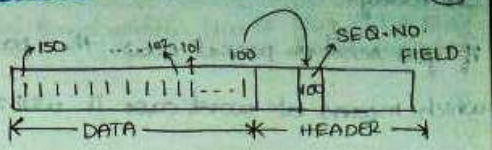
⇒ sockets are used to identify a connection uniquely.



Counting of every byte

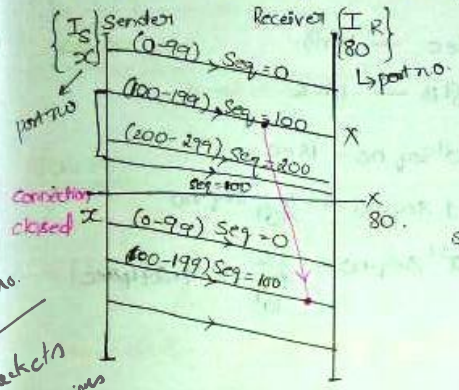
3. SEQ. NO, ACK NO., RANDOM INITIAL SEQ. NO

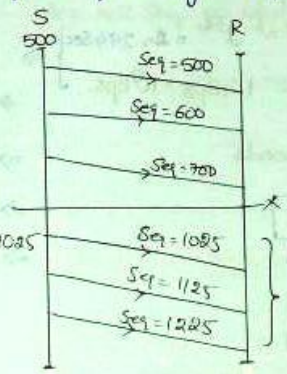
⇒ Tcp is a **Byte Stream protocol**.
⇒ Ip is a **packet Stream protocol**.
⇒ HDLC (DLL) is a Bit Stream protocol.



⇒ In Tcp the data Bits are numbered. the seq.no field contains the **value of starting data bit**

⇒ Ack field is used when the sender sends the Tcp packet and is waiting for Acknowledgement. Ack field contains the value of the data bit that is **expected next** (seq no of the Byte expected to come next)





TCP ↓
USE ANY **RANDOM** SEQUENCE NUMBER

TCP uses Random Sequence no. to deal with late packets of previous sessions

4. WRAP AROUND TIME AND PROBLEMS ON WRAP AROUND TIME

⇒ wrap around is nothing but using up all the seqnos present and reusing the seq.no's that are already been used is called wraparound. From this we get "wrap Around time".

WAT

⇒ Wrap Around Time (WAT) depends on the Bandwidth.

⇒ **Seq. No's field contain 32 bits ⇒ 2^{32} seq.nos are possible**

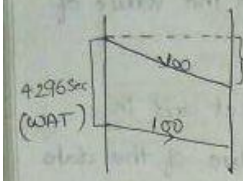
⇒ Now, Letus say Bandwidth = 1 MBps

WAT of 'n' seqnos = $\frac{n}{\text{Bandwidth}}$

⇒ 1 sec — 1 MB
⇒ 10^6 B — 1 sec
⇒ 10^6 seq.nos — 1 sec
⇒ 1 seq.no — $1/10^6$ sec
⇒ 2^{32} seq.no — $2^{32}/10^6$ sec = 4296.967296 sec

In today's internet there is a concept called Life time which means if you send a packet now the packet will be alive for sometime (3 min) which means at worst case it will reach after 3minutes after you send it.

LT = 3min = 180sec



{practical value} ⇒ As long as WAT > LT there is no problem

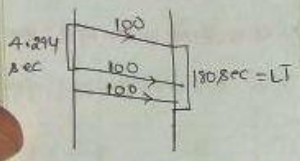
II.

Let us consider WAT = 2^{32} = 4,294sec
Bw = 1GBps = 10^9 Bps.

⇒ 1sec — 1GB
⇒ 10^9 B — 1sec
⇒ 10^9 seq.no — 1sec
⇒ 1 seq.no — $1/10^9$ sec
⇒ 2^{32} seq.no — $\frac{2^{32}}{10^9}$ = 4.294sec

Life time = 180 seconds

⇒ Here WAT ≪ LT



Now, to solve the above problem, the possible solution is Decreasing the Bandwidth, But this is not possible because we are intrested in having high Bandwidth (The speed at which the data gets transfered) so the other possible solution is increasing the ↑ bits in the sequence no field.

WAT > LT ⇒ No problem

WAT < LT ⇒ problem ⇒ so calculate how many seq.no's are transmitted in 180sec

⇒ 1 sec — 1GB
⇒ 1sec — 1G seq.no's
⇒ 180 sec — 180 × (1G seq.no's)

∴ The min seq no's required to avoid wrapAround within Life time

= 180 × 1G seq.no

∴ The No.of bits in seq.no field is = $\lceil \log_2 (180 \times 1G) \rceil$ = 42

∴ The no.of additional bits needed to avoid above problem = 42 - 32 = 10

[These 10 bits are used in options and called as Time stamp]

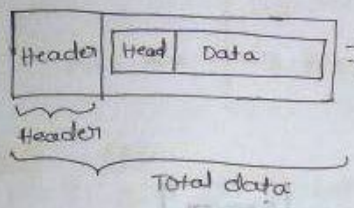
Additional bits are stored in Options

⇒ The no of bits in the sequence no field such that there wont be any problem with WAT and LT, given at Bandwidth Bw is $\lceil \log_2(LT * Bw) \rceil$ (40)

5. HEADER LENGTH AND CALUCULATION OF ACKNOWLEDGENT NUMBERS

⇒ Header length field is 4 bits, but the min size of the header is 20B

⇒ Scaling factor of $\frac{60}{15} = 4$ is used. $\left\{\frac{\text{max size of header}}{\text{largest no by 4 bits}} = \text{scalufactor}\right\}$



SEQ NO: Seq no of I Byte

ACK NO: Seq no of Byte expected next.

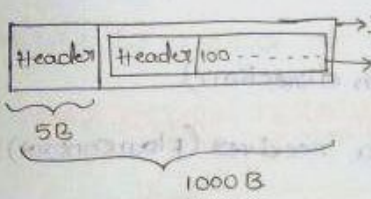
PROBLEM

TL = 1000 B } for Ip Datagram
HLF = 5

HLF = 5
Seq no of Tcp segment = 100B } for Tcp Segment

then what is the ack number of the next Byte expected?

SOL: Tcp segment will be in the Ip Datagram

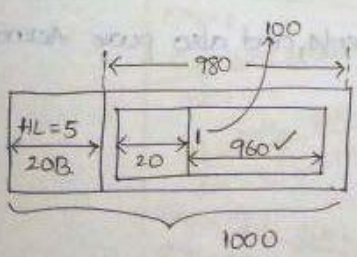


⇒ Now, the data part in the Ip datagram = 1000 − (5 * 4)
= 980 B

⇒ 980 B = Header + Data (in Tcp)

⇒ 980 − (5+4) = Data

⇒ 960 B = Data ⇒ Ack = (960 + 100) + 1
= 1059



⇒ last Byte seq no = 100 + 960 − 1

⇒ 1059

⇒ Next Byte seq no = 1059 + 1
= 1060

6. TCP CONNECTION ESTABLISHMENT

⇒ Flags are nothing but 1 Bit information, Tcp is connection oriented.

SYN (SYNCHRONIZATION FLAG)

ACK (ACKNOWLEDGEMENT FLAG)

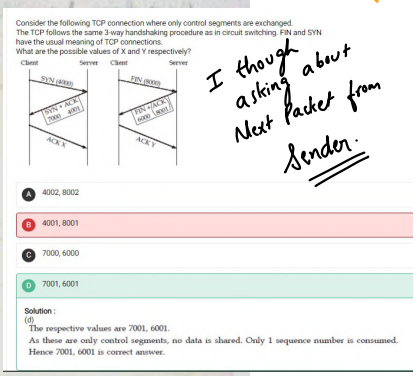
NOW, Tcp is connection oriented protocol and it has 3 phases,

1) Connection Establishment

2) Data Transfer

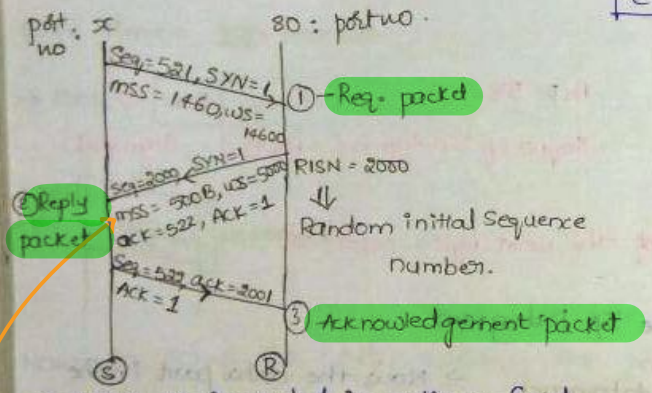
3) Connection Termination.

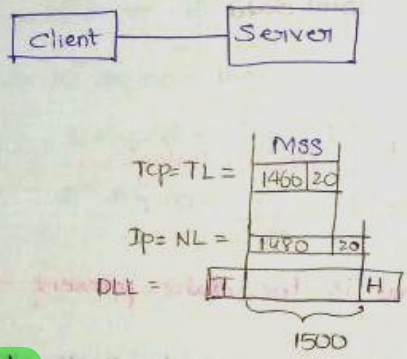
Mock Test-4



I thought asking about Next Packet from Sender.

CONNECTION ESTABLISHMENT





Bottleneck of Data Link (1500)

⇒ MSS is included in options field.

⇒ Tcp is full duplex (Data transfers in both direction)

⇒ window size : capacity of the host as a receiver (Flow control)

⇒ "SYN" PACKET WILL EATUP 1 SEQ NUMBER.

⇒ Tcp uses "piggy Backing" Acknowledgements, and also pure Acknowledgements

⇒ "ACK" 1 TAKE '0' NO OF SEQ NO's

⇒ "FIN=1" TAKE '1' SEQ NO's.

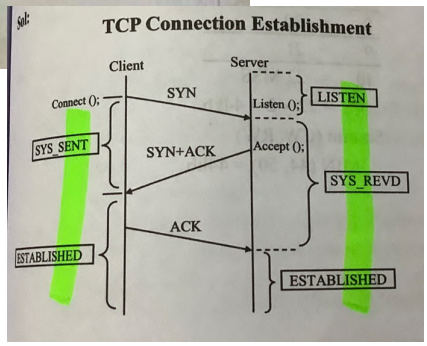
⇒ 1 DATA BYTE TAKES 1 SEQ NO's.

⇒ THIS METHOD OF CONNECTION ESTABLISHMENT IS CALLED "3-WAY HANDSHAKE" PRINCIPLE.

Only 'Syn', 'Fin', Data consume Sequence no.

An Acknowledgement by TCP sender guarantee

- ✓ Data has been delivered to the application
- ○ Data has been received by TCP module



Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	Request a release of the connection

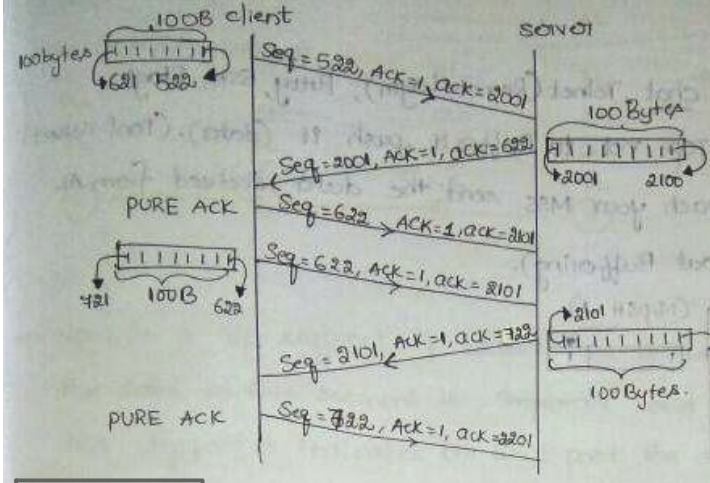
Figure 6-2. The primitives for a simple transport service.

09. *Identify* the correct order in which a server process must invoke the function calls accept, bind, listen, and *recv* according to UNIX socket API. **(GATE-15-Set2)**

(a) listen, accept, bind, recv
(b) bind, listen, accept, recv
(c) bind, accept, listen, recv
(d) accept, listen, bind, recv

09. Ans: (b)
Sol: TCP bind() binds port and socket, then TCP listens on socket, accept connection and then receive data. So sequence is bind(), listen(), accept(), recv().

7. TCP DATA TRANSFER AFTER CONNECTION ESTABLISHMENT



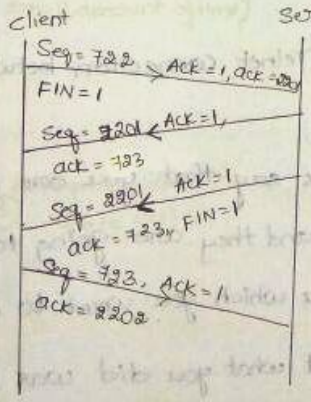
SYN	ACK	
1	0	⇒ 1st packet = Ist Segment = Request segment
1	1	⇒ 2nd Segment = Reply Segment
0	1	⇒ pure Acknowledgement (ACK is present in the header)
0	0	⇒ (Not possible)

⇒ sender is not going to send Acknowledgements immediately, he is going to wait for some time

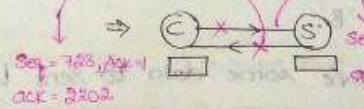
⇒ The Reciver also waits fore some time before transmiting the data.

⇒ If u dont have data to send immediately we should not wait because there will be a timer at the other end. so we should send PURE ACK.

8. TCP CONNECTION TERMINATION



⇒ FIN = FINISH FLAG (used to terminate the Connection)



⇒ After client sending FIN packet the events that are possible and not possible are

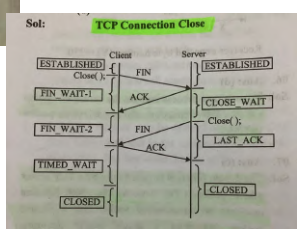
⇒ Data C → S ✗
⇒ Data S → C ✓
⇒ ACK C → S ✓ (pure ACK)
⇒ ACK S → C (Piggy Backed)

SYN: Synchronising Seq numbers
ACK: Indicate whether Ack num field is valid/not
FIN: Request for connection termination.

Primitive	Meaning
SOCKET	Create a new communication endpoint
BIND	Associate a local address with a socket
LISTEN	Announce willingness to accept connections; give queue size
ACCEPT	Passively establish an incoming connection
CONNECT	Actively attempt to establish a connection
SEND	Send some data over the connection
RECEIVE	Receive some data from the connection
CLOSE	Release the connection

Figure 6-5. The socket primitives for TCP.

Sol: **TCP Connection Close**



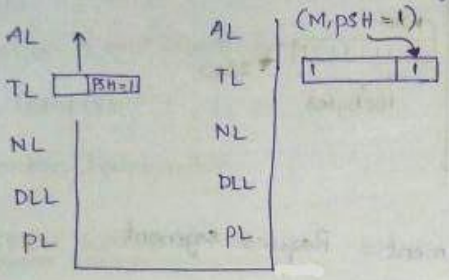
9. PSH FLAG

PSH = PUSH FLAG

⇒ Interactive Applications = chat, Telnet (Remote Login), Putty, SSH, Rlogin.

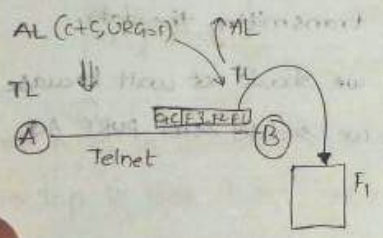
⇒ PUSH is used to say TCP not to Buffer it, push it (data). (Dont collect the data until you reach your MSS send the data received from AL at the same time without Buffering).

⇒



10. URG FLAG AND URGENT POINTER

URG = URGENT FLAG



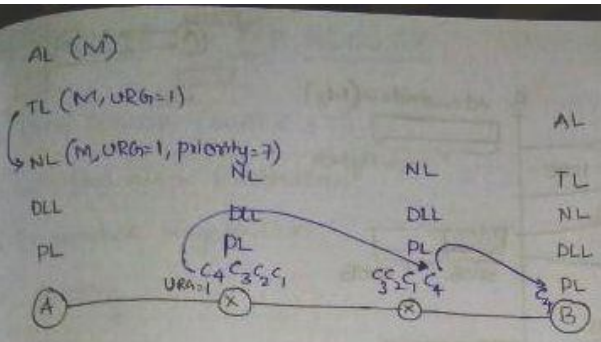
⇒ Let us assume that there is a Telnet connection between the two hosts 'A' and 'B'.

⇒ you have some data to sent Let us say that you are sending the data in the form of files F1 F2 F3 and they are going to sit in Buffer at host 'B'. All those are existing files which you want to modify

⇒ Now, suddenly you realised that what you did was wrong and you want to execute the command (Ctrl+c)(c+c) before all the files. [Ctrl+c is used for stopping]

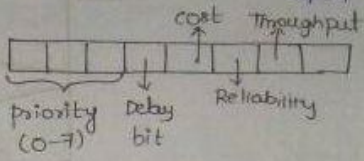
⇒ so urgent flag is used here, which means you have to say that last command is urgent when compared to other things.

⇒ so for "(Ctrl+c) send URG=1"

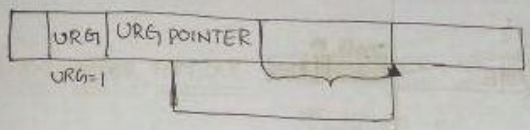


⇒ for urgent packet the priority is set to seven.

⇒ Type of service (8bits) in IPv4

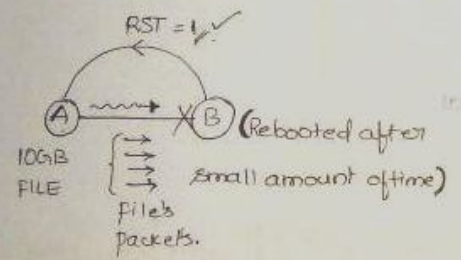


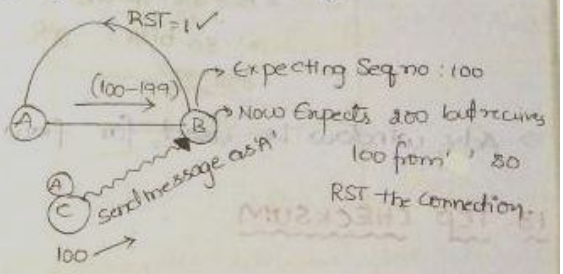
⇒ Now, in a Tcp segment if URG=1 then it indicates that some part of the data in this segment is important and the nextone is urg pointer this urg pointer indicates till what part the data is urgent.

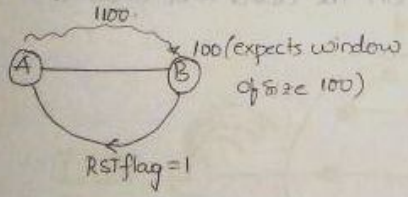


11. RST FLAG

⇒ RESET Flag is used when there is a wrong in the connection. If you see anything unexpected then you are going to use Reset flag.





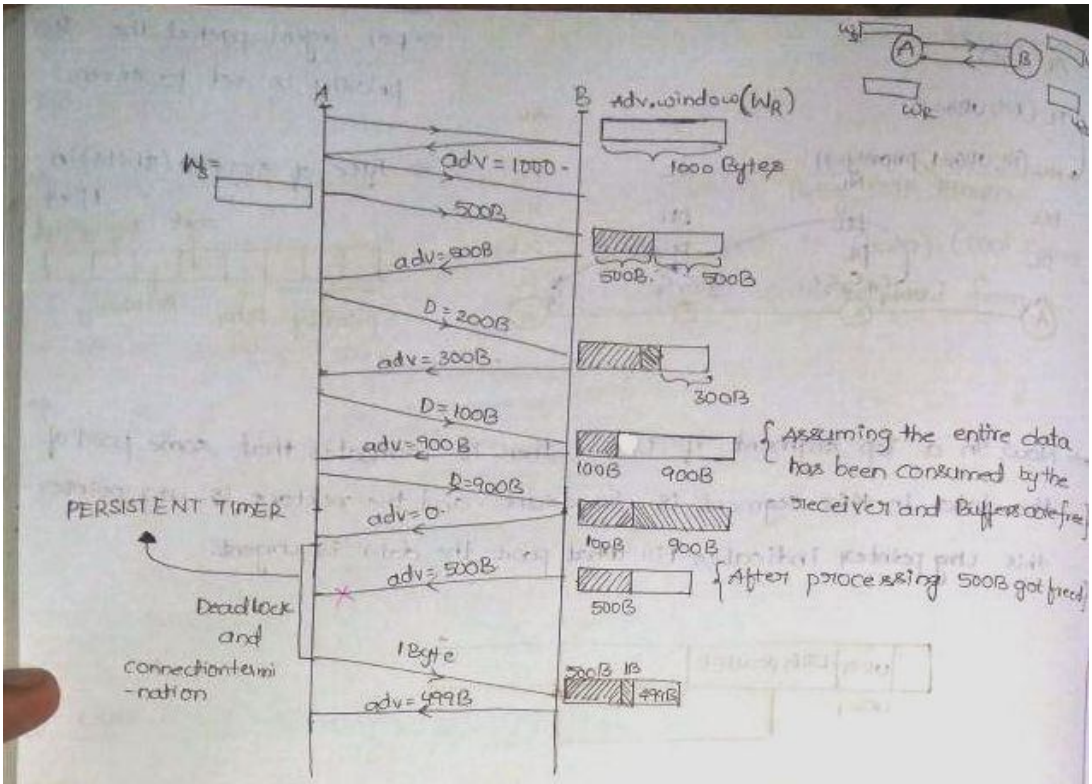


⇒ when RST=1 it means that, please terminate the connection i'm not expecting anything from you.

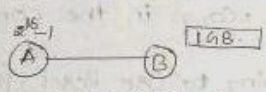
12. TCP FLOW CONTROL USING ADVERTISEMENT WINDOW

⇒ Flow control, a sender should never send what a receiver can't receive. for that Reason we are going to use window size.

Useful in Flow Control



⇒ The window size is 16bits ⇒ Max no = $2^{16}-1$ = 65,535



= 16 + 14 (options)

= 30 bits = 2^{30} = 1GB.

⇒ Adv window is used for flow control.

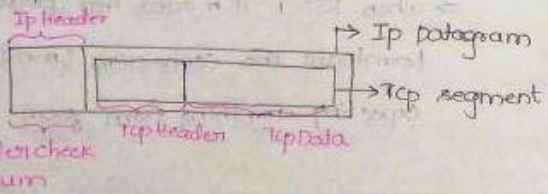
13. TCP CHECKSUM

→ for Double Checking

⇒ Tcp Header has 16-bit checksum

⇒ In Tcp the checksum is caluculated both on the data and Header.

⇒



⇒ Checksum is caluculated on TcpHeader, Tcpdata, IpHeader → only some field of IP Header

{caluculate check sum only on the fields in pseudo Ip Header} Because other fields in Ipv4 Header will change when the packet is received by Receiver

Psedo IP Header

PIpH:

Pseudo Ip Header.

SIP(32)		
DIP(32)		
000 (8)	Protocol (8)	Tcp segment Length (16)

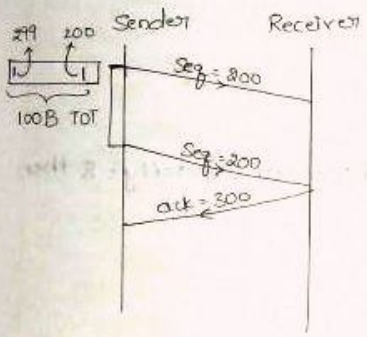
14. OPTIONS IN TCP HEADER

1) Time stamp (WAT < LT)
2) Window size Extension
3) Parameter Negotiation
4) Padding

15. RETRANSMISSIONS IN TCP

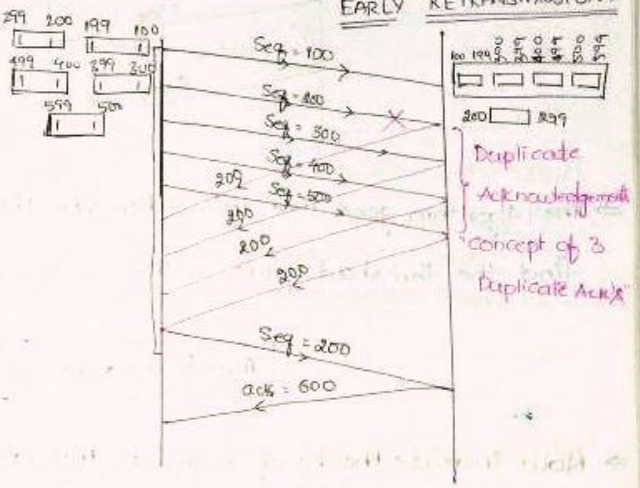
⇒ TCP uses SR + GBN
⇒ $w_s = w_R$ | ⇒ Acknowledgements are cumulative
⇒ out of order packets are possible | ⇒ 25% GBN
• 75% SR

RETRANSMISSION AFTER TIMEOUT

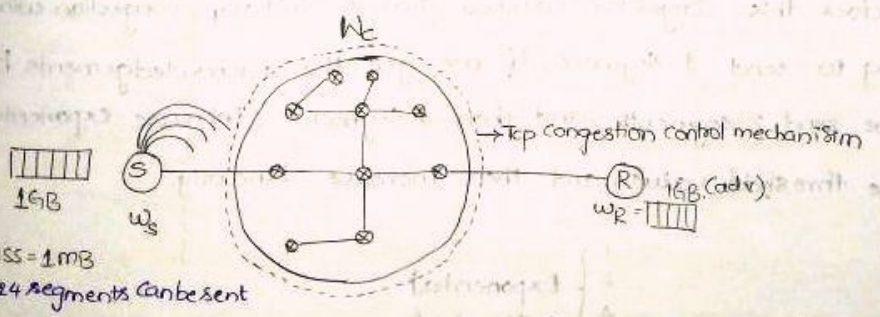


RT AFTER 3 DUPLICATE ACKNOWLEDGEMENTS

EARLY RETRANSMISSIONS



16. INTRODUCTION TO TCP CONGESTION CONTROL



⇒ Assume that the Receiver has said that sender can send 1GB of data in the Advertising window. ⇒ w_s = 1GB, w_R = 1GB

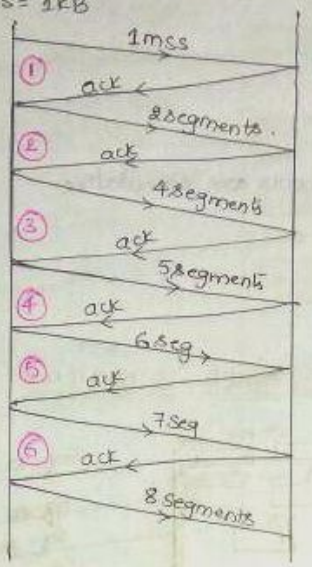
⇒ The problem here is even though the Receiver can hold 1GB of data the underlying Network cannot hold 1024 packets.

⇒ So the sender should not dump the data on the Network without finding the capacity of the Network (W_c).

⇒ A sender should always send $\min(W_c, W_R)$ data to the Network & Receiver so we should stop the traffic at sender side.

Advwin: 8KB
MSS = 1KB.
W_R = 8 segments
W_c = 1 Segment
$W_s = \min(1, 8)$
$= \min(W_c, W_R)$
$W_s = 1$

Advwin = 8KB
MSS = 1KB



⇒ Even though you can send 8 segments at a time dont do it because the underlying N/w may not be in a position to handle the segments. So send segments one by one in some order.

⇒ The Algorithm goes like this whenever the Receiver capacity = 8 then find the threshold value = $W_R/2 = 8/2 = 4$

Threshold value = 4

⇒ Now increase the no of segments that are being sent, exponentially upto the threshold value and after that send the packets Linearly.

⇒ How does this congestion window grow is initially congestion window is going to send 1 segment, if we get the acknowledgements back then we send 2 segments, and then 4 segments (increase exponentially till the threshold value) and then increase Linearly.

1
2 } Exponential
4 → Threshold
5
6
7 } → Linear Growth of No of Transmissions.
8

9.

[Medium]
Que: 2 Compute the fraction of the bandwidth that is wasted on overhead (headers and retransmissions) for protocol on a heavily loaded 50-kbps satellite channel with data frames consisting of 40 bits header and 3960 data bits. Assume that the signal propagation time from the earth to the satellite is 270 msec. ACK frames never occur. NAK frames are 40 bits. The error rate for data frames is 1%, and the error rate for NAK frames is negligible.

a. 1.21%
b. 2.12%
c. 1.99%
d. 1.71%

3960 + 40 + 40 + 40 + 40
Data Head NAK Data Header

$\left[\frac{160}{3960} \times 100\right] = 4.04\ \%$

Count No. of Lines

V. Imp

(46)

1) AFTER HOW MANY RTT'S ARE WE GOING TO REACH THE MAX SENDER WINDOW SIZE (8)?

Ans 6 Roundtrip times.

1 | 2 | 4 | 5 | 6 | 7 | 8

1RTT 2RTT 3RTT 4RTT 5RTT 6RTT

2) Adv Win = 16KB

MSS = 1KB

W_R = 16 Segments ⇒ Threshold = $16/2 = 8$

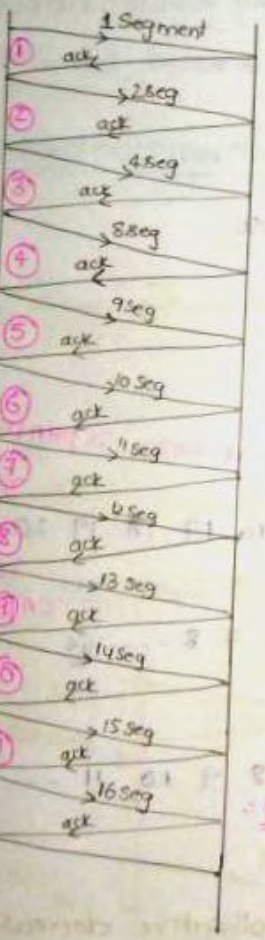
W_c = 1 Segment

AFTER HOW MANY RTT'S WILL WE REACH TOTAL CAPACITY?

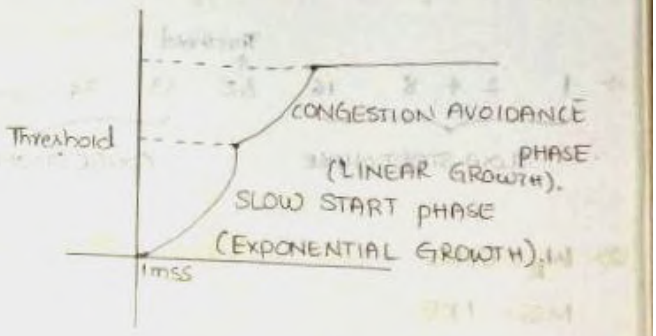
⇒ 1 | 2 | 4 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16

1RTT 2RTT 3RTT 4RTT 5RTT 6RTT 7RTT 8RTT 9RTT 10RTT 11RTT

⇒ 11 RTT's



∴ 11 RTT's



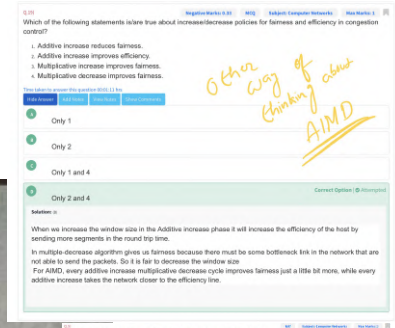
SS PHASE = "EXPONENTIAL GROWTH".

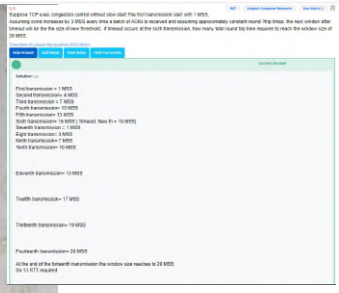
CA PHASE = "LINEAR GROWTH".

13. Ans: (c)

Sol: In slow start phase of TCP congestion control algorithm.

- The CWND increases by 1 MSS on every successful ACK.
- The CWND approximately doubles every RTT.





17. TCP CONGESTION CONTROL ALGORITHM WITH EXAMPLE

⇒ The congestion control Algorithm has three steps they are

1. Slow start phase
2. Congestion Avoidance phase
3. Congestion Detection phase

⇒ There are 3 ways to detect congestion they are

Strong possibility of congestion
1. Time out (Severe Congestion) ⇒ (SS PHASE)

Weak possibility of congestion
2. Three Duplicate Acknowledgements (Mild Congestion) ⇒ (CA PHASE)
3. ICMP Messaging (Source Quench). (Most of the Implementations dont consider it)

1) W_R = 64 KB

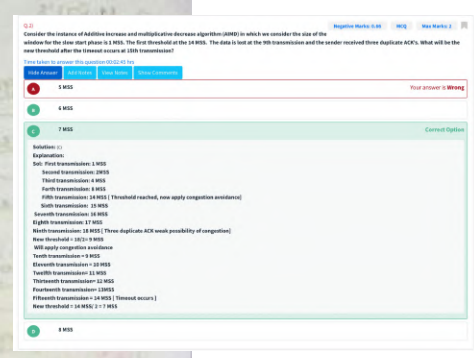
MSS = 1 KB

W_R = 64 Segments ⇒ Th = 64/2 = 32 MSS

Threshold

⇒ 1 2 4 8 16 32 33 34 ---- 64

SLOW START PHASE — CONGESTION AVOIDANCE PHASE.



2) W_R = 64 KB

MSS = 1 KB.

W_R = 64 MSS ⇒ Th = 32 mss.

⇒ 1 2 4 8 16 32 33 34 1 2 4 8 16 17 18 19 20

Th = 17 = (34/2)+ AND ALGO ENTERS SS PHASE

Th = 20/2 = 10

TO — 3 Dup Ack — 'CA PHASE'

10 11 12 1 2 4 6 7 8 4 5 6 7 8 ---- 64

Th = 12/2 = 6 — TO — 3DA — Th = 8/2 = 4

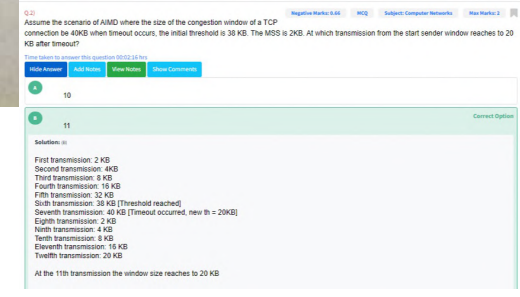
64 1 2 4 8 16 32 16 17 1 2 4 8 9 10 11 ------

Th = 32 — TO — Th = 16 — 3DA — Th = 8 — To

GATE

Consider an instance of Tcp Additive Increase Multiplicative decrease (AIMD) Algorithm where the window size at the start of ssphase is '2' MSS and the Threshold at the start of 1st transmission is '8' mss. Assume timeout occurs during 5th transmission, find the Congestion window size at the end of 10th transmission?

(A) 8 Mss (B) 14 mss (C) 7 mss (D) 12 mss



Sol

⇒ Initial value = 2

⇒ Threshold = 8 ⇒ 2 (1st Trans) 4 (2nd Trans) 8 (3rd Trans) 9 (4 Trans) 10 (5th Trans) Timeout, Th=5, 2 (6th Tr) 4 (7th Trans) 5 (8th Trans) 6 (9th Trans) 7 (10th Trans)

18. TCP TIMER MANAGEMENT

1) Time-wait timer ⇒ To handle late packets: Dont close the connection immediately wait for 2*LT

2) Keep-Alive timer ⇒ close All the idle connections

3) persistent timer ⇒ For finding the capacity of Receiver

4) Acknowledgement timer ⇒ for cumulative Acknowledgement and Piggy Backing

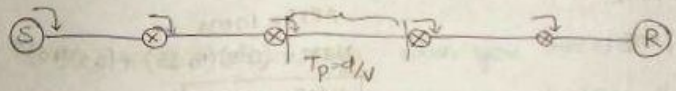
5) Time-out timer ⇒

Retransmission timer: It is used when expecting an acknowledgment from the other end.

Keep alive timer is used to prevent a long idle connection between the 2 TCP'S

It keep window size information flowing even if the other end closes its receiver window.

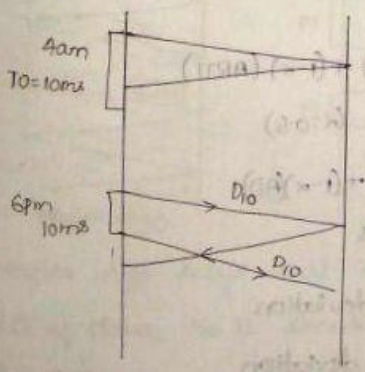
19. INTRODUCTION TO TIME-OUT TIMER



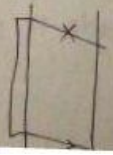
RTT = 2*Tp

TO = 2*RTT = 4*Tp

⇒ At tcp static time out timeouts cannot be used



⇒ Initially there is no congestion but after that because of your time out timer settings it might lead to congestion so have a large time out timer, but the disadvantage of having Large TOT is if a packet is lost you have to wait for a long time before Retransmitting it.



Q. 65 — Have any Doubt ?

Suppose a client C repeatedly connects via TCP to a given port on a server S and that each time it is C that initiates the close. How many TCP connections a second can C make here before it ties up all it's available ports in TIME_WAIT state? Assume client ports are in the range of 1024 to 5223 and TIME_WAIT lasts 60 seconds

70 — Correct Option

Solution :
70
No of available ports = 5223 – 1024 +1 = 4200
Due to time wait of 60 seconds, any repeated connection to same port requires an interval of atleast 60 sec

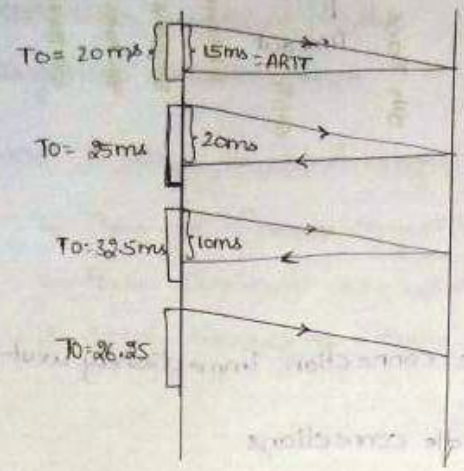
So average connection that can be opened per second is = $\frac{4200}{60}$ = 70.

Your Answer is 120

20. BASIC ALGORITHM FOR TOT COMPUTATION

⇒ The first Algorithm used to set timeout timer dynamically at Tcp is

"BASIC ALGORITHM"



IRTT = 10ms. (Guessing)

TO = 2 * IRTT = 20ms

ARTT = 15ms.

NRTT = α IRTT + $(1-\alpha)$ ARTT

α = Smoothening Factor

$0 \le \alpha \le 1$ $\alpha = 0.5$

NRTT = 0.5 × 10 + (0.5) 15

NRTT = 12.5ms ⇒ TO = 25ms

⇒ This Algorithm is Dynamic Nature

⇒ The disadvantage is TO = (2) * RTT

↓

No logic why we are using "2"

∴ For Next packet IRTT = 12.5ms

TO = 2 * IRTT = 25ms.

ARTT = 20ms

NRTT = (0.5)(12.5) + (0.5)(20)

NRTT = 16.25ms

IRTT = INITIAL ROUNDTRIP TIME

ARTT = ACTUAL ROUNDTRIPTIME

NRTT = NEXT ROUNDTRIP TIME

For Next packet IRTT = 16.25

TO = 32.5ms

ARTT = 10ms

NRTT = (0.5)(16.25) + (0.5)(10)

NRTT = 13.125

21. JACOBSON'S ALGORITHM FOR TIMEOUT COMPUTATION AND KARN'S MODIFICATION

⇒ The Jacobsons Algorithm is used to set the time out timer.

①

IRTT = 10ms

ID = 5ms

TO = 4 * ID + IRTT

= 4 * 5 + 10

= 30ms

ARTT = 20ms

AD = 10ms (|IRTT − ARTT|)

NRTT = α(IRTT) + $(1-\alpha)$ (ARTT)

= 15ms (α = 0.5)

ND = α(ID) + $(1-\alpha)$(AD)

= 7.5ms

ID = Initial deviation

AD = deviation.

For the 2nd segment that you are sending

IRTT = 15ms

ID = 7.5ms

TO = 4 * ID + IRTT

= 4 * 7.5 + 15

TO = 45ms

ARTT = 30ms

AD = (30ms - 15ms) = 15ms

NRTT = α(IRTT) + (1-α)(ARTT) {α=0.5}

= (0.5)(15) + (0.5)(30)

= 7.5 + 15 = 22.5ms

ND = α(ID) + (1-α)(AD)

= (0.5)(7.5) + (0.5)(15)

= 11.25 ms

For the 3rd segment that you are sending

IRTT = 22.5 ms

ID = 11.25ms

TO = 4 * ID + IRTT

= 4 * 11.25 + 22.5

= 67.5

ARTT = 10 ms

AD = 12.5

NRTT = α(IRTT) + (1-α)(ARTT) {α=0.5}

= (0.5)(22.5) + (0.5)(10)

= 16.25

ND = α(ID) + (1-α)(AD)

= 0.5(11.25) + (0.5)(12.5)

= 11.875

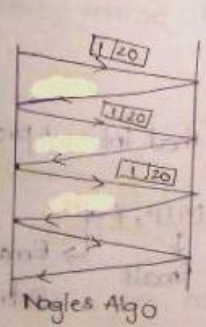
TO = 4 * D + RTT = 63.75

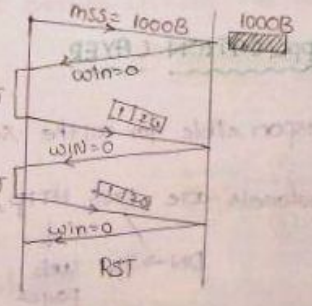
⇒ Karns modification says when you receive the Acknowledgement for the packet after the timeout, keep doubling the TOT for the next packets.

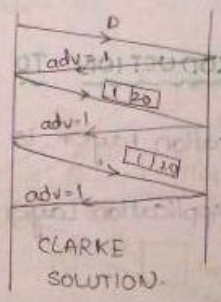
Also known as Probe Seg mode

Scenario: Receiver has advertised its window size as 1000 and sender has filled the window after some packets.
Now, window size is ZERO. So, sender will send 1 bit of data after persistent timer.

21. SILLY WINDOW SYNDROME







Another scenario: when sender is producing very small amount of data

⇒ Nagles Algo says that if sender is very slow the TL should not send 1B of data, the TL should wait for 1RTT and collect the data that has come in 1RTT time and send that data in one Segment.

⇒ Clarke Algo says that Receiver should not advertise 1 it should wait until it gets a size of 1mss or half of the Buffer.

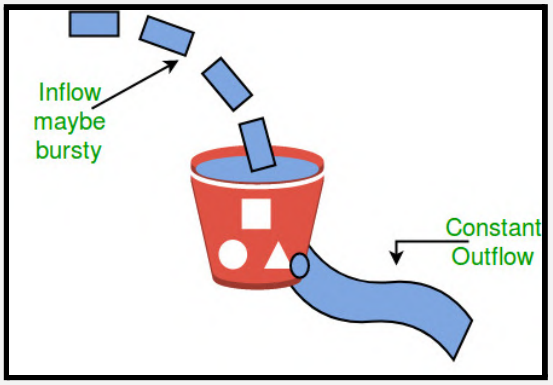
Traffic Shaping

- Another way of Congestion control is to "Shape the Traffic" before it enters the network.
- During Connection establishment, the sender and receiver negotiates a traffic pattern.
- Traffic shaping helps to regulate the rate of data transmission and reduces congestion. There are 2 types of traffic shaping algorithms:
    - Leaky Bucket
    - Token Bucket

Leaky Bucket Algorithm

Let us consider an example to understand: Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate.When the bucket is full with water additional water entering spills over the sides and is lost.

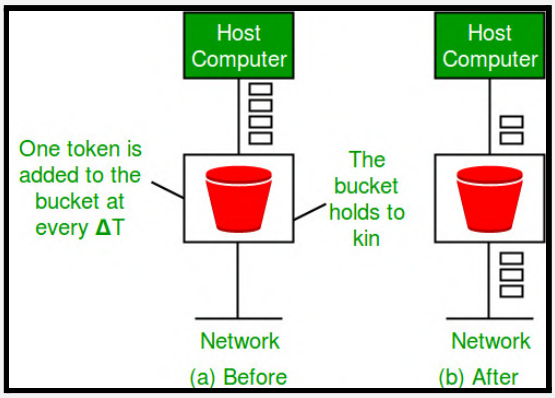
Similarly, each network interface contains a leaky bucket and the following steps are involved in leaky bucket algorithm:



- When the host wants to send a packet, the packet is thrown into the bucket.
- The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
- Bursty traffic is converted to uniform traffic by the leaky bucket.
- In practice the bucket is a finite queue that outputs at a finite rate.

Token bucket Algorithm

Need of token bucket Algorithm: The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost.

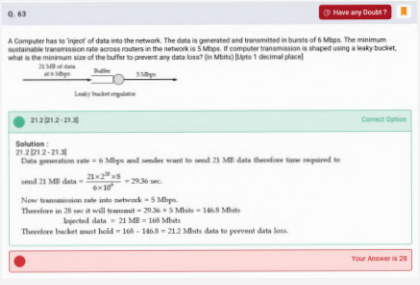


Formula: $M * t = C + \rho * t$

where t – is time taken, M – Maximum output rate

ρ – Token arrival rate

C – Capacity of the token bucket in byte



The process with the connected UDP socket can call connect() again for the socket for one of the two reasons :
* to specify a new IP address and port
* to disconnect the socket

UDP is used for IP Tunnelling & Remote procedure call(RPC)

12. UDP

1. NEED FOR UDP

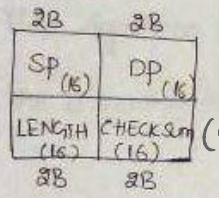
⇒ Tcp is going to be disadvantageous fore some applications they are

1> If Application needs 1 Request and 1Reply Ex: DNS, BOOTP, DHCP, NTP (Network Time protocol), NNP (Network News protocol), "Quote of day" protocol, TFTP, RIP, OSPF

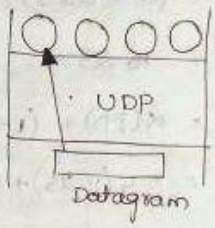
2> Broadcast or Multicast

3> fastness rather than Reliability (Multimedia Applications) (Onlinegame)

UDP HEADER



(Optional)



⇒ Check sum is calculated on UDP Header + UDP Data + pseudo Header from Ip

⇒ Udp should communicate the options to the Ip Datagram, the various options are 1> Trace route 2> Record Route 3> Time Stamp

⇒ Additional Responsibilities of UDP is, if we get any icmp error packets Udp should inform Application Layer

[Udp neither handles congestion control nor flow control.]

14. APPLICATION PROTOCOLS

1. INTRODUCTION TO APPLICATION LAYER

⇒ Application Layer is responsible for all the services that internet provide

⇒ The Application Layer protocols are DNS, HTTP, FTP, SMTP, POP

DNS → Ip
HTTP → web pages
FTP → files
SMTP → Email
POP → Email Retreiving

DNS actually uses both UDP and TCP

DNS

DNS PORT NO: 53

(47)

⇒ DNS = DOMAIN NAME SERVICE (DNS uses UDP at Transport Layer)

⇒ To convert Domain name to Ip Address we use DNS.

⇒ The various domains are 1> Generic Domains (.com, .edu, .mil, .org, .net)

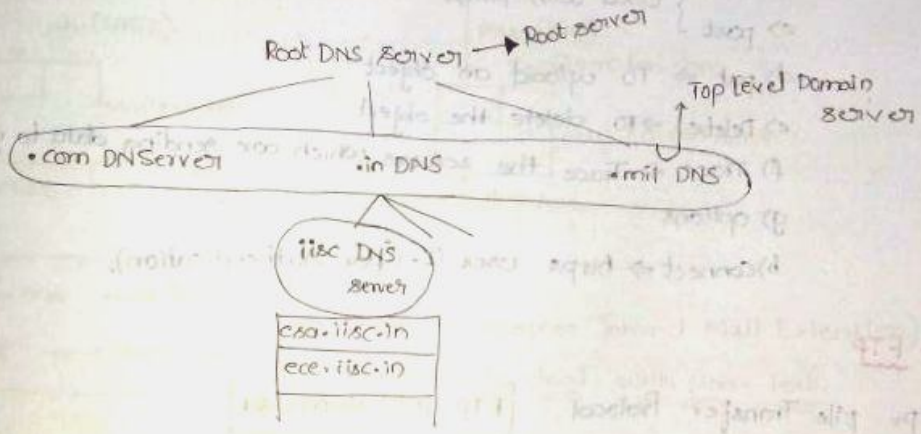
2> country Domain (.in, .us, .uk...)

3> Inverse Domain (Given Ip Address → find Domain Name)

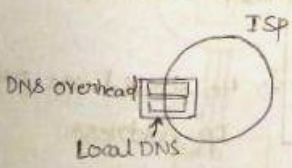
⇒ To find the ip Address of a website type "NSlookup www.google.com"

⇒ DNS is also used for Load Balancing

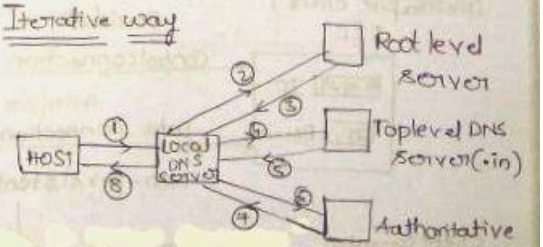
⇒ DNS Database is organised in this way (Distributed Database)



⇒ what if the Root DNS server fails, so IETF (INTERNET ENGINES TASK FORCE) mange 13 Root serves across the world.



① Iterative way

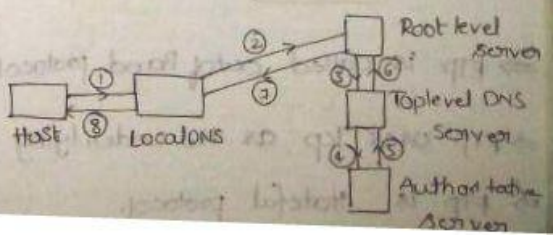


⇒ Now, let us see how local DNS is going to contact Root DNS.

1) Iterative way

2) Recursive way

② Recursive way



Story of xxx domain, 2010)

Tanenbaum - CN

https://www.geeksforgeeks.org/http-non-persistent-persistent-connection-set-2/

Q.51) NAT Subject: Computer Network Max Marks: 1

Assume that we are retrieving a HTML base file with 20 embedded objects. Consider total Round trip time(RTT's) are required to retrieve the base file and the objects under non persistent HTTP with no parallel connection. [Ignore the processing delays, closing TCP connection or any other delays].

Time taken to answer this question 00:03:59 hrs

Hide Answer | Add Notes | View Notes | Show Comments

Correct Answer

Solution: nil

Note: Marks is assigned to all here as no question is being asked here.

For non persistent HTTP with no parallel connection:
2 RTT = one for TCP connection + one for base file.
20 objects = Each object requires 2 RTT = 40 RTT
X = 2 + 20 = 42 RTT.

Q. 41 Have any Doubt ?

Assume that you have made a request for a web page through your web browser to a web server. Initially the browser cache is empty. Further, the browser is configured to send HTTP requests in persistent mode. The web page contains text and 26 very small images. The minimum number of TCP connections required to display the web page completely in your browser is _____.

27 Correct Option

Solution :
27
Since requests in persistent mode. So, it requires connection setup every time each object. Here 1 text and 26 images.
So, total 27 connections are required.

Your Answer is 28

3. HTTP

HTTP => PORT NO = 80

⇒ Hyper text transfer protocol (For getting web pages).

⇒ Http always need Reliability.

⇒ Http uses "Tcp" at Transport Layer

⇒ Http is Inband protocol (Both data and commands goin one connection)

⇒ Http is stateless protocol.

⇒ The two popular versions of Http are: Http1.0 (Non-persistent connection)
Http1.1 (persistent connection)

⇒ The popular methods that are used by Http are

a) Head ⇒ Get the Header of webpage (metadata).

b) Get } used with forms
c) post }

d) put ⇒ To upload an object

e) Delete ⇒ To delete the object

f) Trace ⇒ Trace the servers which are sending data to you.

g) options

h) Connect ⇒ https uses it. (For Authentication).

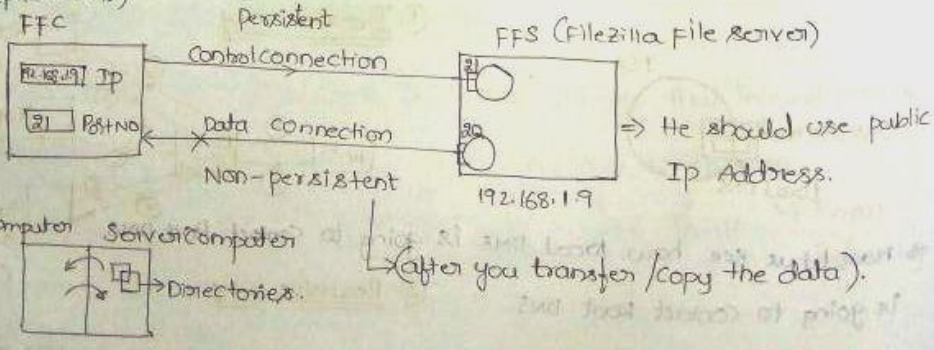
4. FTP

FTP = File Transfer Protocol. FTP PORT NUM = 21

⇒ Tecfia, filezilla are the two most popular FTP's.

⇒ FTP is used to transfer files.

(filezilla file client)



⇒ FTP is called out of Band protocol and requires Reliability.

⇒ FTP uses Tcp as the underlying protocol

⇒ FTP is stateful protocol.

Stateful protocols

5. SMTP AND POP

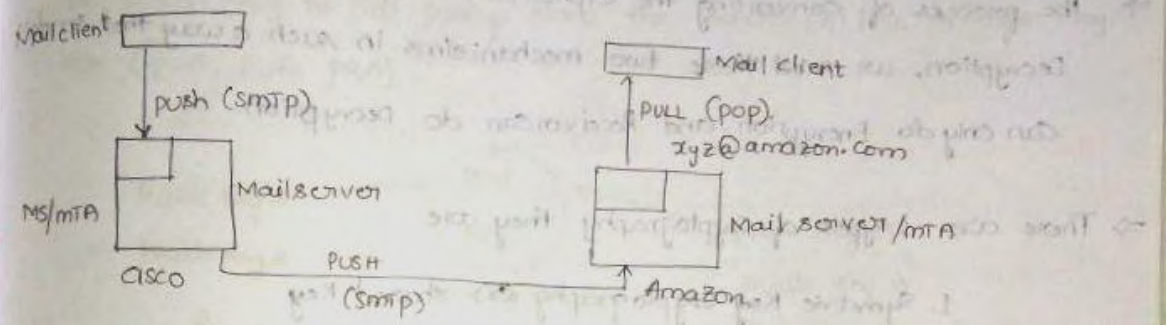
SMTP= Simple Mail Transfer Protocol, POP= post office protocol.

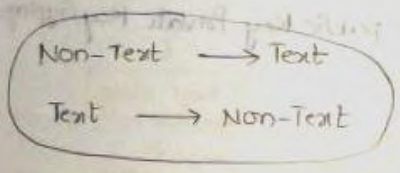
⇒ E-mails are transfered using SMTP

⇒ we cannot transfer the files using FTP because to transfer the files using FTP both server and client should be online.

⇒ Gmail is the webBased mail

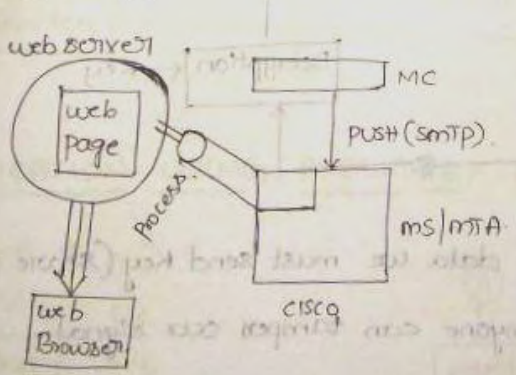
⇒ MTA= Mail Transfer Agent

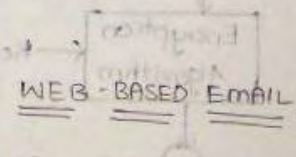




→ MIME (Multipurpose Internet Mail Extension) protocol) To deal with Non-Text.

What Gmail does is,





⇒ SMTP and pop are In band protocol.

Computer Networks - Marks Distribution

	Physical layer	Data link layer	Network layer	Transport layer	Application layer	Security	Mixed que	Total
2021 set-2	0	4	2	1	0	0	0	7
2021 set-1	0	4	3	2	0			9
2020	0	0	3	2	1	0	0	6
2019	0	2	4	0	1	2	0	9
2018	0	0	2	4	0	0	1	7
2017-1	0	4	0	1	0	3	0	8
2017-2	0	2	3	1	0	0	0	6
2016-1	0	2	4	0	2	2	0	10
2016-2	0	7	0	0	1	1	0	9
2015-1	0	2	1	3	1	1	0	8
2015-2	0	1	4	3	0	0	0	8
2015-3	0	3	4	1	0	0	0	8
2014-1	0	2	1	2	0	1	0	6
2014-2	0	1	3	1	0	2	0	7
2014-3	0	1	6	0	0	0	1	8
Avg Marks:	0.0	2.9	3.3	1.8	0.5	1.0	0.2	9.7

		Sub Topics	2014-1	2014-2	2014-3	2015-1	2015-2	2015-3	2016-1	2016-2	2017-1	2017-2	2018	2019	2020	2021-1	2021-2	Total	
4	**Physical layer**																		No questions seen recently.
6	**Data link layer**	Flow control	2			2	1	2	2	2	2	2				2		17	**1.** Stop and wait **2.** Go back N **3.** Selective repeat
7		MAC protocols						1		2							2	5	1. CSMA/CD 2. Aloha
8		LAN technologies		1						3								4	**1.** 802.11 specification **2.** 802.3 specification 3. Token ring
9		Error detection									2					2	2	6	**1.** Cycle redundncy check (CRC) **2.** Hamming distance **3.** Parity
10		Framing			1													1	**1.** Bit stuffing **2.** Byte stuffing
11		LAN devices												2				2	**1.** Switch **2.** Hub **3.** bridge
13	**Network layer**	IPV4 header			3	1						1						5	Every field of IPV4 header is important
14		Fragmentation			2		2		2				2		1	2		11	**1.**Maxmum transmission unit **2** DF, MF, ID bit
15		Routing	1	1								1					2	5	**1.** Distance vector **2.** Link state **3.** RIP/OSPF protocols
16		IP addressing			2		2	2						2	2			10	**1.** Classful addressing **2.** CIDR **3.** Subnetting **4.** Supernetting
17		Switching		2				2										4	**1.** Packet switching **2.** Circuit Switching
18		Protocols												2		1		3	**1.** ARP/RARP **2.** DHCP/ BOOTP **3.** ICMP
19		Traffic shaping							2									2	**1.** Token bucket
21	**Transport layer**	Flow control				1	2	1					1					5	**1.** Retransmissions in TCP **2.** TCP flow control using advertised window
22		Congestion control	2			2							3		2			9	**1.** Slow start **2.** Congestion avoidance **3.** Multiple decrease [AMID]
23		TCP transition state									1					2	1	4	**1.** State transition diagram
24		TCP socket		1			1											2	**1.** Connet, listen functionality
25		UDP										1						1	**1.** UDP header **2.** Comparison between UDP and TCP
27	**Application layer**	HTTP/SMTP/POP3/ IMPA4				1			1					1	1			4	Mixed question from all protocols, HTTP question on persitent and non p
28		DNS/DHCP		2					1									3	All protocols are imortant , mixed question from all
30	**Mixed Questions**	Layering			1								1					2	Mixed question on OSI layers, network devices

https://docs.google.com/spreadsheets/u/0/d/13mQ0FpVFPNV88vzRsqtlfQCbewcEGmU32dsoE8U3kbc/htmlview#gid=0