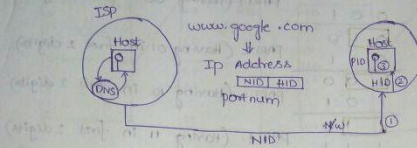


COMPUTER NETWORKS

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 number are already predefined and fixed

http $\Rightarrow$ port num = 80

SMTP port num = 25

Ftp $\Rightarrow$ port num = 21

⇒ Even though your intention is to reach google.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 overhead 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, 1

Binary = 0, 1

Octal = 0, 1, 2, ..., 7

Decimals = 0, 1, 2, ..., 9

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

A 16 -- F
10 11 15

$2^2 = 4$

$2^{10} = 1024 = K$

$M = 2^{20}$

$G = 2^{30}$

$T = 2^{40}$

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

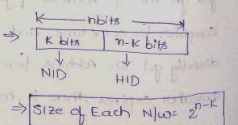
⇒ So, if i have 'n' bits the no. of possible ways are 2^n K bits 2^n combinations

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

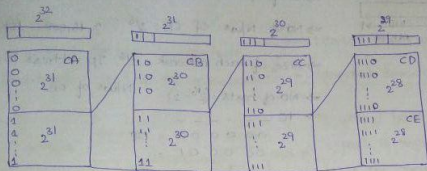


⇒ In operating system 'n' bits = Address, K = page offset / Block no / Segment no

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

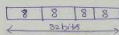
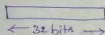
⇒ IP Address size = 32 bits in CN. ⇒ 2^{32} IP Address are possible

CLASS FULL 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^{20} class D = 2^{28}

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



Dotted decimal Notation (192.168.173.9)

CA = start with 0

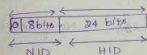
CD = starts with 1110

CB = start with 10

CE = start with 1111

CC = start with 110

CLASS A



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

⇒ 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

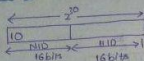
0 - - - - -
 00000000 = 0
 00000001 = 1
 11111111 = 127

⇒ we don't use the starting Address (All 0s) and Last Address (All ones)

⇒ ∴ No. of N/ws in CA = $128 - 2 = 126$ practically.

RANGE = 0-126

CLASS B



$$\Rightarrow \text{No of Ip Addresses} = 2^{16}$$

$$\Rightarrow \text{No of N/w's of CB} = 2^{16} \approx 16,000 = 16K \text{ N/w's}$$

$$\Rightarrow \text{Size of each network} = 2^{16} \text{ Ip Address in one N/w's of CB.}$$

$$\Rightarrow \text{No. of hosts} = (2^{16} - 2)$$

$$\Rightarrow 10 \text{ --- --}$$

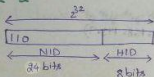
$$00 \ 00 \ 00 = 128$$

$$00 \ 00 \ 01 =$$

$$11 \ 11 \ 11 = 191$$

$$\Rightarrow \text{RANGE} = 128 - 191$$

CLASS C



$$\Rightarrow \text{No. of Ip Addresses} = 2^{24}$$

$$\Rightarrow \text{No. of N/w's of CC} = 2^{24} \text{ N/w's} = 2 \text{ million}$$

$$\Rightarrow \text{Size of Each N/w} = 2^{24} \text{ Ip Address are in one N/w of CC}$$

$$\Rightarrow 110 \text{ --- --}$$

$$00 \ 00 \ 00 = 192$$

$$00 \ 00 \ 01 = 193$$

$$111 \ 111 \ 111 = 223 \Rightarrow \text{No. of hosts} = (2^{24} - 2)$$

$$\Rightarrow \text{RANGE} = 192 - 223$$

CLASS D

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

CD

$$1110 \text{ --- --}$$

$$00 \ 00 = 224$$

$$111 \ 111 = 239$$

$$\text{RANGE} = 224 - 239$$

CE

$$1111 \text{ --- --}$$

$$00 \ 00 =$$

$$111 \ 111 = 255$$

$$\text{RANGE} = 240 - 255$$

- ↓
- Used for Multicasting
 - Group Emailing, Group Broadcasting

- ↓
- Used for Military Applications

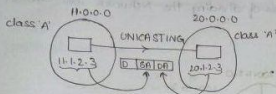
2. TYPES OF CASTING - UNICAST, LIMITED BROADCAST, DIRECTED BROADCAST

CASTING

1. Unicast - one host to one host
2. Broadcast - one host to many hosts

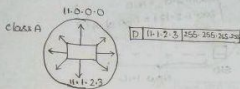
Limited Broadcasting

Directed Broadcasting



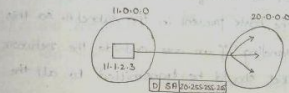
⇒ when i have All 0s in the HID part it represents NID that is the reason we don't use 1st Ip Address as the valid Ip Address to any host

LIMITED BROADCASTING



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

DIRECTED BROADCASTING



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

DBA = NID, HID = all 1s

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

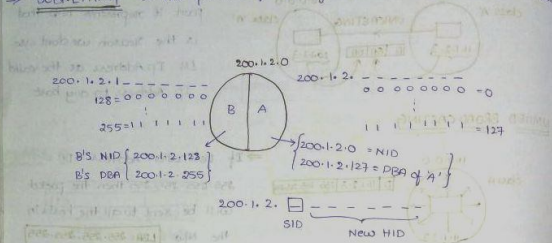
X

3 SUBNETS, SUBNET MASK, ROUTING

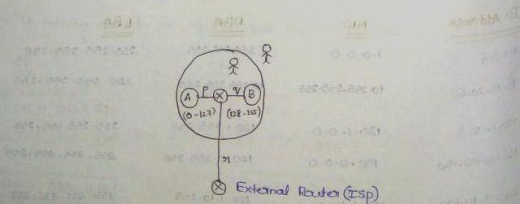
⇒ when the size of the N/w is Big then the maintenance will be difficult.

⇒ 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 Network.

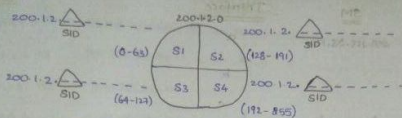


Now, ambiguity arises in the above subnetting, if I say 200.1.2.0 I mean the whole network or only the first subnet and if I say 200.1.2.128 then there is a dilemma whether to transfer the packet to all the hosts in the Network or only to the hosts present in the subnet A. so this depends upon where 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 transmitted to the hosts in subnet A.

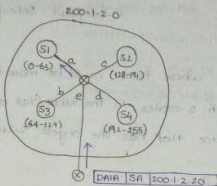


*) There will be loss of IP addresses due to "SUBNETTING"

FOUR SUBNETS



The, practical view is.



⇒ Here the challenge is you should identify the N/w 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 N/w will be

$\frac{NID}{200.1.2.} \quad \frac{HID}{SID}$

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 belongs

Ip: 11001000.00000001.00000010.10000000 = 200.1.2.130

SM: 11111111.11111111.11111111.11000000 = 255.255.255.192

NID: 11001000.00000001.00000010.10000000

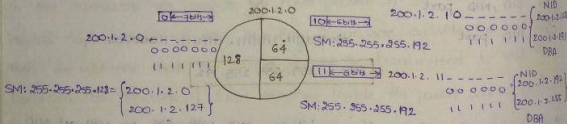
200.1.2.128

ROUTING TABLE

<u>NID</u>	<u>SM</u>	<u>Interface</u>
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 specific)

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

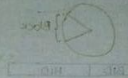
⇒ The N/w that are having same sizes have the same "subnet mask".

⇒ 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

$$: 11111111 \cdot 11111111 \cdot 11111111 \cdot 11000000 = (26 \text{ bits, } 6 \text{ bits})$$

$$: \text{NID} + \text{SID} = \text{No of bits}$$

$$: \text{NID} + \text{SID} = 26 \rightarrow \text{If class is subnetted, then,}$$

$$0 - 00000000$$

$$128 - 10000000$$

$$192 - 11000000$$

$$224 - 11100000$$

$$240 - 11110000$$

$$248 - 11111000$$

$$252 - 11111100$$

$$254 - 11111110$$

$$255 - 11111111$$

$$8 + \text{SID} = 26 \Rightarrow \boxed{\text{SID} = 18}$$

$$= \text{No of Subnets} = 2^8$$

$$\rightarrow \text{If CB, NID} + \text{SID} = 26$$

$$\boxed{\text{SID} = 26 - 16 = 10} = 2^{10} \text{ Subnets}$$

$$\rightarrow \text{If CC, NID} + \text{SID} = 26$$

$$\boxed{\text{SID} = 26 - 24 = 2} = 2^2 \text{ Subnets}$$

5. SUBNET MASKS

SUBNET MASK	NO. OF HOSTS	SUBNETS IN CA	CB	CC
CA 255.0.0.0	$2^{24} - 2$	$2^0 - 2$	—	—
255.128.0.0	$2^{23} - 2$	$2^1 - 2$	—	—
255.192.0.0	$2^{22} - 2$	$2^2 - 2$	—	—
255.240.0.0	$2^{20} - 2$	$2^4 - 2$	—	—
CB 255.255.0.0	$2^{16} - 2$	$2^8 - 2$	$2^8 - 2$	—
255.255.96.0	$2^{17} - 2$	$2^{15} - 2$	$2^7 - 2$	—
CC 255.255.255.0	$2^8 - 2$	2^{16}	2^8	1
255.255.255.224	$2^5 - 2$	2^{19}	2^4	2^3
255.255.255.240	$2^4 - 2$	2^{20}	2^{12}	2^4

CLASSLESS INTER DOMAIN ROUTING (L-6)

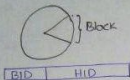
IANA = Internet Assigned Number Authority.

⇒ Generally the IP Addresses in CIDR Notation

is represented as a.b.c.d/n

⇒ n = NID bits ⇒ if n = 20, NID = 20 bits

⇒ n = Slash Number



FORMATION OF CIDR BLOCKS

These are the Rules for forming CIDR Blocks

1) All the IP Addresses should be contiguous :

2) The Block size should be a power of 2

$(n-k)$ bits | k bits
← n-bit → Binary Number

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

$[m/2^k] \Rightarrow$ last k bits = Remainder
last (n-k) bits = Quotient

if 100.1.2.32 } Whether these IP Addresses form a CIDR Block?

100.1.2.33 } Rule 1 ✓

100.1.2.47 } Rule 2: No. of IP Addresses = 16 = 2^4 ✓ HID = 4, BID = 28

Rule 3: 100.1.2.00100000 $\div 2^4 =$ LSB (4 bits) { Least significant Bits }
= 0000 ✓

∴ They form CIDR Block

2) 20.10.30.32 } Rule 1 = ✓

20.10.30.33

20.10.30.34

20.10.30.63

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

Rule 3: 20.10.30.00100000 $\div 2^5 =$ last 5 bits
= 00000 ✓

∴ They form CIDR Block

37

150.10.20.64
150.10.20.65
150.10.20.66
150.10.20.127

Rule 1 ✓

Rule 2: $(127 - 64) + 1 = 64 = 2^6 \checkmark \Rightarrow \text{HID} = 6, \text{BID} = 26 \text{ Bits}$

Rule 3: $150.10.20.01000000 \div 2^6 = 000000 \checkmark$

FORM
CIDR
BLOCK ✓

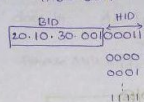
47

20.10.30.35/27

Derive the Range of CIDR Block?

$\Rightarrow \text{BID} = 27 \text{ bits}$

$\text{HID} = 5 \text{ bits}$



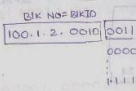
$\Rightarrow \text{Block} = 20.10.30.32$
 $20.10.30.33$
 $\vdots$
 $20.10.30.63$

57

100.1.2.35/28

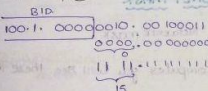
$\text{BID} = 27 \text{ bits}$

$\text{HID} = 5 \text{ bits}$



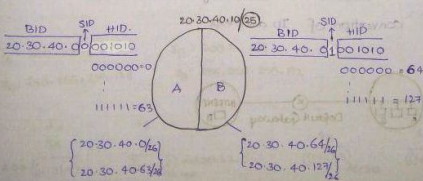
$100.1.2.32$
 $100.1.2.33$
 $\vdots$
 $100.1.2.47$

67 100.1.2.35/20



$100.1.0.0$
 $\vdots$
 $100.1.15.255$

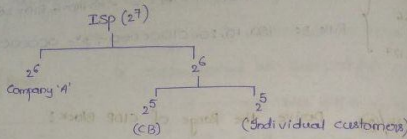
1. SUBNETTING IN CIDR, VLSM IN CIDR



$\{ 20.30.40.0/26$
 $20.30.40.64/26$

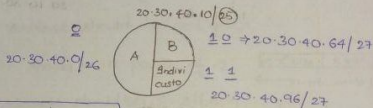
VLSM IN CIDR BLOCKS

1) 20.30.40.10/25



Now, BLK ID
20.30.40.0000 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 INTERESTING PROBLEM ON SUBNET MASK

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

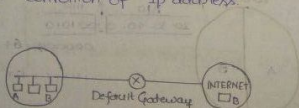
⇒ whenever you open "ipconfig" in your computer you will see these things

1) IPv4 Address: provided by ISP

2) Default Gate way: Default Router connected to your n/w

3) Subnet Mask: Subnet mask which you should use

4) DNS: Conversion of Ip address.



Let I_A = Ip Address of 'A' I_B = Ip Address of 'B' (7)

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 DSW and DSW 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

$$\text{Bitwise AND} = \frac{I_A}{S_A} \quad \frac{I_B}{S_B}$$

$$\frac{((NID)A)}{AcctoA} \quad \frac{((NID)B)}{AcctoA}$$

If $\frac{((NID)A)}{AcctoA} = \frac{((NID)B)}{AcctoA}$ then A/B are in same N/w

1/

$I_A: 200.1.2.10$

$I_B: 200.1.2.130$

$S_A = 255.255.255.128$

Now, $I_A: 11001000.00000001.00000010.00001010$

$S_A: 11111111.11111111.11111111.10000000$

$200.1.2.10$

$\frac{((NID)A)}{AcctoA} = 200.1.2.0$

$I_B: 200.1.2.130$

$S_B: 255.255.255.128$

$\frac{((NID)B)}{AcctoA} = 200.1.2.128$

$\frac{((NID)A)}{AcctoA} \neq \frac{((NID)B)}{AcctoA}$ ∴ 'A' assumes that 'B' is in diff Network.

2/ $I_A: 200.1.2.10$

$I_B: 200.1.1.69$

$S_A: 255.255.255.128$

$S_B: 255.255.255.128$

$I_A: 200.1.2.10$

$I_B: 200.1.1.69$

$S_A: 255.255.255.128$

$S_B: 255.255.255.128$

$\frac{((NID)A)}{AcctoA} = 200.1.2.0$

$\frac{((NID)B)}{AcctoA} = 200.1.2.0$

$I_B: 200.1.1.69$

$S_B: 255.255.255.128$

$\frac{((NID)B)}{AcctoB} = 200.1.1.0$

$I_A: 200.1.2.10$

$S_B: 255.255.255.128$

$\frac{((NID)A)}{AcctoB} = 200.1.2.0$

If $\frac{((NID)A)}{AcctoA} = \frac{((NID)B)}{AcctoA}$ ⇒ '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/super the Networks.

RULES FOR AGGREGATION

- 1) All the N/w's should be contiguous. (N/w Id's)
- 2) Size of each N/w should be same and intwin they should be in powers of 2.
- 3) Int. Address should be divisible by size of Block.

Aggregate the following N/w's

$$200.1.0.0/24$$

Rule 1 ✓

Total size of N/w's
 $= 2^{10}$

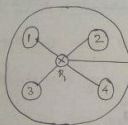
$$200.1.1.0/24$$

Rule 2: ✓

$$200.1.2.0/24$$

$$\text{Rule 3: } \checkmark \quad 200.1.0.00000000.00000000 \div 2^{10} \\ = \text{Divisible}$$

$$200.1.3.0/24$$



The Routing table at R_2 looks like

NID	BM	INTERFACE
200.1.0.0	255.255.255.0	a
200.1.1.0	255.255.255.0	a
200.1.2.0	255.255.255.0	a
200.1.3.0	255.255.255.0	a

SUPERNET MASK

Supernet mask: 32bits

: No. of 1's = Fixed part

: No. of 0's = Variable part

FIXED PART	VARIABLE PART
200.1.0.000000	00.00000000
200.1.0.000000	01.00000000
200.1.0.000000	10.00000000
200.1.0.000000	11.00000000
255.255.111111	00.00000000

Supernet = 255.255.252.0
mask

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

SHORT CUT TO FIND FIXED AND VARIABLE PARTS

⇒ Size of all N/w = $2^8 + 2^8 + 2^8 + 2^3 = 2^{10}$ ⇒ Host id part should contain 20 bits

⇒ All N/w's will at least contain 20 bits ⇒ BID part contain 22 bits

⇒ Now, the Routing table at R₂ look like

NID	SM	INTERFACE
200.1.0.0	255.255.252.0	a

27

100.1.2.0/25

100.1.2.128/26

100.1.2.192/26

Aggregate them!

⇒ All the Address are contiguous ✓, but of diff size

⇒ The N/w's $\left. \begin{matrix} 100.1.2.128/26 \\ 100.1.2.192/26 \end{matrix} \right\}$ These can be Aggregated first ← Rule 1 ✓
 Rule 2 ✓
 Rule 3 ✓

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



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

Data = 10 bits

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

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

$$\text{Transmission delay} = \frac{L}{B} \text{ sec}$$

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

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

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

DATA

$$K = 1024 \text{ bits}$$

$$M = 1024 \times 1024$$

$$G = 1024 \times 1024 \times 1024$$

BANDWIDTH

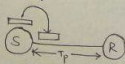
$$K = 1000$$

$$M = 1000 \times 1000 = 10^6$$

$$G = 1000 \times 1000 \times 1000 = 10^9$$

PROPAGATION 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 "propagation delay".



The propagation delay depends upon 1) distance

2) velocity

$$T_p = \frac{d}{V}$$

⇒ In case of optical fiber the speed of the signal is approximately 70% of speed of Light ⇒ $v = \frac{70}{100} \times 3 \times 10^8 \text{ m/s}$

$$\Rightarrow v = 2.1 \times 10^8 \text{ m/s}$$

1) $d = 2.1 \text{ km}$

$$v = 2.1 \times 10^8 \text{ m/s}$$

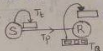
$$T_p = \frac{d}{v} = \frac{2.1 \times 10^3 \text{ m}}{2.1 \times 10^8 \text{ m/s}} = 10^{-5} \text{ sec} = \frac{10^{-5} \times 10^3}{10^3} = 10^{-2} \text{ msec}$$

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

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

QUEUING DELAY (T_q):

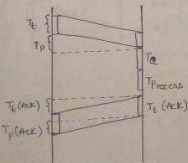
⇒ The amount of time the packet sits in the queue before it gets processed is called queuing delay (T_q).



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



$$\text{Total time} = T_L(\text{data}) + T_P(\text{data}) + T_R + T_P(\text{ack}) + T_L(\text{ack})$$

$$= T_L(\text{data}) + T_P(\text{data}) + T_P(\text{ack}) + T_L(\text{ack})$$

$$= T_L(\text{data}) + 2 * T_P + T_L(\text{ack})$$

$$\text{Total time} = T_L + 2 * T_P \text{ for sending 1 packet}$$

$$\eta = \frac{\text{Useful time}}{\text{Total cycle time}} = \frac{T_L}{T_L + 2 * T_P} = \frac{T_L}{T_L(1 + 2 \frac{T_P}{T_L})} = \frac{1}{1 + 2a} \text{ (where } \frac{T_P}{T_L} = a \text{)}$$

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

$$\Rightarrow \text{Throughput} = \frac{L}{T_t + 2 * T_p} \Rightarrow \frac{L * B * (\frac{1}{8})}{T_t + 2 * T_p} = \frac{T_t}{T_t + 2 * T_p} * Bw$$

Effective Bandwidth/
Bandwidth utilization
Link utilization

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

$$\therefore \text{Throughput} = \eta * Bw$$

1)

$$T_t = 1 \text{ msec}$$

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

$$T_p = 1 \text{ msec}$$

2)

$$T_t = 2 \text{ msec}$$

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

$$T_p = 1 \text{ msec}$$

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

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

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

$$\Rightarrow T_t \geq 2 * T_p$$

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

$$p4) Bw = 4 \text{ Mbps}$$

$$T_p = 1 \text{ msec}$$

$L = ?$ so that η is atleast 50%.

$$L \geq 2 * T_p * Bw$$

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

$$L \geq 8 * 10^3 \text{ bits}$$

$\Rightarrow \text{Now, } \eta = \frac{1}{1+2a} = \frac{1}{2 + 2(\frac{TP_p}{TP_d})} = \frac{1}{1 + 2 * \frac{d}{V} * \frac{R}{L}} \Rightarrow \boxed{\eta \propto \frac{1}{d}}$ Saw. index for LANs. (15)
 $\Rightarrow \boxed{\eta \propto L}$

57

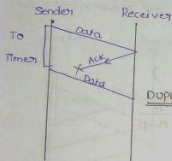


$\therefore$ STOP AND WAIT + TIMEOUT TIMER

$\Rightarrow$ STOP AND WAIT ARQ {Automatic Repeat Request}

DATA PACKET LOSS PROBLEM $\Rightarrow$ {overcome by TO timer}

58 ACK LOST PROBLEM

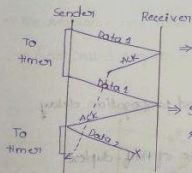


$\Rightarrow$ Acc to sender both the data packets are same but Acc to Receiver both the packets are different.

DUPLICATE PACKET PROBLEM $\Rightarrow$ {To overcome this have sequence numbers}

SAW + TO + SEQ NO TO DATA PACKET

59 DELAYED ACKNOWLEDGEMENT



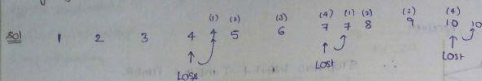
$\Rightarrow$ This problem can be overcome by having Seqno on Ack also.

$\Rightarrow$ If the Receiver receives D_1 successfully then it sends Ack A_2 which means { "I have successfully received D_1 , please send D_2 }



$\Rightarrow$ SAW + TO + SEQ NO TO DATA AND ACK

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



∴ Total = 13, (4/7/8) → packets are Retransmitted

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 transmitted totally

$$\underline{\text{sol}} \Rightarrow 400 + 400(0.2) + \{400(0.2)\}(0.2) + \dots$$

$$\Rightarrow n + np + np^2 + \dots \Rightarrow n(1 + p + p^2 + p^3 + \dots)$$

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

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

3. CAPACITY OF PIPE AND PIPELINING

CAPACITY OF A CHANNEL / WIRE / LINK

The capacity of channel depends on Bandwidth and propagation delay

$$\text{Capacity of the channel} = \text{BW} \times T_p \quad \text{Increase of half-duplex}$$

$$\text{Capacity} = 2 \times \text{BW} \times T_p \Rightarrow \text{Increase of full duplex}$$

PIPELINING

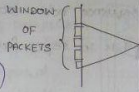
T_L sec - 1 packet

1 sec - $\frac{1}{T_L}$ packets

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

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

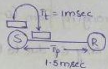
$$\Rightarrow T_L + 2 * T_p = (1 + 2a) \text{ packets } (a = T_p / T_L)$$



Given,

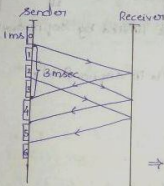
$$T_L = 1 \text{ msec}$$

$$T_p = 1.5 \text{ msec}$$

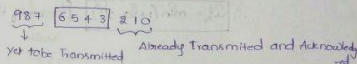


$$\Rightarrow \eta = \frac{T_L}{T_L + 2 * T_p} = \frac{1}{1 + 2(1.5)} = \frac{1}{4} = 25\%$$

Now to increase the efficiency of stop and wait protocol,



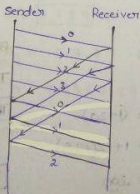
$$\text{Round trip time} = 2 * T_p$$



$\Rightarrow$ The sender window size in sliding window

$$\text{protocol} = W_s = 1 + 2a$$

$\Rightarrow$ 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 field = $\log_2(1 + 2a)$

$$\Rightarrow n \log_2(1 + 2a)$$

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

$2x T_k = 1 \text{ ms}$
 $T_p = 49.5 \text{ ms}$

} what is the sender window size to get max efficiency?

$$\text{sol } w_s = 1 + 2a \Rightarrow 1 + 2(T_p/T_k) = 1 + 2(49.5) = 100$$

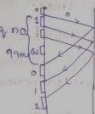
$$\text{Min. no. of sequence no.s} = 100 = (1 + 2a)$$

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

⇒ Now, in the above problem if the min. no. of bits in seq. no. field is 6, then we can get 64 seq. no.s (2⁶) ranging from 0-63

$$\Rightarrow \eta = \frac{64}{100} = 0.64$$

↳ I can send 100 packets in the time available



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

$$w_s = \min(1 + 2a, 2^n) \quad \left\{ \begin{array}{l} n = \text{no. of bits in seq. no. field} \end{array} \right.$$

GO BACK - N (G-B)

Sliding window protocol

Go-Back N (cumulative Ack)

selective Repeat

GOBACK - N (N > 1)

i) Sender window size in GBN is "N"

$$T_k = 1 \text{ msec}$$

$$T_p = 49.5 \text{ msec}$$

$$\text{GOBACK - 10}$$

$$\text{Max window size} = (1 + 2a)$$

$$= 1 + 2(49.5)$$

$$= 100$$

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

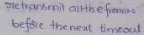
$$Bw = 40 \text{ Mbps}$$

$$\text{Throughput} = ?$$

$$Th \Rightarrow \eta \times Bw$$

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

$$Th = 4 \text{ Mbps}$$



if we have to send 10 packets, then how many transmissions are Required?



1

Transmitted

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

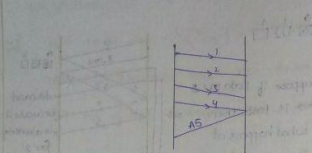
6 7 8 9

67 89 10

9 10 8 9 10

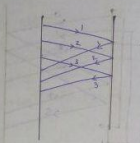
= 17 transmissions

57 Acknowledgements: There are 2 kinds of Ack $\rightarrow$ Cumulative Ack
27 Independent Ack



Advantages: Less traffic

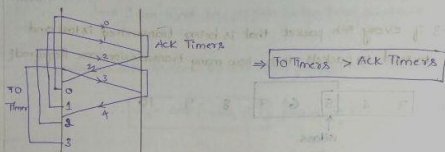
Disadvantages: Less Reliability



Advantages: Reliability is high

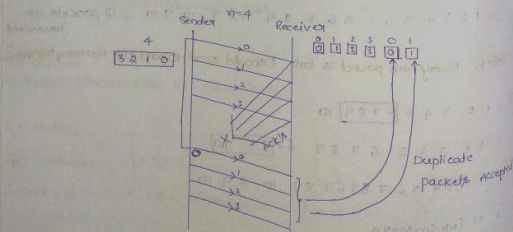
Disadvantage: More Traffic

$\Rightarrow$ GoBack-N uses cumulative Acknowledgements.



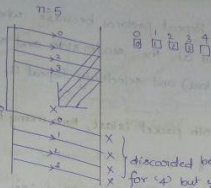
RELATIONSHIP BETWEEN WINDOW SIZES AND SEQUENCE NOS IN GBN

GBN-4 $\rightarrow$ Sender window size = 4 $\rightarrow$ No. of sequence no.



$\therefore$ This scenario $\Rightarrow$ (having the sequence nos = window size) don't work

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



$\Rightarrow$ In general if the sender window size = 'N' and if the Receiver window size = 4 then to detect the Duplicate packets in GBN the No. of Seq. nos. should be $(N+1)$.

$\Rightarrow$ In any sliding window protocol if it has to work without any problem the condition is $(w_3 + w_2) \leq \text{ASN}$ (Available Sequence nos.)

$\Rightarrow$ If $w_3 = N$, $w_2 = 1 \Rightarrow \text{Seq. nos.} = N+1 \Rightarrow \text{No. of bits in Seq. no. field} = \lceil \log_2(N+1) \rceil$

$\Rightarrow$ If Seq. Nos. = N then what is the max value of $w_3 = N-1$, $w_2 = 1$

$\Rightarrow$ No. of bits in Seq. no. field = K then $w_3 = 2^K - 1$, $w_2 = 1$, No. of Seq. Nos. = 2^K

SELECTIVE REPEAT AND COMPARISON BETWEEN ALL SLIDING

WINDOW PROTOCOLS

1) $w_3 > 1$

$T_f = 1 \text{ ms}$, $T_p = 49.5 \text{ msec}$, $w_3 = 50$, In SR-protocol $\eta = ?$

$$\eta = \frac{50}{100} \Rightarrow \boxed{\eta = 50\%}$$

Max window size = 1+20
of sender = 1+2(49.5)
= 100

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

if $w_R = w_S$

→ 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 10

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

= 12 transmissions

SR $\cong$ GBN Intermix of efficiency

SR $\cong$ SAW Intermix of Retransmissions

3r The Ack case independently 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).

	$\frac{SAW}{1}$	$\frac{GBN}{N}$	$\frac{SR}{N} \rightarrow$ Sender window size
Efficiency	$(1+2\alpha)$	$(1+2\alpha)$	$(1+2\alpha)$

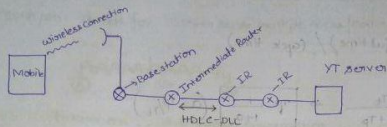
Buffers $2N$ $N+1$ $N+1$ $N+1$

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 Repeat protocol with n-bit frame sequence numbers is 2^{n-1}

PRACTICAL SCENARIO WHERE SR AND GBN ARE USED

(19)



- ⇒ Generally the Intermediate Routers are connected with Thick wires.
- ⇒ Bandwidth is high and error rate is low, out of order are not possible.
- ⇒ cpus 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 ↑

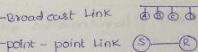
⇒ SR protocol is used.

∴ Link to Link protocols like HDLC-(BL) uses "GBN" mode.

End to End protocols like TCP uses "SR" TCP-(Transport layer)

6. INTRODUCTION TO ACCESS CONTROL METHODS, TDM, POLLING

The are two types of Links



TDM

⇒ TDM stands for Time Division Multiplexing.

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



$$\eta = (\text{cycle time})^{-1} \times (\text{useful time})$$

$$\eta = (\text{useful time}) / (\text{cycle time})$$

$$\eta = \frac{T_L}{T_L + T_P} \Rightarrow \boxed{\eta = \frac{1}{1+a}} \cdot (a = T_P/T_L)$$

1) $T_L = 1 \text{ msec}$ and η of TDM? $\eta = \frac{1}{1+a} = \frac{1}{1+1} = \frac{1}{2} = 50\%$
 $T_P = 1 \text{ ms}$

BW = 4 Mbps Throughput = $\eta \times \text{BW} = \frac{1}{2} \times 4 = 2 \text{ Mbps}$

Now, if 'N' Stations, are connected to the channel and each station

Requires 2 kbps BW then what is the max value of N?

$$\Rightarrow N \times 2 \text{ kbps} = 2 \text{ Mbps}$$

$$\Rightarrow \boxed{N = 1000}$$

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 allotted will be wasted.

POLLING



$$\eta = (\text{useful time}) / (\text{cycle time})$$

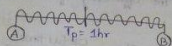
$$\eta = \frac{T_L}{T_{\text{poll}} + T_L + T_P}$$

$$\boxed{\eta = \frac{T_L}{T_{\text{poll}} + T_L + T_P}} \quad \text{Throughput} = \eta \times \text{BW}$$

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

7. CSMA/CD

⇒ The CSMA/CD stands for Carrier Sense Multiple Access / Collision Detection.



$t = 10:00 \text{ AM}$, A/B starts transmitting

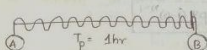
$t = 10:30 \text{ AM}$, collision

$t = 11:00 \text{ AM}$, collision signals observed by A/B

⇒ Now, if A/B must be aware about their data (i.e., whether the data that they are transmitting got collided or others data) the condition is

$$T_E > T_p$$

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



10:00:00 AM, A starts transmitting

10:59:59 AM, B starts transmitting

11:00:00 AM, collision

12:00:00 AM, A sees the collision signal.

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

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

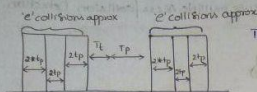
$$\Rightarrow T_E \geq 2 * T_p \Rightarrow L_B \geq 2 * T_p$$

$$\Rightarrow L \geq 2 * T_p * B = \text{This is the min. size of packet to detect collision}$$

⇒ There are NOACK in CSMA/CD.

⇒ CSMA/CD is used in Ethernet

EFFICIENCY OF CSMA/CD/ETHERNET



The efficiency of csma/cd is

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

$$\eta = \frac{T_c}{[C * 2 * t_p] + T_c + T_p} \Rightarrow \eta = \frac{\text{Transmission delay}}{[(\text{no. of contention slots}) * 2 * p_d] + T_D + P_D}$$

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 transmission if only one station transmits the data and other stations Refrain = probly for successful trans =

$$P_{\text{success}} = \eta_c p * (1-p)^{n-1}$$

$$P_{\text{success}} = \eta p * (1-p)^{n-1}$$

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

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

2) No. of tries (n) times we should try before getting first success = $1/P_{\text{max}} = e$

$$\eta = \frac{T_c}{C * 2 * T_p + T_c + T_p}$$

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

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

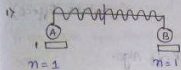
csma/cd
⇒ $\eta \downarrow$ as $d \uparrow$ {NOT SUITABLE FOR WIRELESS}

⇒ $\eta \uparrow$ as $L \uparrow$ {send bigger packet for good efficiency}

8. BACK OFF ALGORITHM FOR CSMA-CD

(15)

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



n = collision Number

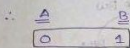
⇒ This Algo says both the stations 'A' and 'B' should randomly choose a no between $(0, 2^n - 1)$

⇒ $(0, 2^1 - 1)$

⇒ $(0, 2^1 - 1)$

⇒ $(0, 1)$

⇒ $(0, 1)$



A's waiting time = $0 * T_{slot} = 0$

B's waiting time = $1 * T_{slot} = T_{slot}$

A' won Backoff race

0

0

collisions

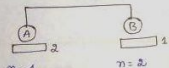
$p(A) = 1/4$

$p(B) = 1/4$

$p(\text{collision}) = 1/2$

Now, Suppose let us Assume 'A' wins the Backoff Race ⇒ 'A' has successfully transmitted its 1st Data packet and

station B is ready with 2nd Data packet



$n = 1$

$n = 2$

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

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

$= (0, 1)$

$= (0, 3)$

$= (0, 1)$

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

A

B

0

0

⇒ collision

1

1

⇒ 'A' win

0

2

⇒ 'A' win

0

3

⇒ 'A' win

1

0

⇒ 'B' win

1

1

⇒ collision

1

2

⇒ 'A' win

1

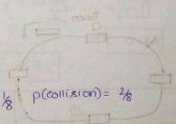
3

⇒ 'A' win

$p(A) = 5/8$

$p(B) = 1/8$

$p(\text{collision}) = 3/8$



$$\Rightarrow \text{Waiting Time} = K \times T_{slot}$$

$K \in (0, 2^n - 1)$ $n = \text{collision number}$

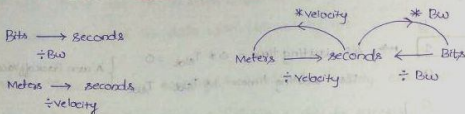
$\Rightarrow$ collision probability is decreasing exponentially.

$\Rightarrow$ If 'A' has won first collision the prob that it wins 2nd collision is High (capture Effect)

$\Rightarrow$ Applicable only for 2 stations.

$\Rightarrow$ Binary Backoff Algo or Binary exponential Back-off Algo.

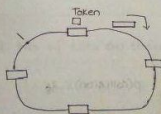
9. TOKEN PASSING ACCESS CONTROL METHOD



How many meters 10bits Equivalent to, given that $Bw = 4 \text{ Mbps}$, $v = 2 \times 10^8 \text{ m/s}$

$$\begin{aligned} \text{Sol: } \text{Bits} &= 10 \text{ bits} \\ \frac{\text{Bits}}{Bw} &= \frac{10}{4} = \frac{2.5 \text{ sec}}{10^6} \times 2 \times 10^8 \text{ m/s} \\ &= \frac{5 \times 10^8 \text{ m}}{10^6} \end{aligned}$$

$$\text{Ans} = 500 \text{ m}$$



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":

$$\text{Ring latency} = \left(\frac{d}{v} \right) + (N \times b)$$

sec Bits

$\left\{ \begin{array}{l} d = \text{length of Ring} \\ v = \text{Velocity} \end{array} \right.$

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

seconds (sec)

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

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

(11)

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

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

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

- 1) Delayed Token Reinsertion $\Rightarrow THT = T_e + T_p \Rightarrow \eta = \frac{1}{1 + \frac{(N+1)}{N} a}$ ($a = T_p / T_e$)
- 2) Early token Reinsertion $\Rightarrow THT = T_e \Rightarrow \eta = \frac{1}{1 + (a/N)}$

10. ALOHA AND DIFFERENCES BETWEEN FLOW AND ACCESS CONTROL

- 1) Any station could transmit data at any time - No carrier sensing.
- 2) collisions are possible, Acknowledgements are there $\Rightarrow$ Collision detection X
- 3) Retransmissions $\checkmark$ after some time (Backoff time)

ALOHA $\begin{cases} \text{pure Aloha} \\ \text{Slotted Aloha} \end{cases}$

pure Aloha

- 1) Vulnerable time = $2T_e$

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

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

$$\text{If } G = \frac{1}{2} \quad \eta = \text{max}$$

$$\Rightarrow \eta_{\text{max}} = \frac{1}{2} * e^{-1}$$

$$= \eta_{\text{max}} = 0.184$$

$$= \eta_{\text{max}} = 18.4\%$$

Slotted Aloha

- 1) Vulnerable time = T_e

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

$$\Rightarrow \eta = 0.368$$

$$\eta_{\text{max}} = 36.8\%$$

FC

$$SAW = \frac{1}{(1+2a)} \quad \text{resp. } \frac{N}{(1+2a)}$$

$$GRN = \frac{N}{(1+2a)}$$

$$SR = \frac{N}{(1+2a)}$$

AC

$$TDM = \frac{1}{1+a} \quad \text{polling: } \frac{T_e}{T_e + T_{poll}}$$

$$CSMA/CD = \frac{1}{1+6*4*a}$$

$$\text{Aloha} \begin{cases} \text{Pure } G * e^{-2G} = 18.4\% \\ \text{Slotted } G * e^{-G} = 36.8\% \end{cases}$$

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, etc.

→ Error Correction → Hamming code {not used in CS}

CRC (CYCLIC REDUNDANCY CHECK)

⇒ CRC is mainly used at Hardware Level

Sender

CRC_G

Receiver

1011011

1101

⇒ If CRC Generator is 'n' bits we

are going to append (n-1) bits (All 0s)

Appended 0's

to the data.

Appended data = 1011011000

⇒ ⊕ = Exclusive OR @ modulo 2 sum

$$\begin{array}{l} 1 \oplus 1 = 0 \\ 0 \oplus 0 = 0 \\ 1 \oplus 0 = 1 \\ 0 \oplus 1 = 1 \end{array}$$

Now, 1101 1011011000 (⇒ If CRC_G = n bits then CRC = n-1 bits)

$$\begin{array}{r} 1101 \\ 0110011000 \\ \hline 0110011000 \\ 000111000 \\ \hline 011101 \\ 001100 \\ \hline 1101 \\ 0001 \\ \hline 0001 \end{array}$$

⇒ 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 beginning will be replaced by CRC and gets transmitted.

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

$$= 1011011001 \\ \text{AD} \quad \text{CRC}$$

At Receiver side, whether the data that is transmitted is Right or wrong

$$\begin{array}{r}
 1011011001 \quad (1011011001) \\
 \underline{1101} \\
 0110011001 \\
 \underline{1101} \\
 000111001 \\
 \underline{1101} \\
 001101 \\
 \underline{1101} \\
 0000 \\
 = CRC
 \end{array}$$

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

2. CRC EXAMPLE

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

If the degree of the polynomial = 3 the no. of bits in CRC Generator are 4 and we append '3' as $\therefore$ Degree of the CRC polynomial = size of CRC generated.

At sender

Data: 11010

CRC: $x^3 + x + 1 = 1011$

$\therefore$ Appended data = 11010000

At Receiver side

$$\begin{array}{r}
 1011 \quad 11010000 \quad (1011) \quad 11010010 \quad (1011) \\
 \underline{1011} \\
 01100000 \\
 \underline{1011} \\
 0111000 \\
 \underline{1011} \\
 010100 \\
 \underline{1011} \\
 00010 \\
 \underline{1011} \\
 00000 \\
 = CRC = 010
 \end{array}$$

CRC = 010

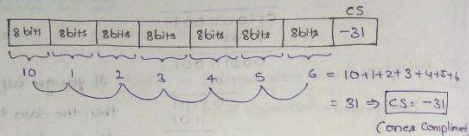
$00000 = 11010 \checkmark$

3. CHECKSUM

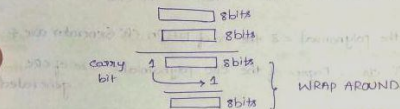
$\Rightarrow$ Tcp, Ip, Udp uses 16 bit checksum, and checksum is used at Software level.

$\Rightarrow$ 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.

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



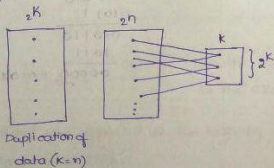
⇒ Suppose if I add two 8 bit no's in the above checksum then I may get a 9 digit Binary number then you take the LSB and add it to the obtained number, This is called 'wrap Around'.



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.

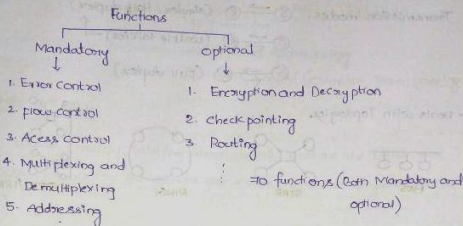


8. CHECKSUM

4. ISO/OSI STACK

(19)

1. ISO-OSI LAYERS



⇒ 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 | } | Various Reference models |
| 2) TCP/IP | | |
| 3) ATM | | |
| 4) X.25 | | |
| 5) IEEE (Mainly deals with LAN Technologies) | | |

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

⇒ The various layers in the OSI model are:

- | | |
|---------------|--------------------------|
| Users | ← 1 → Application layer |
| Interactivity | ← 2 → Presentation layer |
| | ← 3 → Session layer |
| Thick layer | ← 4 → Transport layer |
| Complex | ← 5 → Network layer |
| Both HW/SW | ← 6 → Data Link layer |
| HW | ← 7 → Physical layer |

- 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 }

2. PHYSICAL LAYER

⇒ physical layer deals with Electrical, Mechanical, Functional, procedural characteristics of physical links.

⇒ Transmission modes: $\text{S} \rightarrow \text{R}$ (simplex/half duplex)

$\text{S} \rightleftharpoons \text{R}$ (walkie talkies)

$\text{S} \rightleftharpoons \text{R}$ (full duplex)

⇒ Deals with Topologies.



BUS



STAR



RING



HYBRID/TREE



MESH

⇒ Deals with Encoding (Bits $\rightarrow$ Signals, waves) 1010

MANCHESTER ENCODING

1 - Represented by

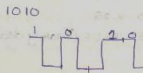
0 - Represented by



DIFFERENTIAL MANCHESTER ENCODING

0 - Represented by

1 - Represented by



In both the Encodings (Manchester and Differential manchester)

$$\boxed{\text{Baud Rate} = 2 * \text{Bit rate}}$$

{ 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

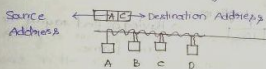
4) physical Addressing

5) Access control (CSMA/CD, Token passing...)

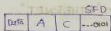
4. FRAMING AT DLL

At DLL we are mainly talking about LANs and all the LANs are multi-access 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 beginning so it has a special field called "SFD" (Starting Frame Delimiter)



Now, SFD represents that the frame is coming 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

$(101010 \dots 11)(0+1)^*$

SFD The data that is present

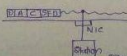
Now we can convert

Regular Expression $\rightarrow$ DFA $\rightarrow$ Sequential Circuit

(Built using flipflops)

Now, this sequential circuit has the capability of Recognising the Bits/RE

ie $(101010 \dots 11)(0+1)^*$ so,



At this point the sequential circuit alerts the station and say that a frame is going. If it is false

⇒ 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: $L = 1000 \text{ Bytes}$ ⇒ The min and max amount of data that can be

sent is 1000 Bytes, if i have to send 1008

$1008 + 900 \text{ Bytes}$

then??

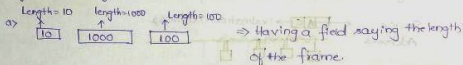
Dummy bits

Added [This procedure is called padding].

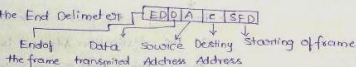
⇒ To identify the ending of frame there are two methods they are,

1. Having a field saying the Length of the frame

2. Having an Ending Delimiter



b) Having the End Delimiter

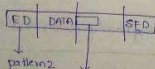


⇒ Fixed Length frames are used in "ETHERNET."

⇒ 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 delimiter is if ED pattern matches with Data (part) then the receiver cannot scan the entire data available



if $p_1 = p_2$ then Receiver scans only a part of data

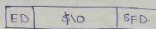
⇒ End Delimiter can be dealt in 2 ways they are : character stuffing
Bit stuffing.

CHARACTER STUFFING



⇒ OBSOLETE TECHNOLOGY

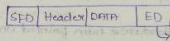
⇒ so, add a null character after \$ so that the Receiver thinks 'sees a \0' followed by a 'f' then it assumes it is not the end of data and it discards the Null character and scans the entire data.



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

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

BIT STUFFING (V. Imp for GATE)



Sender

D: 01111

↓

D: 011101

D: 011101

Receiver

01111

↑

011101

011101

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

If ED = 01111

Sender side

D: 011110

SD: 0111100 (After four ones add a zero)

D: 01111

SD: 0111101

Receiver side

D: 0111100

01110

SD: Stuffed Data

ED = 01111

D = 0111 000 11110

} Now, what is the data after Bit stuffing?

Sol Data = 0111 000 11110

Stuffed Data = 0111 0 000 111010

⇒ ED = 0111111

Data ⇒ At the sender, after the Run of 6 ones im going to add zero
= 01111101

⇒ 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 Addresses { 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.

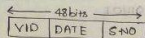
IP Address = 32bit Number, software num.

MAC Address = 48bit Number, hardware num pointed on own "NIC" → RAM → MAC

The MAC Address is divided into three parts (unequal lengths) - they are

1. The Manufacturer ID or Vendor ID
2. What is the date of manufacturing
3. Serial No. of the device on that day

UNIQUE GLOBALLY



⇒ Conceptually Both IP, MAC Addresses can be logical but only IP Address 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

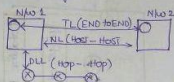
→ LLC takes care of Error control, flow control, (2)

→ MAC takes care of framing, Access control, Error control, physical Address

L-6: INTRODUCTION TO NETWORK LAYER

The main Responsibilities of Network layer is

- 1) Host to Host Connectivity
- 2) Logical Addressing
- 3) Switching (Connecting various Networks together)



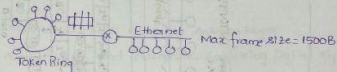
- 4) Routing



⇒ Building the Routing table = Routing
⇒ Using the Routing table = Switching

- 5) Congestion Control

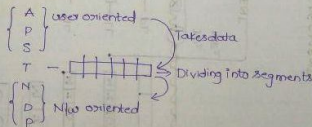
- 6) Fragmentation



7. TRANSPORT LAYER

The main Responsibilities are

- 1) End to End communication using port numbers (port no.s 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

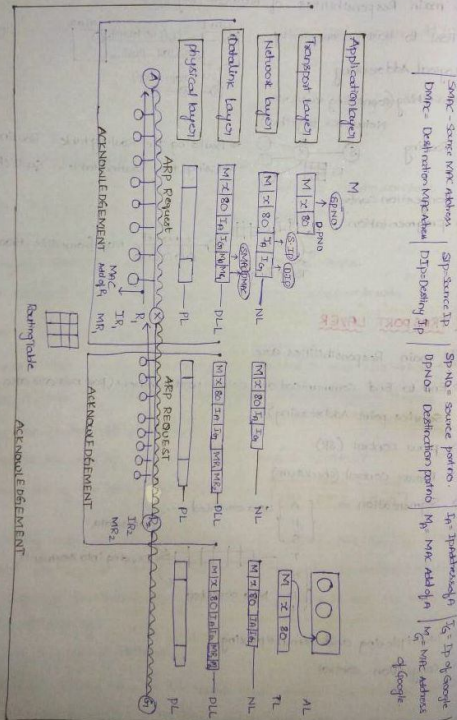
⇒ The protocol used to convert IP address to MAC address is 'ARP'.

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

⇒ In general the physical layer and datalink layer are present on NIC and

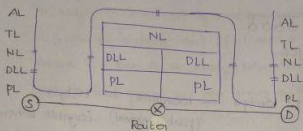
Network layer is present in the operating system.

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



Imp points for Gate

→ Router 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

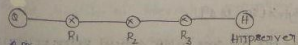
SESSION LAYER

- 1) passwords and usernames will be dealt by session layer
- 2) Main Responsibility Authorization and Authentication (using Digital signatures)
- 3) check pointing (Torrent2 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



A	m
P	m
S	C
T	C X 80
N	C X 80 10 10
D	C X 80 10 10 10 10 10 10 10
P	

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

5. LAN-TECHNOLOGIES

ETHERNET (IEEE 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

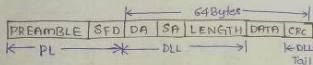
TL = Segment

NL = Datagram

DLL = Frame

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

FRAME FORMAT OF ETHERNET (OR) IEEE 802.3 FRAME FORMAT



PREAMBLE: 7 bytes: 10 10 10 10 10 ---- 10

SFD: [Start frame Delimiter]: 1 Byte: 10 10 10 11

DA: 6 Bytes } MAC Address

SA: 6 Bytes }

CRC: 4 Bytes

TYPES OF MAC ADDRESS

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

1. UNICAST MAC ADDRESS: [LSB of 1st byte is 0] 00010101:00101011

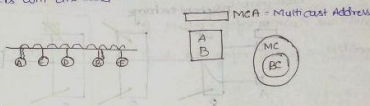
2. MULTICAST MAC ADDRESS: [1st Byte's LSB is 1]

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 multi cast 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 : 2 Bytes = 16 bits

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

: In CSMA/CD : $L \geq 2 * T_p * B_w$ substituting the standard values of T_p and B_w for Ethernet we get
 $L \geq 64$ Bytes

: Max Length : 1500 Bytes

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

DISADVANTAGES

- 1) Not applicable to Realtime Applications
- 2) Not applicable to Interactive Applications [chatting].
- 3) No priorities so not suitable for client server Applications.

∴ PREABLE = 7B

LENGTH = 2B

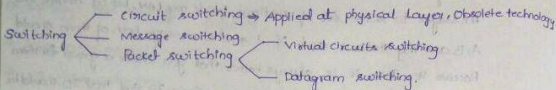
SF B = 1B

CR = 4B

SA = DA = 6B

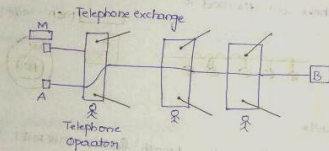
6. SWITCHING

1. INTRODUCTION TO SWITCHING



⇒ Switching is done at Network layer

2. COMPARISON 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

$$= \text{Setup time (connection establishment time)} + T_c + \frac{Xd}{v}$$

$$= \text{Setup time} + \frac{M}{B} + \frac{Xd}{v} + TD \left\{ \begin{array}{l} \text{Tp b/w two hops} = d/v \\ \text{In b/w x hops} = x \cdot d/v \end{array} \right.$$

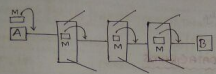
→ Towards the link

$$TT = \text{Setup time} + \frac{M}{B} + \frac{Xd}{v} + TD$$

In the above scenario headers are not Required.
 ⇒ Inorder ✓ (No Reordering of packets) ⇒ NO sequence no. are Required.

PACKET SWITCHING

⇒ Multiplexers are used.



⇒ store and forward N/w.

$$\text{Total time} = x \frac{M}{B} + x \frac{d}{v}$$

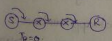
No setup and Teardown time in P.S.

CS	PS
Setup time + Teardown time	$(x-1) \frac{M}{B}$

for Bursty data.
 if $M \cdot B \neq 1$ = go for circuit switching
 if $M = 1$ = go for packet switching

3. PACKETIZATION AND PACKET SWITCHING

Data = 1000 Bytes
 Bw = 1 Mbps = 10^6 Bps
 Header = 100 Bytes
 No of packets = 2
 packet size = $\frac{1000}{2} + \text{Header}$
 $= 1000 + 100$
 $= 1100 \text{ B}$

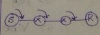


$$T_L = \frac{1}{B} = \frac{1100}{10^6} = 1.1 \text{ msec}$$

$$T_T = 3 \cdot T_L = 3.3 \text{ msec}$$

$$T_T = 3.3 \text{ ms}$$

Data = 1000 Bytes
 Bw = 1 Mbps = 10^6 Bps
 Header = 100 Bytes
 No of packets = 5
 packet size = $\frac{1000}{5} + 100$
 $PS = 300$

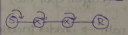


$$1st \text{ packet} = 3 \cdot T_L = 3 \cdot \frac{300}{10^6} = 0.9 \text{ ms}$$

$$\text{Remaining 4 packets} = 4 \cdot T_L = 4 \times 0.9 = 3.6 \text{ ms}$$

$$T_T = 3.6 \text{ ms}$$

Data = 1000 Bytes
 Bw = 10^6 Bps = 1 Mbps
 Header = 100 Bytes
 No of packets = 10
 Each packet size = $\frac{1000}{10} + 100$
 $PS = 200$



$$1st \text{ packet} = 3 \cdot T_L = 3 \cdot \frac{200}{10^6} = 0.6 \text{ ms}$$

$$\text{Remaining 9 packets} = 9 \cdot \frac{200}{10^6} = 1.8 \text{ ms}$$

$$T_T = 2.4 \text{ ms}$$

$$x \frac{d}{v}$$

$$= d/v$$

$$= x \cdot d/v$$

$$= x \cdot d/v$$

Ethernet

IPv4 Header

Top Header

Time

Basic

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 too small if it is the case the total time taken to transmit the data will increase, so the packet size must be chosen appropriately.

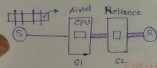
4. VIRTUAL CIRCUITS AND DATAGRAMS

There are two types of packet switching they are Virtual circuits, Datagram.

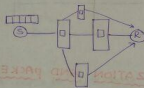
⇒ Our phone call is going through Virtual circuit.

⇒ Our data usage is going through Datagram circuit.

Virtual circuit



Datagram 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 → Smaller packets
- 5) Highly Reliable
- 6) Costly
- 7) ATM (Asynchronous Transfer Mode) Network uses ATM VC.

- 1) Headers are Req for all packets
- 2) Connectionless oriented
- 3) No Guarantee, they may follow diff. path, they may appear out of order.
- 4) Not Reliable
- 5) Not very costly.
- 6) Video, whatsapp call have VoIP (Voice Over Internet Protocol)
- 7) IP Network uses datagram

INTRODUCTION

IPv4 Header

Version (4)
Ident (16)
TTL (8)

HL:

there are min. 4 parts of 4, so we use the 4 parts of 4.

VERSION: The

if version is appropriately.

IDENTIFICATION

→ Identification out of a host we do fragment number.

7. INTERNET PROTOCOL

1. INTRODUCTION TO IP HEADER

IPv4 Header

Version (4)	HL (4)	Type of service (8)	Total Length (16)	32 bits = 4 Bytes
Identification (16)	Flags (3)	Fragment Offset (13)	Header checksum (16)	4 Bytes
TTL (8)	Protocol (8)	Source IP (32)	Destination IP (32)	4 Bytes
Options (0-40) Bytes				4 Bytes
Data				Max Header length = 20 + 40 = 60 B

HL:

Here the min size of the Header is 20B, but the Header Length field HLF is of 4 bits $\therefore$ only the numbers ranging from (0-15) can be represented. So we use the process called scaled arithmetic (divide by 4).

$\therefore$ If Header Length = 20B $\Rightarrow$ HLF contain (5)

HL HLF

20B $\rightarrow$ 5

32B $\rightarrow$ 8

40B $\rightarrow$ 10

$\Rightarrow$ In exam if a number is given and if you want to identify if whether it is a

Header Length or Header length field the process is: Convert to decimal and check

the Ranges (HL (20B-60B))

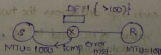
HLF (5-15)

VERSION: The version (of the IP Address IPv4/IPv6). If version = 0100 = IPv4, if version = 0110 $\Rightarrow$ IPv6 $\rightarrow$ the packet must be processed by the routers

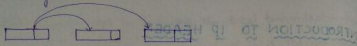
2. IDENTIFICATION, MF, DF AND FRAGMENT OFFSET

$\Rightarrow$ 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.

$\Rightarrow$ DF: Don't fragment



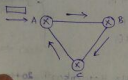
⇒ Fragment offset is no. of data bytes ahead of this particular fragment
In this particular diagram.



3. TTL, PROTOCOL, HEADER CHECKSUM

TTL (8):

consider the following scenario,



⇒ A, B, C are the routers and when a packet goes to router 'A' then the router takes the IP address of the packet and tries to 'AND' with SM if it doesn't match it is going to send to default entry.

⇒ Let us say, Router A's default entry = Router B and Router B's default entry goes/leads the packet go to Router C and Router C's 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 result, the buffers are full, Router 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 infinite loop.

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

Q1: 14 marks

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

Ans: 26



PROTOCOL



⇒ Now consider

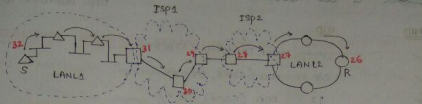
Buffers at +
at their full
Buffers are
It is better
packet is T
is a Reliable
instead of
KMP, TCM
of more
in which the

HEADER CHECKS

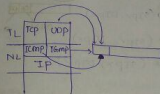


Fragment

Ans: 26

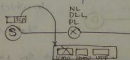


PROTOCOL



protocol 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 whose 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, don't 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):

Header $\Rightarrow$ 16Bit $\Rightarrow$ 16Bit checksum $\Rightarrow$ The Header is divided into no. of parts each of size = 4Bytes = 16 Bits



Header checksum (Initially Zero)



1) FO, MF, TTL

2) Options

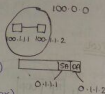
SOURCE IP AND DESTINATION IP

SIP = Source Ip add.
DIP = Destination Ip Add.

NID

UID

- ✓ - Valid IpAddress (SIPx, DIPx)
- ✓ 0's = NID (SIPx, DIPx)
- ✓ 1's = DBA (SIPx, DIPx)
- 1's = LBA (SIPx, DIPx)
- 1's = SM or NM (SIPx, DIPx)
- 0's ✓ = Host within a N/w (SIPx, DIPx)
- 0's = I don't have IP (SIPx, DIPx)
- 127 ✓ = loop back Address (SIPx, DIPx)



1. DIFFERENCE

MTU = Max. frame

⇒ The next field

: The max. A

Message = A

Segment = TL

datagram = N

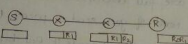
frame = DL

IPDU = PL

5. OPTIONS

⇒ This field is optional

Record Route:



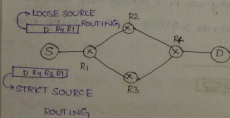
The max. no. of IP Address that could be recorded on a packet is '9'.

⇒ 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 options.

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 Router from which your packet must depart go

⇒ In the diagram, packets go as R1, R2, R3, R4, D.

⇒ In addition padding is also done at 'options' in order to make Header Length: multiple of '2'.

⇒ IP is a protocol the max. size of

⇒ IP we remove payload/headers

⇒ Here we are at each and every 20B

⇒ Now Application now it is the given by the process of

⇒ Now the data is the problem is Ethernet then

8. FRAGMENTATION

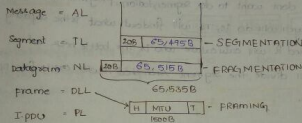
1. DIFFERENCE BETWEEN SEGMENTATION AND FRAGMENTATION

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

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

The max possible number with 16 bits = 2^{16}
= 65,535

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



⇒ IP is a protocol that operates at Network layer. And now, at NL, 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 remaining data is called Payload/data of that layer.

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

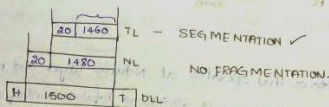
⇒ Now Application Layer could give any amount of data to transport layer. Now it is the responsibility of the Transport layer to divide that packet given by AL into parts so that each part could fit in 65,495B. And the process of dividing the packet into parts is called "Segmentation".

⇒ Now the data from the TL can easily fit into NL but here there is a problem. The problem is DL 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 can 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 process 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, 3FD... and this process is called "FRAMING".

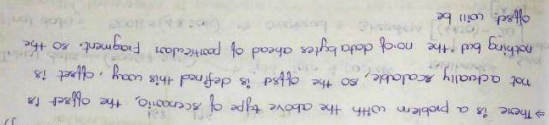
→ The problem here is whether the Network Layer is going to be Bottleneck or DLL is going to be bottleneck. Sometimes DLL can hold the data sent by NL without fragmentation, the Bottleneck will be NL. So at the same host if we don't want to do segmentation, Fragmentation then what transport layer will do is, TL will find out what is the capacity of NL and DLL and it will calculate who is the bottle neck and accordingly TL will divide the segment such that it will easily fit in DLL without any problem.



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

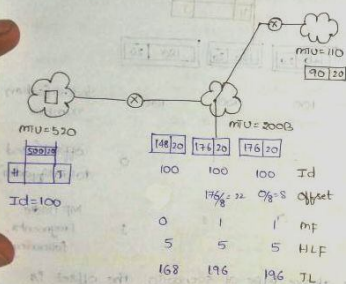
[illegible]

→ Now the problem scenario is, fragment offset = 13 bits → the max no. of offset field = $2^{13} - 1 \approx 8000$

→ The worst case fragment offset in a datagram = $\boxed{20} = 65,535 - 1$
 $\boxed{128} \quad \boxed{65,535} \quad \boxed{128} \quad \boxed{128} = 65,514,368$

Now, At worst case I have to put number = 2^{16} but my fragment offset contains only 13 bits $\Rightarrow 2^{13}$ $\therefore$ scale down factor for offset = 8 $\left[\because \frac{2^{16}}{2^{13}} = 2^3 \right]$

→ $\therefore$ The offset must be divided by 8. But the problem with this is we get decimal points. So in order to avoid floating point numbers we should always see that the datagram in the fragment should be divisible by 8.



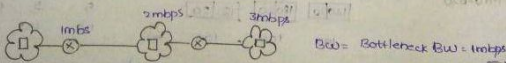
88	20	88	20
100	100	100	100
200	33	22	offset

The offset for the last fragment can be deduced
 → Each fragment's size should be divisible by 8.
 → HLF should be divided with four.

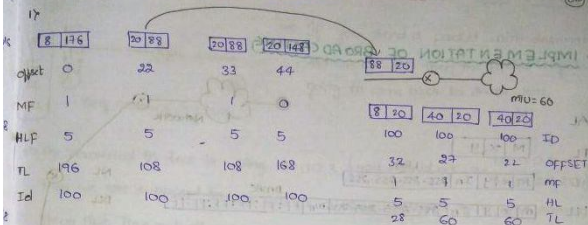
Initial data = (500B + 20B) → Split into 4 packets
 Final data = 500B + (4 * 20B) → Overhead = 3 headers $\left[\frac{(4 * 20) - 20}{8} = 3 * 20 \right]$

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

Bandwidth Utilization/Throughput = $\eta \times Bw = \eta \times 1 \text{ Mbps}$



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	⇒ 1st fragment
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, offset)

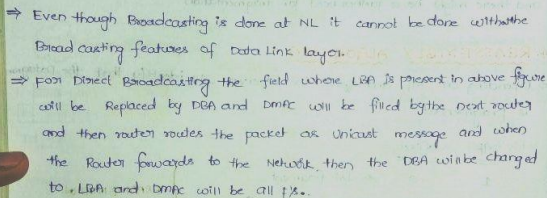
Step-2: Destination should also identify that what fragments belong a particular datagram by using Identification number.

Step-3: Identify the first fragment (MF=1, offset=0) $\uparrow$ $[TL - (HL * 4)] \div 8$

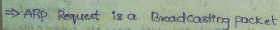
Step-4: Identify the subsequent fragments $[Data \div HL] \div 8$ - offset of 2nd fragment

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

1. IMPLEMENTATION OF BROADCASTING



Arp (IpAddress $\rightarrow$ MAC Address)

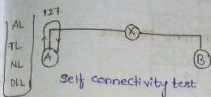


⇒ ARP Reply is a unicast packet

→ ARP is applied when

- Router wants to find MAC Address of another Router (R-R)
- Host wants to find MAC Address of another Host (H-H)
- Router wants to find MAC Address of another Host (R-H)
- Host wants to find MAC Address of another Router (H-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.

PL

⇒ 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 $\approx 15ms$. 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 $\rightarrow$ IP)

NFS = Network File Server.

MAC $\rightarrow$ ROM

IP $\rightarrow$ Ram



1) The disadvantages of RARP are:

a) Every NLS should have a RARP server.

OBSELETE TECHNOLOGY

b) Static mapping (eg: IP > no. of Hosts)

AL

TL

NL

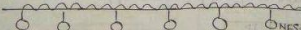
DLL

M

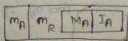
RARP Request

MAC 00:00:00:00:00:00

MAC 00:00:00:00:00:00 FF:FF:FF:FF:FF:FF

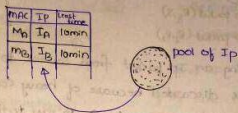


RARP Server



MAC	IP
M1	I1
M2	I2
Mn	In

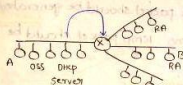
⇒ Let us say, A host M_A wants its Ip Address then the Dynamic pool look like this



⇒ only one DHCP server is Enough

⇒ The Table is a Dynamic table (No. of Ip Address = No. of stations online)

⇒ To make DHCP backward compatible 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

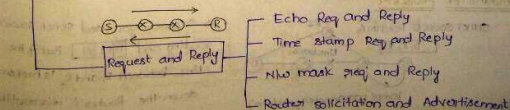
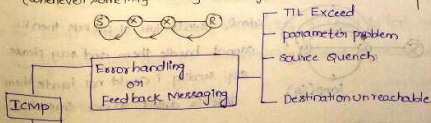
⇒ But practically DHCP can be applied on the routers also, if you buy Cisco's **IOSRSE** router you are going to be provided with DHCP facility at Router itself.

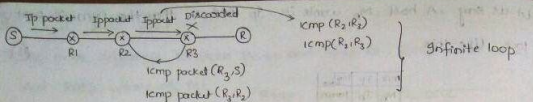
6. INTRODUCTION TO ICMP (v Imp for GATE)

⇒ ICMP works at Network Layer

⇒ ICMP = Internet Control message protocol

(Whenever something is wrong then we get icmp packet)





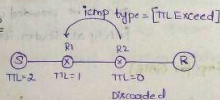
⇒ Suppose you are sending an IP packet from source to receiver but on the way the IP packet is discarded because of heavy congestion at Router R_3 . Now the Router R_3 sends ICMP packet (R_3/S) to say to the source that I discarded your packet. Now the Router R_3 sends "ICMP (R_3/S)" first to Router R_2 but because of heavy congestion at R_2 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.

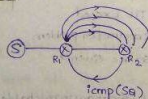
∴ ICMP + IP UNRELIABLE

7. ICMP FEEDBACK MESSAGING

TTL EXCEED



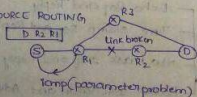
SOURCE QUENCH



When R_1 sends lots of packets then R_2 cannot handle them and say please stop sending I could not handle them. This is called Source Quench.

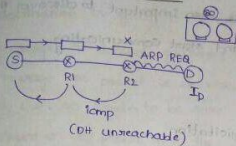
PARAMETER PROBLEM

STRICT SOURCE ROUTING



⇒ Suppose you used Strict Source routing and $[D, R_2, R_1]$ But if the link between R_1 and R_2 is broken then the Router R_1 discards the packet and sends ICMP message.

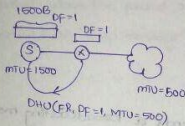
DESTINATION UNREACHABLE



⇒ Destination unreachable is of 2 types they are

1. Destination Host unreachable
2. Destination port unreachable

⇒ R2 send ARP Req. for getting mac add. if the host is down then there won't be reply then the Router R2 sends icmp DH unreachable error message).

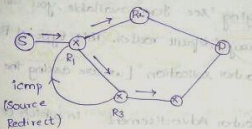


DH = Destination Host unreachable

DF = Don't fragment = 1

FR = Fragmentation Required.

SOURCE REDIRECT



⇒ Now source sends a packet to

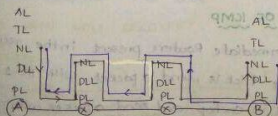
R₁ and at R₁ due to some errors in the routing table if it has chosen Router R₃ (actually the best path is "R₁ R₃ D") then

if there is some manual mechanism in R₃ which knows that there is a better path b/w S and D then R₃ sends icmp packet saying "see there is another better path so you please redirect don't send 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.

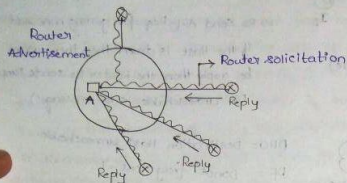
PING: PACKET INTERNET GOFER



AL TL NL PL ⇒ 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 Router 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 solicitation" [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 use me as your default router."

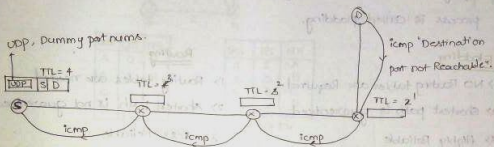
Time Stamp Req and Reply

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, in order to that there is a special type of icmp message called "Time Stamp Req and Reply" message. This is a obsolete technology and now we are using "Network time protocol".

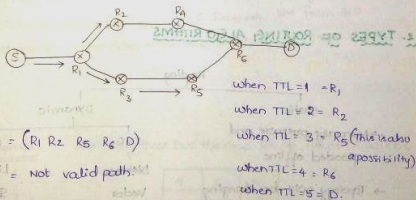
9. TRACEROUTE APPLICATION OF ICMP

⇒ In order to find the intermediate Routers present in the route between source and destination the trick is, send a packet with TTL=1 in order 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 / sender.

$\Rightarrow$ 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 doesn't guarantee that when we don't receive a icmp message the packet is delivered to the destination, the icmp may be lost. so should 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".

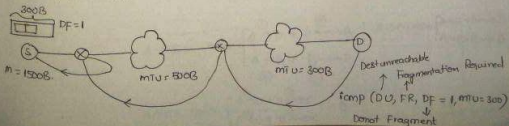


$\Rightarrow$ The Trace route might not give you the actual path, but in almost majority cases we get actual path. for example,



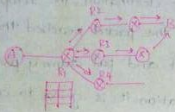
10. PMTDU APPLICATION OF ICMP

PMTDU = PATH MTU DISCOVERY



10. ROUTING

1. DIFFERENCE BETWEEN ROUTING AND FLOODING



⇒ How does the Router R1 come to know about the destination, i.e., 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 don't know which way to send, send it in all possible paths, this process is called flooding.

Flooding

- 1> NO Routing tables are Required
- 2> Shortest path is guaranteed.
- 3> Highly Reliable

Disadv

- 1> More Traffic
- 2> Duplicate packets are possible

Routing

- 1> Routing tables are needed
- 2> Shortest path is not guaranteed
- 3> Less Reliable

Adv

- 1> Less Traffic
- 2> NO Duplicate packets.

2. TYPES OF ROUTING ALGORITHMS



3. DISTANCE VECTOR ROUTING

(35)

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

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

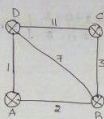
Step 1

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

→ DV

Des	Dfs	NH
A	∞	-
B	3	B
C	0	C
D	11	D

→ DV



⇒ Building Local Routing table with knowledge of Neighbours.

Des	Dfs	NH
A	0	A
B	2	B
C	∞	-
D	1	D

→ Distance vector

Des	Dfs	NH
A	2	A
B	0	B
C	7	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 receives DV from A/B/C.

At A:

DVs from B/D

From B

- 2
- 0
- 3
- 7

From D

1	2	A
7		
11		
0		

⇒ Using these two the new DV of Router A will be

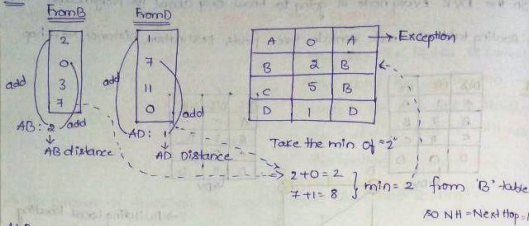
A	0	A
B	2	B
C	5	B
D	1	D

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

$$A \rightarrow C = \min \begin{cases} A \xrightarrow{1} D + D \xrightarrow{3} C \\ A \rightarrow B + B \xrightarrow{2} C \end{cases} = 5$$

The shortcut is

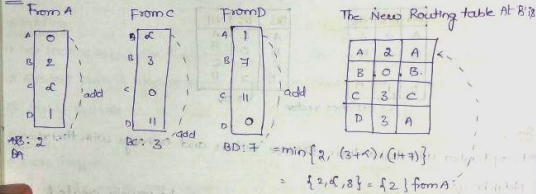
At A:



At B:

Divs 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

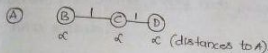
After the Routing table converges the edges that are unused is $D \rightarrow C$, $D \rightarrow B$.

(36)

4. COUNT TO INFINITY

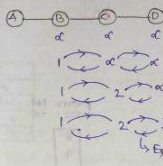
There is a problem with DVR the problem is called count to infinity.

Initially

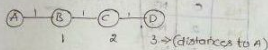


Step-1

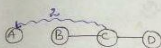
Suppose if 'B' is connected to A



Suppose if Everything is stabilized



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



(Initial values before the link is broken)

$\infty \rightarrow 2 \rightarrow 3$

Dist. from B $\rightarrow A$ via C: $3 \rightarrow 4 \rightarrow 3$ are exchanged in neighbours. Here, B says 'I cannot reach A' but C says 'I'm able to reach A in 2 hops'.

C: $5 \rightarrow 4 \rightarrow 5$

Distances from that node to A: $7 \rightarrow 6 \rightarrow 7$

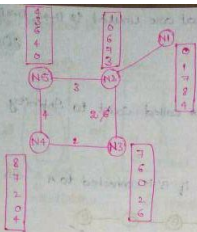
$9 \rightarrow 8 \rightarrow 9$

$9 \rightarrow 10 \rightarrow 9$

∞

$\Rightarrow$ 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 to N_3 and N_2 which is 6, falls down to 2, then what is the distance vector at N_3 (after 1 round of exchange).

At N_3 :

From N_2

1
0
6
7
3

$N_3 N_2: 2$

From N_4

8
7
2
0
4

$N_3 N_4: 2$

New routing table at N_3 is

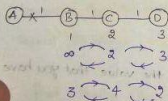
N_1	3	N_2
N_2	2	N_2
N_3	0	N_3
N_4	2	N_4
N_5	5	N_2

Ans: 3 2 0 2 5

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	B	-
1	1	1
1	1	1
1	1	1

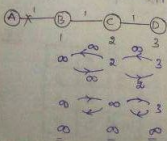
A	2	B
1	1	1
1	1	1
1	1	1

A	3	C
1	1	1
1	1	1
1	1	1

Initially

⇒ This procedure repeats until all the values are stabilized.

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



⇒ Now, At 'C', C is depending on B, in order to get to 'A' ∴ when 'C' is already depending on 'B' to get to 'A' it should not say I can take 2 in some hops, I am already depending on 'B' so please don't do that.

⇒ 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.

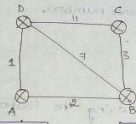
6. LINK STATE ROUTING

⇒ 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	1
B	3
A	1

C	
Seq	
TTL	
D	11
B	3



A	
Seq	
TTL	
B	2
D	1

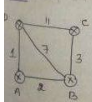
B	
Seq	
TTL	
A	2
D	11
C	3

⇒ In ROUND 2 EVERY NODE IS SUPPOSED TO FLOOD THE INFO TO EVERY OTHER NODE. THEREFORE 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:



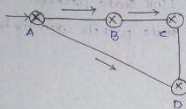
⇒ Then at 'A', 'A' will start applying single source shortest path (Dijkstra Algo) and 'A' comes to know all the shortest path to all nodes and 'A' will construct its Routing table.

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 flooding, it is going to lead heavy traffic.

⇒ Now, consider the following scenario,



⇒ Now if a packet is flooded 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 arrival we may think that the packet which came late is the latest packet and the packet arrived quickly is the old packet. so

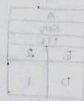
harder to correct that we have sequence numbers.

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

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

Router	Latest
B	1015
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 overcome by having TTL field

1. DIFFERENCE BETWEEN DVR, LSR, RIP AND OSPF

58

DVR

- 1) used in 1980's
- 2) Bw requested 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

LSR

1. used in 1990's
2. High Band width
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

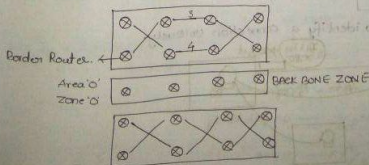
RIP (ROUTING INFORMATION PROTOCOL)

- ⇒ Rip is the implementation of (DVR) Simple to Implement
- ⇒ Metric = Hopcount (weights)
- ⇒ Infinity cannot be represented in programming 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 flooding is Restricted to that Region, and there will be one router designated as "Border Router" (It will take all the flooded 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

4 bits	SOURCE PORT (16)	DESTINATION PORT (16)	= 4 Bytes
	SEQUENCE NUMBER (32)		= 4 Bytes
	ACKNOWLEDGE NUMBER (32)		= 4 Bytes
	WINDOW SIZE (16)		= 4 Bytes
	ADV. WINDOW (16)		= 4 Bytes
	CHECK SUM (16)	URGENT POINTER	= 4 Bytes
	OPTIONS (0-40) Bytes		= 40 Bytes
	DATA		

∴ 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 $(2^{16}-1)$] ports can be represented

= (0, 65,535)

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

0
1023 } well known services
port number

1024
49,151 } Reserved

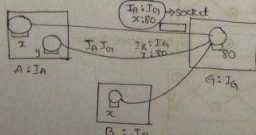
49,152
65,535 } General public

⇒ open your browser and type "Netstat" to see all the connections, and port numbers (source port number, destination port number)

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

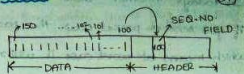
⇒ $\text{Socket} = \text{Ip} + \text{portnum} = 32 + 16 = 48 \text{ bits}$

⇒ sockets are used to identify a connection uniquely.



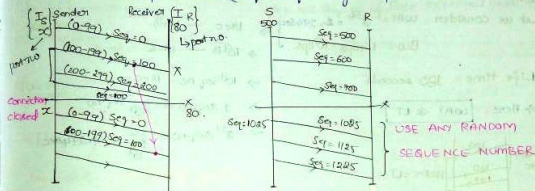
3. SEQ. NO., ACK NO., RANDOM INITIAL SEQ. NO.

- ⇒ 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)



4. WRAP AROUND TIME AND PROBLEMS ON WRAP AROUND TIME

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

WAT

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

⇒ Seq. No's field contain 32 bits $\Rightarrow 2^{32}$ Seq. no's are possible

⇒ Now, Let us say Bandwidth = 1 MBps

$$\Rightarrow 1 \text{ sec} = 1 \text{ MB}$$

$$\text{WAT of 'n' Seq. no's} = \frac{n}{\text{Bandwidth}} \Rightarrow \frac{10^6 \text{ B}}{1 \text{ MBps}} = 1 \text{ sec}$$

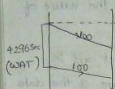
$$\Rightarrow 10^6 \text{ Seq. no's} = 1 \text{ sec}$$

$$\Rightarrow 1 \text{ Seq. no} = \frac{1}{10^6} \text{ sec}$$

$$\Rightarrow 2^{32} \text{ Seq. no} = \frac{2^{32}}{10^6} \text{ sec} = 4294.967296 \text{ sec}$$

→ 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 (3min) which means at worst case it will reach after 3 minutes after you send it.

$$LT = 3\text{min} = 180\text{sec}$$



→ As long as $WAT > LT$, there is no problem

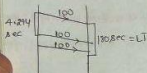
II.

$$\text{Let us consider } WAT = 2^{32} = 4.294\text{sec} \Rightarrow 1\text{sec} - 1\text{GB}$$

$$Bw = 1\text{GBps} = 10^9\text{bps} \Rightarrow 10^9 - 1\text{sec}$$

Life time = 180 seconds

⇒ Here $WAT \ll LT$



$$\Rightarrow 10^9 \text{seq.no} - 1\text{sec}$$

$$\Rightarrow 1\text{seq.no} - \frac{1}{10^9} \text{seq.no}$$

$$\Rightarrow 2^{32} \text{seq.no} - \frac{2^{32}}{10^9} = 4.294\text{sec}$$

Now, to solve the above problem, the possible solution is Decreasing the Bandwidth, but this is not possible because we are interested in having high Bandwidth (The speed at which the data gets transferred) so the other possible solution is Increasing the sequence no. field.

$WAT > LT \Rightarrow$ No problem

$WAT < LT \Rightarrow$ problem $\Rightarrow$ so calculate how many seq.no.s are transmitted in 180sec

$$\Rightarrow 1\text{sec} - 1\text{GB}$$

$$\Rightarrow 1\text{sec} - 10^9 \text{seq.no.s}$$

$$\Rightarrow 180\text{sec} \rightarrow 180 \times (10^9 \text{seq.no.s})$$

2. The min seq.no.s required to avoid wraparound within Life time

$$= 180 \times 10^9 \text{seq.no}$$

$$\therefore \text{The No. of bits in seq.no. field is } = \lceil \log_2 (180 \times 10^9) \rceil = 42$$

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

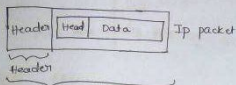
[These 10 bits are used in option and called as Time stamp]

⇒ The no. of bits in the sequence no. field such that there won't be any problem with WAT and LT, given at bandwidth, BW is $\lceil \log_2(LT \cdot BW) \rceil$

5. HEADER LENGTH AND CALCULATION OF ACKNOWLEDGMENT 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. $\left\{ \frac{\text{max size of header}}{\text{largest no. by 4 bits}} = \text{scale factor} \right\}$



SEQ NO: Seq. no of 1 Byte

ACK NO: Seq. no of Byte expected next.

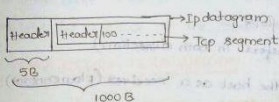
PROBLEM

TL = 1000B } for Ip Datagram
HLF = 5

HLF = 5 } for Tcp
Seq no of Tcp segment = 1000B } Segment

then what is the seq. number of the next byte expected?

Sol: Tcp segment will be in the Ip Datagram



⇒ Now, the data part in the

Ip datagram = $1000 - (5 \times 4)$
= 980B

⇒ 980B = Header + Data (in Tcp)

⇒ 980 - (5 × 4) = Data

⇒ 960B = Data ⇒ Ack = (960 + 1000) + 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 1Bit information, Tcp is connection oriented.

SYN (SYNCHRONIZATION FLAG)

ACK (ACKNOWLEDGEMENT FLAG)

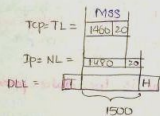
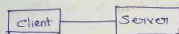
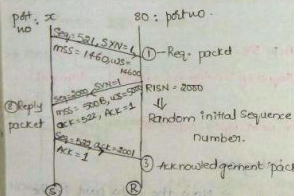
Now, Tcp is connection oriented protocol and it has 3 phases,

1) Connection Establishment

2) Data Transfer

3) Connection Termination.

CONNECTION ESTABLISHMENT



⇒ 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 NOS

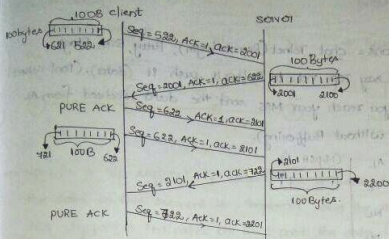
⇒ "FIN" = 1 TAKE '1' SEQ NOS

⇒ 1 DATA BYTE TAKES '1' SEQ NOS.

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

7: TCP DATA TRANSFER AFTER CONNECTION ESTABLISHMENT

(41)



SYN

ACK

- 1 0 $\Rightarrow$ 1st packet = 1st Segment = Request segment
- 1 1 $\Rightarrow$ 2nd Segment = Reply segment
- 0 1 $\Rightarrow$ pure Acknowledgement (ACK flag present in the header)
- 0 0 $\Rightarrow$ (Not possible)

$\Rightarrow$ sender is not going to send Acknowledgements immediately, he is going to wait for some time

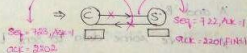
$\Rightarrow$ The Receiver also waits for some time before transmitting the data.

$\Rightarrow$ 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

Client Server

$\Rightarrow$ FIN = FINISH FLAG (used to terminate the connection)



$\Rightarrow$ After client sending FIN packet the events that are possible and not possible are

- $\Rightarrow$ Data C $\rightarrow$ S X
- $\Rightarrow$ Data S $\rightarrow$ C $\checkmark$

- $\Rightarrow$ ACK C $\rightarrow$ S $\checkmark$ (pure ACK)
- $\Rightarrow$ ACK S $\rightarrow$ C (Piggy Backed)

SYN: Synchronising Seq numbers

ACK: Indicate whether Ack num-field is valid/not

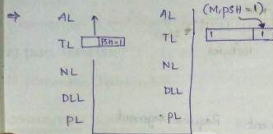
FIN: Request for connection termination.

9. PSH FLAG

PSH = PUSH FLAG

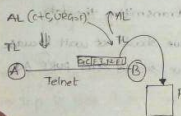
⇒ Interactive Applications = chat, Telnet (Remote Login), Putty, SSH, Rlogin

⇒ PSH is used to say TCP not to Buffer it, push it (data). (Don't 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 send 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 $(Ctrl+C)(C)$ before all the files. [Ctrl+C is used for stopping]

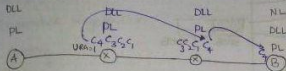
⇒ so urgent flag is used here, which means you have to say that last command is urgent when compared to other things.

⇒ so for $(Ctrl+C)$ send $URG=1$

AL (M)

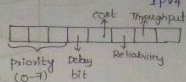
TL (M, URG=1)

NL (M, URG=1, priority=2)

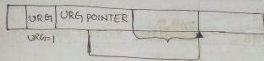


⇒ for urgent packet the priority is set to seven.

⇒ Type of service (8 bits) in IPv4

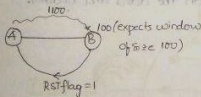
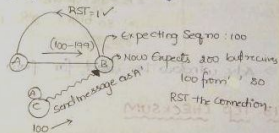
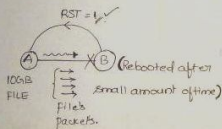


⇒ Now, In a Tcp segment if $URG=1$ then it indicates that some part of the data in this segment is important and the next one is urgent pointer. this Urg pointer indicates till what part the data is urgent.



11 RST FLAG

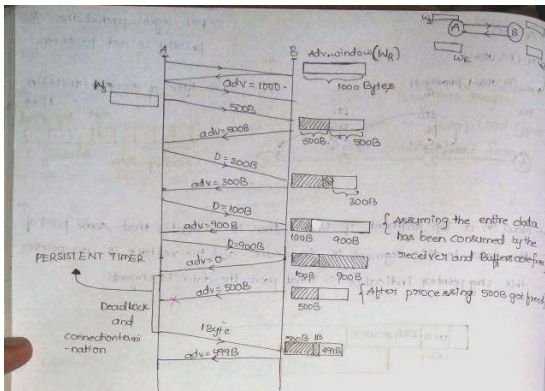
⇒ RESET Flag is used when there is a wrong in the connection. If you see anything unexpected then you are going to use Reset-flag.



⇒ when $RST=1$ it means that, please terminate the connection, i must 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.



⇒ The window size is 16kbits ⇒ Max no. of seq. = 65,535

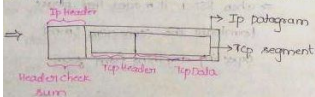
$$\begin{aligned}
 &= 16 + 14 \text{ (options)} \\
 &= 30 \text{ bits} = 2^{30} \text{ 16kbits}
 \end{aligned}$$

⇒ Adv window is used for flow control.

13. TCP CHECKSUM

⇒ Tcp Header has 16-bit checksum.

⇒ In Tcp the checksum is calculated both on the data and header.



⇒ checksum is calculated on, tcpheader, tcpdata, ipheader

PIPH:

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

seudo Ip Header.

Calculate check sum only on the fields in pseudo

Ip Header

Because other

fields will change

when the packet is

received by receiver

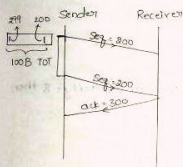
14. OPTIONS IN TCP HEADER

- ▷ Time Stamp ($WAT < LT$)
- ▷ Window size Extension
- ▷ Sack Extension
- ▷ Padding

15. RETRANSMISSIONS IN TCP

- ⇒ TCP uses SR + GBN
 - ⇒ $W_B = W_R$ → Acknowledgements are cumulative
 - ⇒ out of order packets are possible → 25% GBN
 - 75% SR

RETRANSMISSION AFTER TIMEOUT

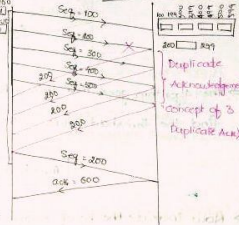


RT AFTER 3 DUPLICATE

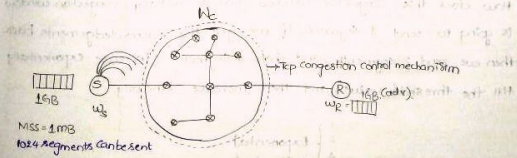


ACKNOWLEDGEMENTS

EARLY RETRANSMISSIONS



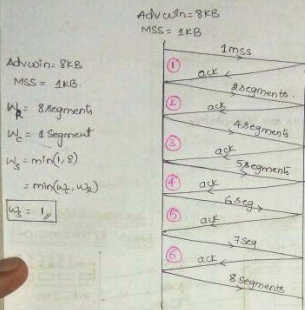
16. INTRODUCTION TO TCP CONGESTION CONTROL



- ⇒ Assume that the Receiver has said that sender can send 16B of data in the Advertising window. ⇒ $W_B = 16B$, $W_R = 16B$
- ⇒ The problem here is even though the Receiver can hold 16B of data the underlying network cannot hold 1024 packets.

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

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



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

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

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.

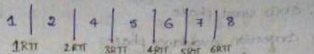
⇒ How does this congestion window grow? Initially congestion window is going to send 1 segment, if we get the acknowledgements back then we send 2 segments, and then 4 segments (increase exponentially till the threshold value) and then increase Linearly.

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

W. Imp

1) AFTER How MANY RTT's ARE WE GOING TO REACH THE MAX SENDER WINDOW SIZE (c)?

Ans 6 Roundtrip times.



2) AN Win = 16KB

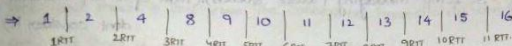
MSS = 1KB

$W_R = 16 \text{ Segments} \Rightarrow \text{Threshold} = 16/2 = 8$

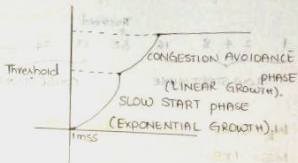
$W_L = 1 \text{ Segment}$

AFTER HOW MANY RTT's WILL WE REACH

TOTAL CAPACITY?



$\Rightarrow 11 \text{ RTT's}$



SS phase = "EXPONENTIAL GROWTH"

CA phase = "LINEAR GROWTH"

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

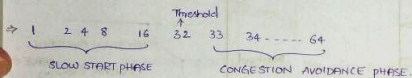
⇒ There are 3 ways to detect congestion they are

- ✓ 1. Time out (Severe Congestion) ⇒ (SS phase)
- ✓ 2. Three Duplicate Acknowledgements (Mild Congestion) ⇒ (CA phase)
- ✓ 3. ICMP Messaging (Source Quench). (Most of the implementations don't consider it)

1) $W_R = 64 \text{ KB}$

$MSS = 1 \text{ KB}$

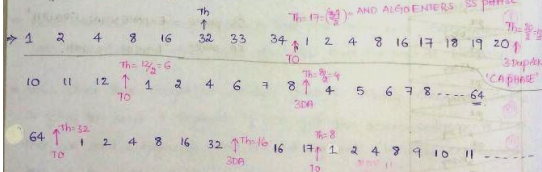
$W_R = 64 \text{ Segments} \Rightarrow Th = 64/2 = 32 \text{ MSS}$



2) $W_R = 64 \text{ KB}$

$MSS = 1 \text{ KB}$

$W_R = 64 \text{ MSS} \Rightarrow Th = 32 \text{ MSS}$



GATE

consider an instance of TCP Additive Increase Multiplicative decrease

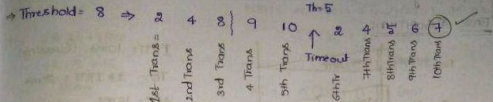
(AIMD) Algorithm where the window size at the start of ssphase is 2 MSS

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

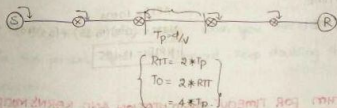
Initial value = 2



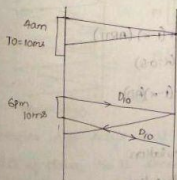
18. TCP TIMER MANAGEMENT

- 1) Time-wait timer $\Rightarrow$ Don't close the connection immediately wait for $3 \times RTT$
- 2) Keep-Alive timer $\Rightarrow$ close All the idle connections
- 3) persistent timer $\Rightarrow$ For finding the capacity of Receiver
- 4) Acknowledgement timer $\Rightarrow$ cumulative Acknowledgement and Piggy Backing
- 5) Time-out timer $\Rightarrow$

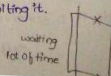
19. INTRODUCTION TO TIME-OUT TIMER



$\Rightarrow$ At Tcp static time out timer cannot be used



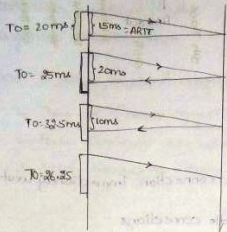
$\Rightarrow$ Initially there is no congestion but after that because of your timeout timer settings it might lead to congestion so have a large timeout timer, but the disadvantage of having large T_o is if a packet is lost you have to wait for a long time before Retransmitting it.



20. BASIC ALGORITHM FOR TOT COMPUTATION

→ The first Algorithm used to set timeout timer dynamically at TCP is

"BASIC ALGORITHM"



IRIT = 10ms (Guessing)

$T_o = 2 * IRIT = 20ms$

ARIT = 16ms

$NRTT = \alpha IRIT + (1-\alpha) ARIT$

$\alpha = \text{Smoothing Factor}$

$0 \leq \alpha \leq 1$

$NRTT = 0.5 * 10 + (0.5) 15$

$NRTT = 12.5ms$

⇒ This Algorithm is Dynamic Nature

⇒ The disadvantage is $T_o = 2 * RTT$

No logic why we are using 2.

For Next packet IRIT = 12.5ms

$T_o = 2 * IRIT = 25ms$

ARIT = 20ms

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

$NRTT = 16.25ms$

For Next packet IRIT = 16.25

$T_o = 32.5ms$

ARIT = 10ms

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

$NRTT = 13.125$

IRIT = INITIAL ROUNDTIME

ARIT = ACTUAL ROUNDTIME

NRTT = NEXT ROUNDTIME

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

→ The Jacobson's Algorithm is used to set the timeout timer.

① Initial Round Trip Time

IRIT = 10ms

$NRTT = \alpha (IRIT) + (1-\alpha) (ARIT)$

ID = 5ms

$ND = \alpha (ID) + (1-\alpha) (AD)$

$T_o = 4 * ID + IRIT$

$= 4 * 5 + 10$

$= 30ms$

$ND = 7.5ms$

ARIT = 20ms

ID = Initial deviation

AD = 10ms (IRIT - ARIT)

AD = deviation

For the 2nd segment that you are sending

$$IRIT = 15ms$$

$$ID = 7.5ms$$

$$TO = 4 * ID + IRIT$$

$$= 4 * 7.5 + 15$$

$$TO = 45ms$$

$$ARTT = 30ms$$

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

$$NRTT = \alpha (IRIT) + (1-\alpha) (ARTT) \quad \{\alpha=0.5\}$$

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

$$= 7.5 + 15 = 22.5ms$$

$$ND = \alpha (ID) + (1-\alpha) (AD)$$

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

$$= 11.25ms$$

For the 3rd segment that you are sending

$$IRIT = 22.5ms$$

$$ID = 11.25ms$$

$$TO = 4 * ID + IRIT$$

$$= 4 * 11.25 + 22.5$$

$$= 67.5$$

$$ARTT = 10ms$$

$$AD = 12.5$$

$$NRTT = \alpha (IRIT) + (1-\alpha) (ARTT) \quad \{\alpha=0.5\}$$

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

$$= 16.25$$

$$ND = \alpha (ID) + (1-\alpha) (AD)$$

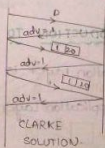
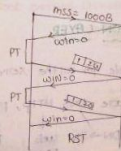
$$= 0.5(11.25) + (0.5)(12.5)$$

$$= 11.875$$

$$TO = 4 * D + RTT = 63.75$$

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

2. SILLY WINDOW SYNDROME



⇒ 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 1ms or half of the buffer.

12. UDP

1. NEED FOR UDP

⇒ Tcp is going to be disadvantageous for some applications they are

1> If Application needs 1 Request and 1 Reply Ex: DNS, BOOTP, DHCP, NTP
(Network Time protocol),

NNP (Network News protocol), "Globe of
day" protocol,

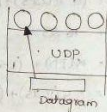
TFTP, RIP, OSPF

2> Broadcast or Multicast

3> fastness rather than Reliability (Multimedia Applications) (onlinemovies)

UDP HEADER

2B	2B
SP (16)	DP (16)
LENGTH (16)	CHECKSUM (16)
2B	2B



⇒ 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

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
↓ ↓ ↓ ↓ ↓
DN → IP web pages files Email
Retrieving

DNS

DNS PORT NO: 53

⇒ 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)

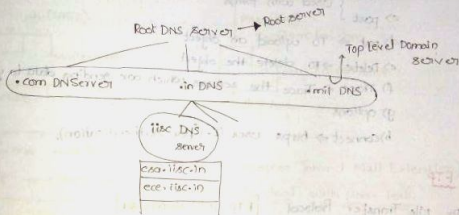
2) Country Domain (.in, .us, .uk...)

3) Inverse Domain (Given IP Address → find Domain Name)

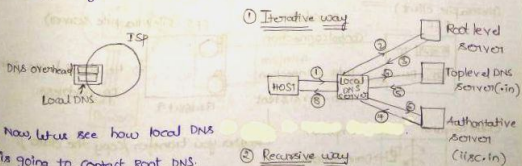
⇒ To find the IP Address of a website type "nslookup www.google.com"

⇒ DNS is also used for Load Balancing

⇒ DNS Database is organised in this way (Distributed Database)

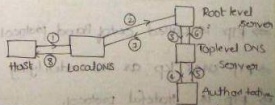


⇒ what if the Root DNS server fails, so IETF (INTERNET ENGINEERING TASK FORCE) made 13 Root servers across the world.



⇒ Now, let us see how local DNS is going to contact Root DNS.

- 1) Iterative way
- 2) Recursive way



3. HTTP

HTTP $\Rightarrow$ PORT NO = 80

- $\Rightarrow$ Hyper text transfer protocol (For getting web pages).
- $\Rightarrow$ HTTP always need Reliability.
- $\Rightarrow$ HTTP uses 'TCP' at Transport layer.
- $\Rightarrow$ HTTP is Inband protocol (Both data and commands go in one connection).
- $\Rightarrow$ HTTP is stateless protocol.
- $\Rightarrow$ The two popular versions of HTTP are: HTTP 1.0 (Non-persistent connection)
- $\Rightarrow$ HTTP 1.1 (persistent connection)
- $\Rightarrow$ The popular methods that are used by HTTP are

- a) Head $\Rightarrow$ Get the Header of webpage (metadata).
- b) Get } used with forms
- c) post }
- d) put $\Rightarrow$ To upload an object
- e) Delete $\Rightarrow$ To delete the object
- f) Trace $\Rightarrow$ Trace the servers which are sending data to you.
- g) options
- h) connect $\Rightarrow$ https uses it. (For Authentication).

4. FTP

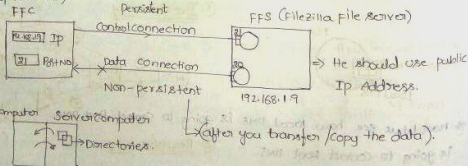
FTP = File Transfer Protocol.

FTP PORT NUM = 21

$\Rightarrow$ Tectia, File Zilla are the two most popular FTP's.

$\Rightarrow$ FTP is used to transfer files.

(FileZilla file client)



$\Rightarrow$ FTP is called out of Band protocol and requires Reliability.

$\Rightarrow$ FTP uses TCP as the underlying protocol.

$\Rightarrow$ FTP is stateful protocol.

5. SMTP AND POP

(48)

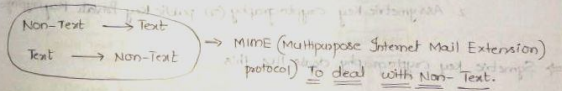
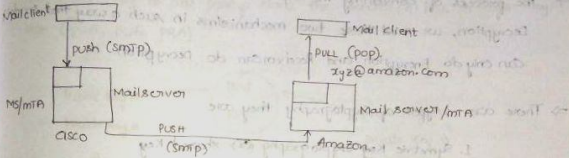
SMTP = Simple Mail Transfer Protocol, POP = post office protocol.

⇒ E-mails are transferred using SMTP

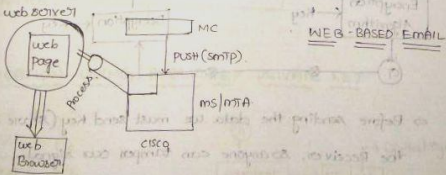
⇒ we cannot transfer the files using FTP because to transfer the files using FTP both server and client should be online.

⇒ Gmail is the web based mail

⇒ MTA = Mail Transfer Agent



What Gmail does is,

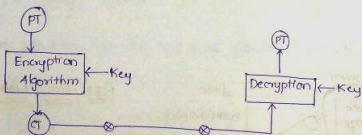


⇒ SMTP and POP are Inband protocols.

19. NETWORK SECURITY

1. INTRODUCTION TO CRYPTOGRAPHY

- ⇒ The main aim of cryptography is to convert a message from plain text into some unreadable form before you send it over the wires.
- ⇒ The process of converting the plain text to cipher text is called Encryption.
- ⇒ The process of converting the cipher text to plain text is called Decryption, we need these two mechanisms in such a way that sender can only do Encryption and Receiver can do Decryption.
- ⇒ There are 2 types of Cryptography they are
 1. Symmetric Key Cryptography (a) shared Key
 2. Asymmetric Key Cryptography (a) public Key Private Key Cryptography
- ⇒ Symmetric key cryptography deals like this

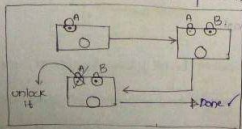


KEY-EXCHANGE

PROBLEM.

- ⇒ Before sending the data we must send Key (Share the Key with the Receiver, so anyone can tamper our signal).

- ⇒ The solution to the above problem comes in form of public, private keys



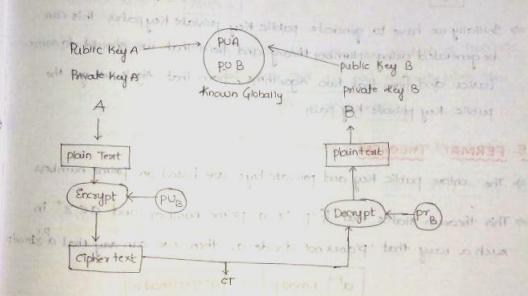
public, private Keys works Analogous this way.

2. ENCRYPTION USING PUBLIC KEY PRIVATE KEY

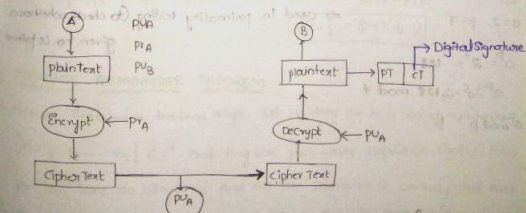
⇒ Before transmission of Data both sender and Receiver should generate a pair of keys called public key and private key. These keys work this way,

⇒ If you encrypt anything with public key of A, you can Decrypt only with private key of A and vice versa.

⇒ Now, after generating pair of keys, Now both public key of A, public key of B should be known Globally, and the private key will only be known only to that party. Now, the sender (A) has 3 keys they are (PUA, PUB, PRA).

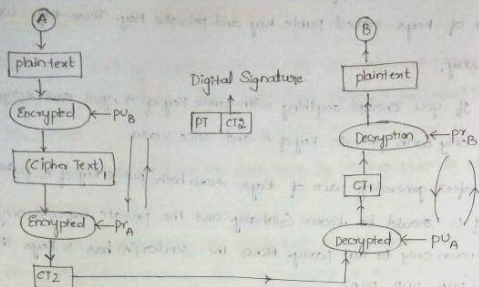


3. AUTHENTICATION USING PUBLIC KEY PRIVATE KEY



HACKED ⇒ so this method is used only for Authentication not for security.

4. ENCRYPTION AND AUTHENTICATION TOGETHER



⇒ Initially we have to generate public Key private Key pairs this can be generated using Number theory and from that we should do some Basics and from that two Algorithms, from that Algo's we get the public Key private Key pairs.

5. FERMAT THEOREM

⇒ The entire public Key and private Keys are based on prime numbers

⇒ This theorem states that if 'p' is a prime number and $a \in \mathbb{Z}^+$ in such a way that 'p' does not divide a; then we can say that $a^{p-1} \equiv 1 \pmod{p}$

$$a^{p-1} \equiv 1 \pmod{p} \quad \equiv \quad a^p \equiv a \pmod{p}$$

Ex:

$$a=2, p=7$$

$$a^p = 2^7 = 128$$

$$a^{p-1} = 2^6 = 64$$

$$a^{p-1} \pmod{p} = 1$$

⇒ used in primality testing (to check whether a given no. is prime)

EULER'S TOTIENT THEOREM

⇒ Euler Totient function says that if we have a number n , then the Euler totient function $\phi(n)$ is defined as the no. of integers k in the range $1 \leq k \leq n$ which are relatively prime to n , $[\gcd(k, n) = 1]$.

$$n=9 \Rightarrow 1, 2, 4, 5, 7, 8 \Rightarrow \phi(9) = 6$$

$\{1, 2, 4, 5, 7, 8\}$ are Relatively prime to 9. $\Rightarrow \gcd(1, 9) = \gcd(2, 9) = \gcd(4, 9) = \gcd(5, 9) = \gcd(7, 9) = \gcd(8, 9) = 1$

$$n=5 \Rightarrow 1, 2, 3, 4 \Rightarrow \phi(5) = 4$$

$$n=7 \Rightarrow 1, 2, 3, 4, 5, 6 \Rightarrow \phi(7) = 6$$

$\therefore$ If n is prime no. then $\phi(n) = (n-1)$

$$n=10 \Rightarrow 1, 3, 7, 9 \Rightarrow \phi(10) = 4$$

⇒ $\phi(n)$ is Multiplicative $\Rightarrow$ If n can be written as product of two no. m, l such that m, l are relatively prime then

$$\phi(n) = \phi(m) \times \phi(l)$$

$$\Rightarrow \phi(10) = \phi(2) \times \phi(5) \quad \text{Relatively prime numbers to each other.}$$

$$= 1 \times 4$$

$$\Rightarrow \phi(10) = 4$$

$$\Rightarrow \phi(35) = \phi(5) \times \phi(7)$$

$$= 4 \times 6$$

$$\phi(35) = 24$$

⇒ If p, q are prime numbers then $\phi(p \times q) = \phi(p) \times \phi(q)$

$$\phi(p \times q) = (p-1)(q-1)$$

1. CHINESE REMAINDER THEOREM

⇒ Chinese Remainder theorem says, Let us say we have set of numbers

$\{n_1, n_2, n_3, \dots, n_k\} \in \mathbb{Z}^+$ and they are pairwise coprimes ($\gcd=1$) then

we can take an integer x and we can represent it uniquely and such

x should be in the range of less than or equal to product of $\{n_1, n_2, \dots, n_k\}$

$$\Rightarrow x \in (1, \dots, n_1 \times n_2 \times n_3 \dots \times n_k)$$

$$x \equiv a_i \pmod{m_i}$$

$$x \equiv a_k \pmod{m_k}$$

⇒ Now let us say I have two relatively prime numbers (2, 5). Now I can take $2 \times 5 = 10$ and I can write all the nos between 1 to 10 uniquely as set of Remainders when divided with 2 and with 5.

	÷ by 2	÷ by 5	Remainder
1 -	1	1	
2 -	0	2	
3 -	1	3	
4 -	0	4	
5 -	1	0	
6 -	0	1	
7 -	1	2	
8 -	0	3	
9 -	1	4	
10 -	0	0	

⇒ Mainly used in Encryption.

8. PRIMITIVE ROOT

⇒ If 'a' and 'n' are Relatively prime numbers then there exists atleast one number 'm' such that $a^m \equiv 1 \pmod{n}$

If $a=7, n=19$ then $m=?$ (Take the smallest value)

$$\Rightarrow 7^m \equiv 1 \pmod{19}$$

$$\Rightarrow m=3 \Rightarrow 7^3/19 = 1 \Rightarrow \boxed{m=3} \quad \left\{ \text{option verification method} \right\}$$

9. CHINESE REMAINDER THEOREM

③ If $a=3, n=7, m=2$

$$\Rightarrow 3^m \equiv 1 \pmod{7}$$

$$\Rightarrow \boxed{9 \equiv 1}$$

Now, $3 \bmod 7 \Rightarrow$

$$\begin{array}{ll} 3^1 \bmod 7 = 3 & 3^5 \bmod 7 = 5 \\ 3^2 \bmod 7 = 2 & 3^6 \bmod 7 = 1 \\ 3^3 \bmod 7 = 6 & 3^7 \bmod 7 = 3 \\ 3^4 \bmod 7 = 4 & \vdots \end{array}$$

I got all numbers from (1 to 6).
 $\therefore$ The repeating sequence (3, 2, 6, 4, 5, 1) is called period = 6 (total n-1).

Now, $2 \bmod 7 \Rightarrow$

$$\begin{array}{ll} 2^1 \bmod 7 = 2 & 2^5 \bmod 7 = 4 \\ 2^2 \bmod 7 = 4 & 2^6 \bmod 7 = 1 \\ 2^3 \bmod 7 = 1 & 2^7 \bmod 7 = 2 \\ 2^4 \bmod 7 = 2 & \end{array}$$

The Repeating sequence is (2, 4, 1) $\Rightarrow$ period = 3.

$\Rightarrow$ Now, If i find $(a \bmod b)$ to all powers of upto 'b' and the period is $\phi(b)$ then 'a' is called as primitive root of 'b'.

9. RSA ALGORITHM (RIVEST SHAMIR ADLEMAN ALGORITHM)

$\Rightarrow$ The most popular algorithm to generate public key, private key $\Rightarrow$ 1977 proposal.

Step-1: CHOOSE TWO DISTINCT PRIME NUMBERS 'P' AND 'Q' (VERY BIG NUMBERS)

Step-2: COMPUTE $N = P \times Q$

Step-3: FIND $\phi(n) = (p-1) \times (q-1) = (p \times q) - (p+q-1) = N - (p+q-1)$.

Step-4: CHOOSE AN INTEGER 'E' SUCH THAT $1 < e < \phi(n)$ & $\gcd(e, \phi(n)) = 1$

$(e, N) \Rightarrow$ PUBLIC KEY

Step-5: DETERMINE 'd' as $d \equiv e^{-1} \pmod{\phi(n)} \Rightarrow ed \equiv 1 \pmod{\phi(n)}$

$(d, n) \Rightarrow$ private key

EXAMPLE

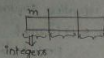
1) $p = 61, q = 53$

2) $n = 61 \times 53 = 3233$

3) $\phi(n) = 60 \times 52 = 3120$

4) $e \Rightarrow 1 < e < 3120 \Rightarrow e = 17 \Rightarrow$ chosen $\Rightarrow$ PUBLIC KEY = (17, 3233)

5) $d \Rightarrow ed \bmod \phi(n) = 1 \Rightarrow [ed \bmod \phi(n)] = 1 \Rightarrow d = 2753 \Rightarrow (2753, 3233) =$ PRIVATE KEY



(A)

$$p_{0A} = (11, 3233)$$

$$p_{rA} = (2753, 3233)$$

$$m = 65$$

$$CT \Rightarrow (65)^{17} \bmod 3233$$

$$CT = 2790$$

Encryption

$$\text{Cipher Text} = (m)^e \bmod n \Rightarrow \text{To Encrypt}$$

$$\text{plain Text} = (CT)^d \bmod n \Rightarrow \text{To Decrypt}$$

$$\Rightarrow \text{At Receiver } m = (2790)^{2753} \bmod 3233$$

$$m = 65$$

10. DIFFIE HELLMANN ALGORITHM

$\Rightarrow$ This Algorithm is based on the concept of primitive Root

$\Rightarrow$ This Algo is used for generated public and private keys

$\Rightarrow$ This Algo is used to share the Key securely. Key Exchange

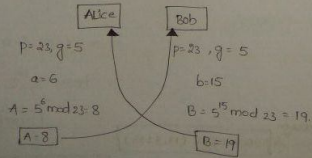
Alice

Bob

- 1) Both Alice and Bob Agreed to use a prime number 'p' and base 'g'.
- 2) Alice choses a secret Key (secret Integer) 'a', then sends $A = g^a \bmod p$
- 3) Bob also choses a secret Integer 'b' then he too sends $B = g^b \bmod p$ to Alice
- 4) Both Alice and Bob compute the secret Key like this.

Alice computes $S = B^a \bmod p = 19^6 \bmod 23 = 2$

5) Bob computes $S = A^b \bmod p = 8^{15} \bmod 23 = 2$



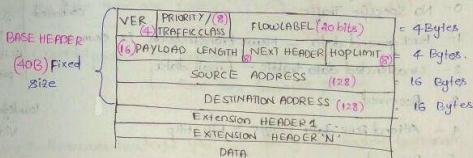
$\Rightarrow$ Not used for Encryption and Decryption used only for Key exchange

20. IPV6 AND WIFI

Need for IPV6:

- IPv4 Address depletion (Not Available no. of Ip Address)
- Realtime Audio/video transmissions
- Encryption (provided at N/w level).
- Authentication
- fast processing (Avoid the process that makes the routers work (Busy))
- Additional functionalities. (Extend Headers concept is used)
- IPv6 is called Ipvng (ng = Next Generation)

IPV6 HEADER



VER → what type of version we are holding. (If VERSION = 0110 = IPV6
0100 = IPV4)

PAYLOAD LENGTH:

8H	PAYLOAD
----	---------

 → IPV6 packet
Base Header

NEXT HEADER: It says what type of Extension Header is just next to the destination Address (Extension Header 1) (same as options)

Hop Limit: Is same as TTL.

Questions that might be possible ques

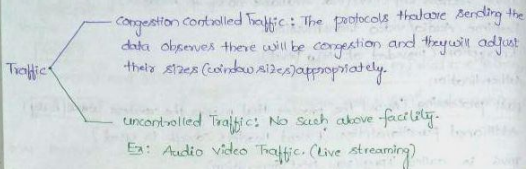
- 1) what are the fields that are present in both IPV4 and IPV6? (VERSION)
- 2) what is the size of source & dest field.

→ TRUE / FALSE QUESTIONS!

→ which of the following has static header IPV6 / IPV4? (Ans: IPV6)

3. TRAFFIC CLASS

The traffic can be classified into 2 types



→ Now the first 4 bits of Traffic field will be given to priority [4 bits (0-15)]
(0-7) (8-15)

Pi Meaning

0 - No specific Traffic

1 - Background data - News transmission is example

2 - Unattended data traffic - Email data

3 - Reserved

4 - Attend Bulk data traffic - FTP, HTTP

5 - Reserved

6 - Interactive traffic - Remote login, putty, ssh

7 - control traffic - Highest priority amongst all (SNMP, Routing data)

congestion controlled
↓
8 - least priority
↓
15 - high priority
↓
low definition videos.

Simple Network management protocol

→ The priorities are set by the upper layers. (above Network layer) and IPv6 should provide an interface to the above layers by which priorities are set.

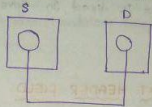
→ Source can set priority, Routers can change priority.

→ Destination should not assume the packet received is of same priority as set by source.

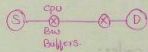
4. FLOW LABEL FIELD

Now, Assume, there are two process within 2 hosts. The stream of packets that go from source-destination is called "flow". And all the packets that belong to same flow have the same requirements, They are

1. Source Address
2. Destination Address
3. priority of all packets should be same
4. Extension headers should be same



→ This says that whenever you are sending the flow, before sending inform all the intermediate routers to allocate appropriate resources for a flow. Generally for informing the routers that you are going to send the data, there are 2 ways.



1. Control packets
 - Resource Reservation protocol
 - Real time transport protocol.

2. Extension headers: you can specify the Routers to allocate Resources.

→ For all the packets in the flow we use a label called flow label. (Randomly chosen)

→ The advantage of flow label is whenever a packet with label 10 arrives at the router, now router will form the flowtable and the contents are

Source address	Flow label	Information
A	10	Bw, Buffer, CPU

→ one entry is enough for all the packets

→ Hashing is used on flow table

Que that might be asked:

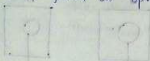
- Between a source and destination there could be more than one flow.
- All the packets need not have flow label, a packet can have flow label = 0
- Router can ignore this facility.

5. PAYLOAD LENGTH

The entire thing that is present after Base header is called payload.

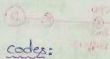
The payload contains: Extension Header, upper layer packets. **

→ Header is fixed in IPv6.



6. NEXT HEADER FIELD

Now, consider an IPv6 packet that contains a TCP packet (TCP header, TCP data) then Next Header field should contain '6' which indicates the packet next is TCP packet.



Next Header codes:

code Next header

0 Hop by Hop option

2 ICMP

6 TCP

17 UDP

43 Source routing

44 Fragmentation

50 Encapsulated Security payload

51 Authentication

59 NULL (No Next header)

60 Destination option.

IPv6		
Next Header = 6	TCP Header	TCP Data

IPv6		
Next Header = 17	UDP Header	UDP Data

IPv6 SRH FRH			
NH=43	NH=6	TCP Header	TCP Data

IPv6 SRH FRH			
NH=43	NH=44	NH=6	TCP Header

7. ORDERING OF EXTENSION HEADER

The order in which the Extension Headers should be placed after Base Header are defined by RFC, and the order is.

1. Hop by Hop options Header
2. Destination option Header
3. Routing Header
4. Fragment Header
5. Authentication Header
6. Encapsulating Security payload Header
7. Destination Header
8. Upper layer Header.

This order is not mandatory but it is a general convention.

(54)

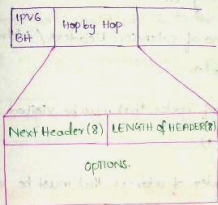
Each Extension Header should not appear more than once, except "Destination Options Header" *** (Atmost 2 times)

If Hop-by-Hop options is even present in a packet then it should always be present immediately after Base Header (Mandatory Rule).

HOP BY HOP OPTIONS HEADER

The importance of Hop by Hop options header is whenever a source is sending the IPv6 packet via some intermediate routers then the packet should be examined by all the intermediate routers and the destination, and check if any functions are specified that must be carried out.

The hop-by-hop options look like.



payload = 16 bits

$\Rightarrow$ max size of payload = $2^{16} - 1$
= 65535

$\therefore$ If payload/data size is > 65535 we use "Jumbo packet".

1. Jumbo packet: payload size > 65535 then we use "Jumbo packet".

2. pad 1: we have to see all the options of bytes in length if we are having 1 option < 8B then we pad some bits.

ROUTING EXTENSION HEADERS - 1

$\Rightarrow$ Source Routing option header: source takes the control over the path in which its packet should be transmitted.

$\Rightarrow$ Assume that source (A) wants to send a packet to destination (B) via 3 intermediate routers (R₁, R₂, R₃). (A - R₁ - R₂ - R₃ - B)

⇒ Now, say the IPv6 contains the Baseheader and Routing Header (RH)
and we know that the Base Header contains (Source Address and Destination Address)

∴ BH $\begin{cases} \text{Source Address} \\ \text{Destination Address} \end{cases}$

RH $\begin{cases} \text{The order of address that the packet should go} \\ \text{SL field} \end{cases}$

DA = R1

A[0] = R2

A[2] = R3

A[3] = B

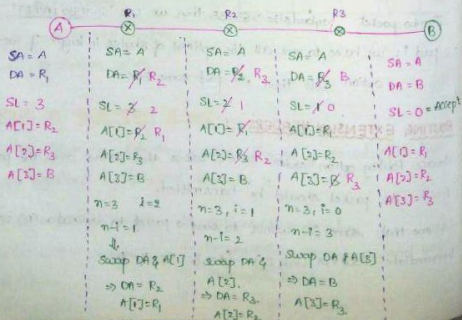
⇒ Along with BH, RH we will have a field called "segments left" which represents the no. of intermediate nodes which are left to be visited before we reach the final destination. In this case, when the packet starts, its SL value = 3 (No. of intermediate routers that have to be visited before reaching 'B').

⇒ Let 'n' represent the no. of extension Headers / Address that are present in Extension Header

⇒ Let 'i' represent the no. of nodes that must be visited before we reach final destination. ($i = SL - 1$)

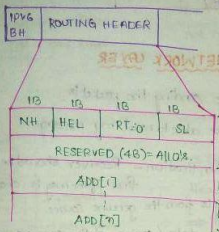
⇒ Now, $(n - i)$ gives the Index of address that must be visited next

⇒ Now swap DA and the A[i]



10. ROUTING EXTENSION HEADER-2

55



HEL = Header Extension length

RT = Routing Type

SL = Segments left

⇒ HEL represent the size of header in terms/units/multiples of '8'.

⇒ Now, say HEL = 8 then what are no. of addresses that are present?

Each Address will contribute 2 to the HEL ⇒ $\frac{16}{2} = 2$ → Address size in IPv6

∴ HEL = 8 ⇒ No. of addresses = $\frac{HEL}{2} = \frac{8}{2} = 4$ addresses are present.

∴ No. of IPv6 Address = $\frac{HEL}{2}$

11. FRAGMENTATION EXTENSION HEADER

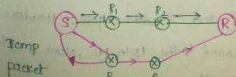
⇒ Not required for all packets

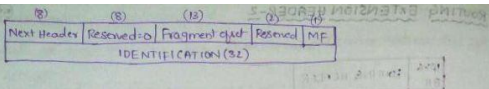
⇒ In IPv4 the fragmentation is done both at the "routers" and at "source".

⇒ In IPv6 the fragmentation is done only at the source. ***

The Routers are not supposed to do the fragmentation.

⇒ The sender finds the path MTU before sending the packet and fragment it appropriately and starts the transmission. But there is no guarantee that the packet follows the path for which we calculated the MTU. In that case, an icmp packet will be generated and sent to the sender.





12. NEED FOR SECURITY AT NETWORK LAYER

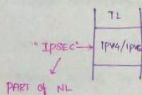
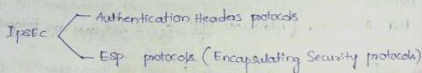
The main things that we need while sending the packet is

- 1) Confidentiality - No one should be able to read my messages.
- 2) Message Integrity/Message Authentication - Receiver should be able to find if the msg is changed or not.
- 3) Source Authentication - If the msg is from the genuine source.
- 4) Reply attack problem - corrupt the data/copies of the same packet.

→ The protocol that is used to provide the above features is called

'Ip security' protocol (or) 'IPSEC'

↓
collection of protocols.



13. MODES OF IP SECURITY

There are two modes in which Ip security operates, they are

1. Transport mode

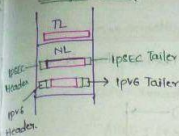
2. Tunnel mode

Transport mode:

Consider a Transport layer packet is passed to the NL then in the NL,

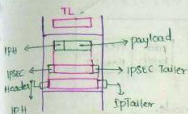
first the packet is received by IPsec and it adds IPsec Header and IPsec Trailer and again it is passed to the IP in NL, Now, IP adds IP Header and IP Trailer and transmits the packet.

Transport mode



⇒ The main point to note is the modification is done only on the payload part but not on the Transport/Network layer Headers.

Tunnel mode



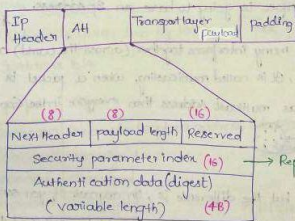
⇒ The transformation is done on both the Headers and payload.

⇒ This is called tunneling because an IP packet is kept inside another IP packet and the two IP headers need not be same.

⇒ In IPv6 the Tunneling is used in between routers.

14. AUTHENTICATION HEADER

→ Authentication Header mainly provides us with message Integrity, Source Authentication.



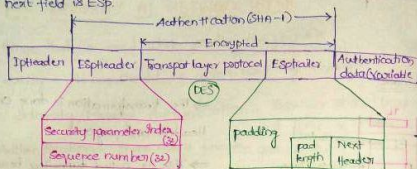
⇒ NH: (8-bit) = Tells what is present in the next field if IP data is present then NH = 6.

⇒ payload length: (8-bit): The length of the 'Authentication Header.' The Authentication Header size is measured in size of 4 Bytes (scale factor 4)

15. ESP

Encapsulation Security payload protocol.

→ If the protocol field of IP header contains the number 50 then it represents that the next field is ESP.



→ The AH and ESP are operated under Transport mode.

16. IPV6 ADDRESSES

Size: 128 Bits

→ Unicast

→ Multicast

→ Anycast

Unicast: Every interface is going to have an IP address.



Multicast: we group many interfaces together (across the world) and assign an IP address to the group. It is called multicasting. When a packet is sent at having the destination IP as multicast address then everyone in the group is going to receive it.



Anycast:

Same as multicast but the difference is, in anycast if you send a packet having destination IP as Anycast address the packet will be delivered to the closest host and it is the responsibility of that host to distribute the packet to every host in the group.



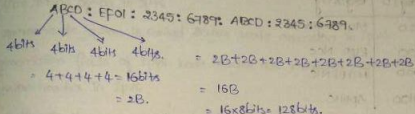
→ In IPv6, Broadcasting is not defined.

IPv6 ADDRESS REPRESENTATION

Colon Hexa Representation

→ IPv4 was using dotted decimal Representation.

→ IPv6 uses colon-hexadecimal Representation.



→ Most of the parts of IPv6 are Zeros.

$ABCD : EF01 : 0000 : 6789 : 0000 : EF01 : 2345 : 6789$
 Actual: $ABCD : EF01 : 0000 : 0789 : 0000 : EF01 : 0345 : 0789$

→ They have used short hand representation by deleting the leading 0's and if all 4 are present they used a single 0.

Short Hand: $ABCD : EF01 : 0 : 789 : 0 : EF01 : 345 : 789$
 $ABCD : EF01 : 0 : 789 : 0 : EF01 : 345 : 789$

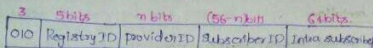
8 TYPES OF IPv6 ADDRESS

When an IPv6 Address is given then by looking at first few bits we can decide what type of Address it is.

prefix	Type
First 8 bits = 00000000	Reserved - Loopback address, don't have IP.
00000001	unassigned
00000010	unassigned
00000011	unassigned
00000100	unassigned
00000101	unassigned
00000110	unassigned
00000111	unassigned
0001	Reserved
001	Reserved
010	provider based unicast Address
011	unassigned
001	Geographic based unicast

* 11111111 010 = link local address
 * 11111111 011 = site local address
 * 11111111 = multicast address

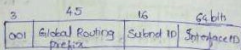
19. PROVIDER BASED UNICAST ADDRESS



SID IID

Registry ID	Registry
10000	Multiregional
01000	RIPE NCC
11000	INTERNIC
00100	APNIC

Geography Based unicast Address



contains Latitude and Longitude locations.

Multicast Address: first 8 bits concerns.

Flag: 0000 = permanent group

0001 = Transient group

Scope: 4 bits = 0000 = Reserved

0001 = Node local

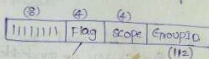
0010 = Link local

0101 = Site local

1000 = Organizational

1110 = Global

1111 = Reserved



0000 = permanent

0001 = Transient

Anycast:



Assign the same IP address to the interface of the Each node and send the packet with that address.

20. SOME SPECIAL ADDRESS

Unspecified: All 0's = 128 bits core 0's.

Loopback Address: Test self connectivity = All 0's except last bit (=1)
= 127.0.0.1 and last '1'.

IPv4 compatible: First 96 bits 0's and last 32 bits represent IPv4 address.

IPv4 mapped: First 80 bits 0, next 16 bits 1's remaining 32 bits = IPv4 address.

Q5: IPv4 VS IPv6

(58)

- 1) No operation and end of options in IPv4 is replaced by 'PAD1' and 'PAD N' in IPv6
- 2) No Record Route option in IPv6
- 3) No time stamp option in IPv6
- 4) The source route option is called source route extension in IPv6
- 5) Fragmentation fields of IPv4 base header are moved to fragmentation extension header in IPv6
- 6) The authentication extension header is new in IPv6
- 7) The encrypted security payload extension header is new in IPv6