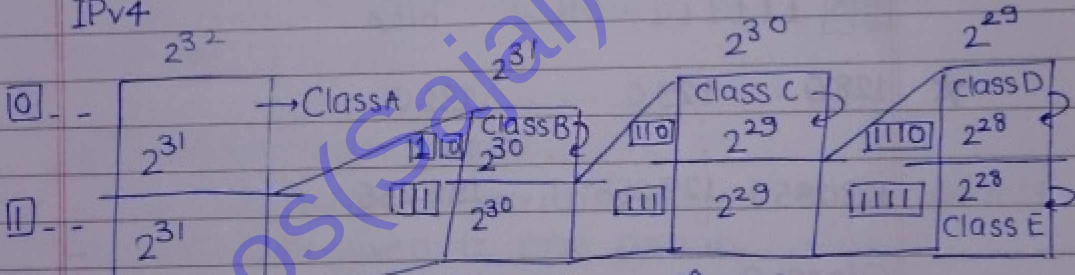
classmate
Date
Page

Date
09.12

- iplookup/ALL
- NSlookup

→ If we type the title of a website, e.g. "www.gmail.com", then to get its IP address of the webpage, then DNS is taken use of to get the IP address,
DNS gives the IP address of that webpage & is composed of netid & hostid which is used to access the network containing that server which contains the webserver. & hostid contains address of that webserver.

IPv4



first bit fixed (0 in upper half, 1 in lower half)

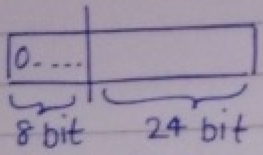
first 2 bits are fixed

first 3 bits are fixed

☆ Class A:-

0 000 0000(0) → not taken as any network id $\boxed{1-126}$
0 000 0001 (1)
0 000 0010 (2)   (1-126 n/w id's are allotted).
⋮
0111 1111 (127) → not taken as any network id (taken as loopback address)

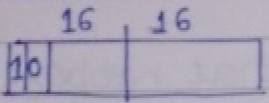
Cosmos(Sajal) @ Techbits



NID HID

2^7 n/w $2^{24}-2$ host

★ Class B :-



2^{14} n/w $2^{16}-2$ hosts n/w

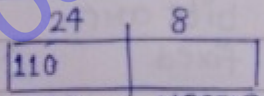
$\boxed{128-191}$

$\boxed{1}\boxed{0}$ 000000 - 128
000001 - 129
000010 - 130
⋮
$\boxed{1}\boxed{0}$ 111111 - 191

64 (first 8 ~~bytes)~~ bits

★ 128.0 . . . 129.0 . . . . . 191.0
⋮ ⋮ ⋮
128.255 129.255 191.255

Class C :-



NID HOSTID

2^{24-3} 2^8-2
$=2^{21}$ N/w host n/w

$\boxed{192-223}$

$\boxed{1}\boxed{1}\boxed{0}$ 00000 - 192
00001 - 193
⋮
11111 - 223

32 (first 8 bits are considered)

→ $2^5 \times 2^{16}$
$= 32 \times 2^{16}$
$= \boxed{2^{21}}$

Cosmos(Sajal) @ Techbits

192.0.0 . . . . . 223.0.0
⋮
192.0.255 223.0.255
⋮
192.255.255 223.255.255

Class D

→ Used for multicasting

$\underbrace{\boxed{1110}}_{4\text{ bits}}\underbrace{\boxed{\qquad\qquad\qquad}}_{28\text{ bits}}$ $\boxed{224-239}$

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

2^{28} = 256 million groups.

- Class D is used for multicasting & each address in class D is given to one group.

Class E

$\underbrace{\boxed{1111}}_{\substack{4\text{ bits}\\(\text{fixed})}}\underbrace{\boxed{\qquad\qquad\qquad}}_{28\text{ bits}}$

- Class E is used for special purposes.

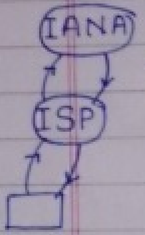
$\boxed{240-255}$

1111 0000 → 240
0001 → 241
⋮
1111 → 255

Cosmos(Sajal) @ Techbits

classmate
Date
Page

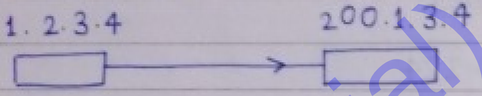
IANA
(Internet assigned Numbers Authority)



IANA provides IP addresses to different requesters.

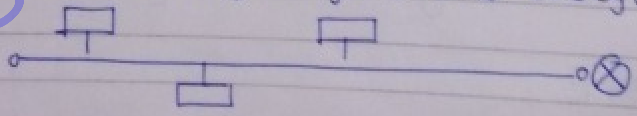
Types of message casting

① Unicast → Sending a message from one host to another (1:1).



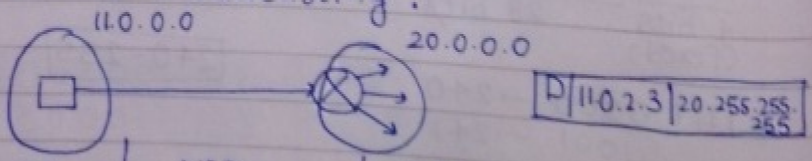
② Broadcast→ sending a message from 1 host to all other hosts is called broadcasting.

a. limited broadcasting: sending a message from 1 host to all other hosts in the same network is called limited broadcasting.
LAN is a switch; everyone sees everything else.



router blocks the traffic.

(b) Directed broadcasting :



IP	NID	DBA	LBA
1.2.3.4	1.0.0.0	1.255.255.255	255.255.255.255
192.1.2.3	192.1.2.0	192.1.2.255	,,
173.1.2.3	173.1.0.0	173.1.255.255	,,

Cosmos(Sajal) @ Techbits

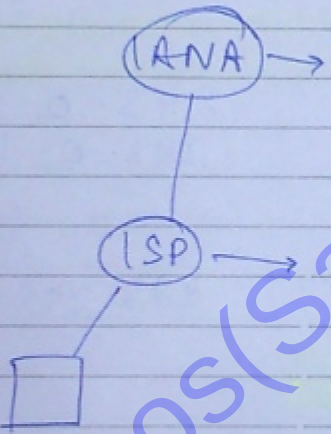
- each address in class D is given to one group.

Class E

- ~~249-2~~ 240-255

- there is no concept of nw id or host id.

- Reserved

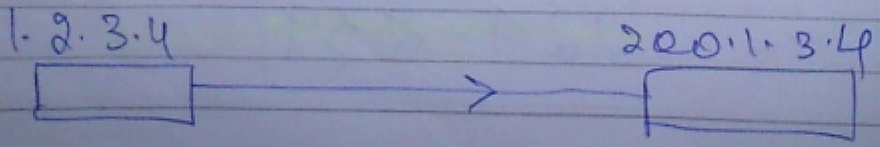


IANA → Internet assigned numbers authority.

ISP → ISP buys class from IANA

Types of message casting

① Unicast → sending a message from 1 host to 1 host. (1:1)



Cosmos(Sajal) @ Techbits

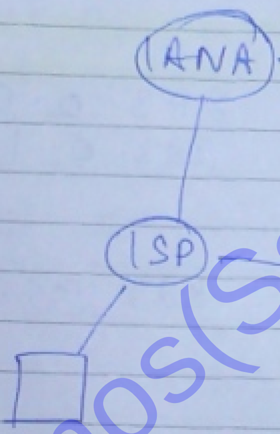
- each addres in class D is given to one group.

Class E

- 249-2 240 - 255

- there is no concept of nw id or host id.

- Reserved

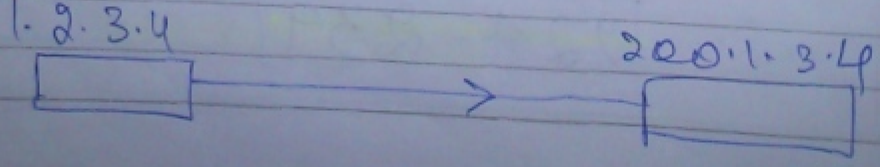


IANA → Internet assigned numbers authority.

ISP → ISP buys class from IANA

Types of message casting

① Unicast → sending a message from 1 host to 1 host. (1:1)



Cosmos(Sajal) @ Techbits

Date :

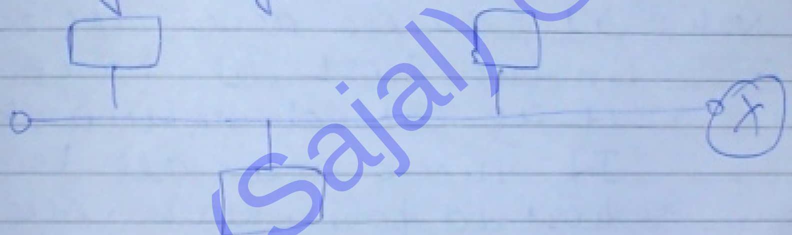
Page No. :

② **Broadcast** → sending a message from 1 host to all other hosts is called broadcasting.

a) **limited broadcasting**: sending a message from 1 host to all other hosts in the same network is called limited broadcasting.

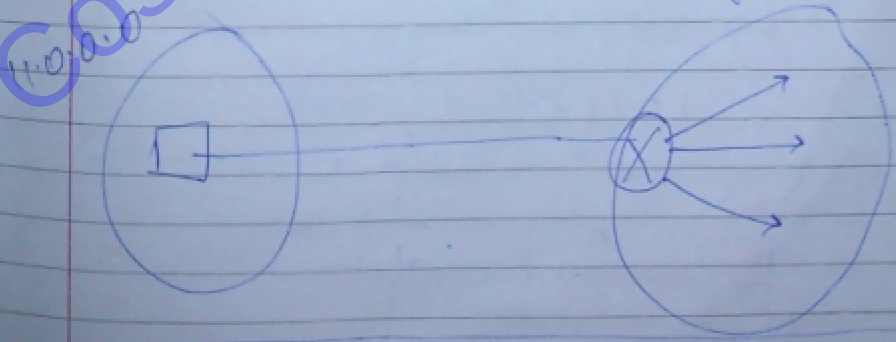
(All 0s signify entire n/w.

LAN is a switch; every one sees everything else!



router blocks the traffic.

b) **Directed broadcasting**: 20.0.0.0



D	11.0.2.3	20.255.255.255

Cosmos(Sajal) @ Techbits

IP	NID	DBA
1.2.3.4	1.0.0.0	1.255.255.255
192.1.2.3	192.1.2.0	192.1.2.255 ~~192.255.255.255~~
173.1.2.3	173.1.0.0	173.1.255.255

LBA

255.255.255.255

"

"

same

Note: if there are all zeros in the host id part, then it is called network id. If there are all 1s in the host id part, then are called directed broadcast address for that network.

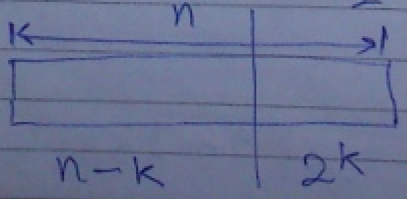
Thus, 2 IP addresses are reserved, first and last.

Cosmos(Sajal) @ Techbits

10110

$2^1 - 0$

$2^2 - 2$



after If there are n bits in a number and if we divide it with 2^k then least significant k bits is remainder and most significant n-k bits is quotient.

Rules for CIDR blocks

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

② Size of a block must be a power of 2. (when size is a power of 2, we can divide it the easy ~~this~~ way)

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

(a) (Rest all will be zeros and first IP address can be made the NID (ID).

Eg 200.1.2.32
⋮
200.1.2.47

$\left.\begin{matrix} 200.1.2.32 \\ \vdots \\ 200.1.2.47 \end{matrix}\right\} \cancel{47}\ 16 = 2^4$

check last 4 bits, if they are 0s, means this is a valid 16 block.

Cosmos(Sajal) @ Techbits

CIDR representation of a block

a.b.c.d/n where a.b.c.d is IP address and n is no of bits used for network id part.)

32-n : host id bits

$2^{32-n}-2$: no of hosts. again, first address identifies block, and last address is reserved for directed broadcast.

- for the eg above, mask is 28 2^{32-28} addresses for hosts.

- eg. 100.100.100.100/27

01100100

01100000 = 96

→ 100.100.100.96 →

⋮

100.100.100.127 →

- any address in the block may be given.

Cosmos(Sajal) @ Techbits

Date:
Page No.:

Q 120.250.250.250

x 11111010.11111010

1111

180.240.0.0

11111011

N/w id.

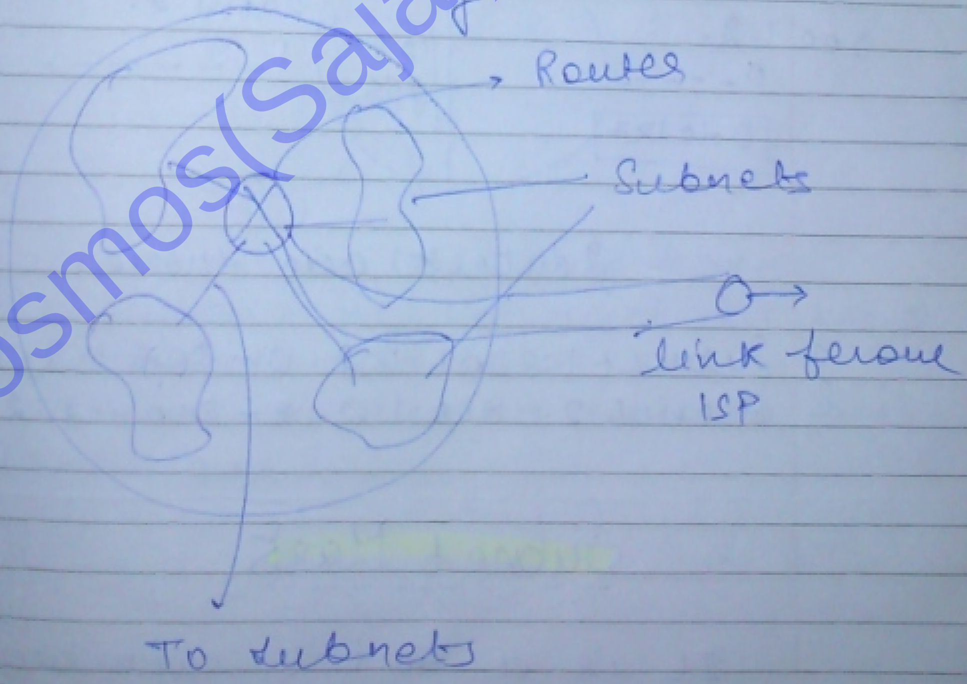
first

120.250.240.0
to
120.250.255.255

directed broadcast

Subnets

dividing a big network into many ~~s~~ smaller networks is called subnetting.

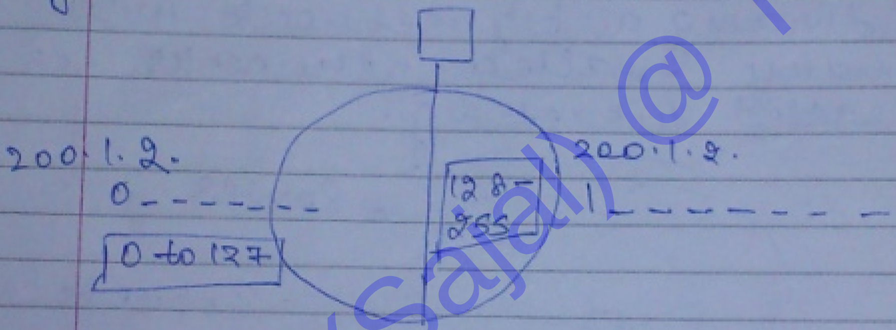


Cosmos(Sajal) @ Techbits

Advantage:
① Maintenance
② Security

Disadvantage:
① Routing becomes difficult.
- Identification of N/w
- Idn of Subnet within N/w.
- Idn of host within subnet
- Idn of process within host

Eg 200.1.2.0



2 subnets are there.

{ Subnet 1: 200.1.2.0 - 200.1.2.127
Subnet 2: 200.1.2.128 - 200.1.2.255

Subnet Mask

It is a 32 bit number in which no of ones indicate n/w id part plus subnet id

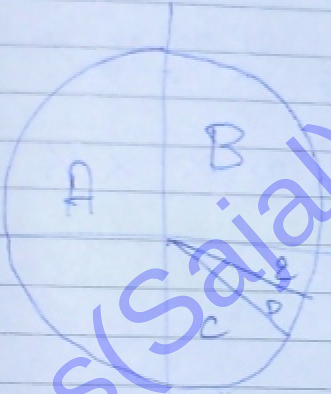
Cosmos(Sajal) @ Techbits

part and number of zeros indicate host id part.

Eg. for a class C address with 4 subnets, the subnet mask will be the following

255.255.255.192

for dividing the n/w into 3 parts; use 3 subnetting bits.



for each subnet, we have different net id and directed broadcast address.
for the n/w as whole, these are unique.

Cosmos(Sajal) @ Techbits

Computer Networking

	#hosts	CA	CB	CC
255.0.0.0	$2^{24}-2$	1	X	X
255.255.0.0	$2^{16}-2$	2^8	1	X
255.255.255.0	2^8-2	2^{16}	28	1
255.128.0.0	$2^{23}-2$	2^1	X	X
255.240.0.0	$2^{20}-2$	2^4	X	X
255.255.192.0	$2^{14}-2$	2^{10}	2^2	X
255.255.248.0	$2^{11}-2$	2^{13}	2^5	X
255.255.255.128	2^7-2	2^{17}	2^9	2
255.255.255.240	2^4-2	2^{20}	2^{12}	2^4
255.255.255.255				
	#hosts	#CA	#CB	#CC

there is no -2 here

Cosmos(Sajal) @ Techbits

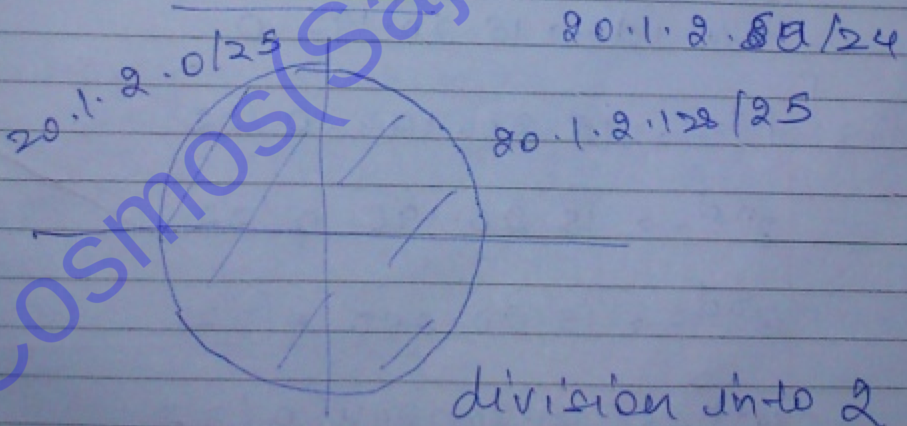
Note: Common mistake

1) Number of subnets
all 0s and all 1s in the subnet id are possible.

If k bits are chosen for subnet id part, then 2^k-2 subnets is wrong.

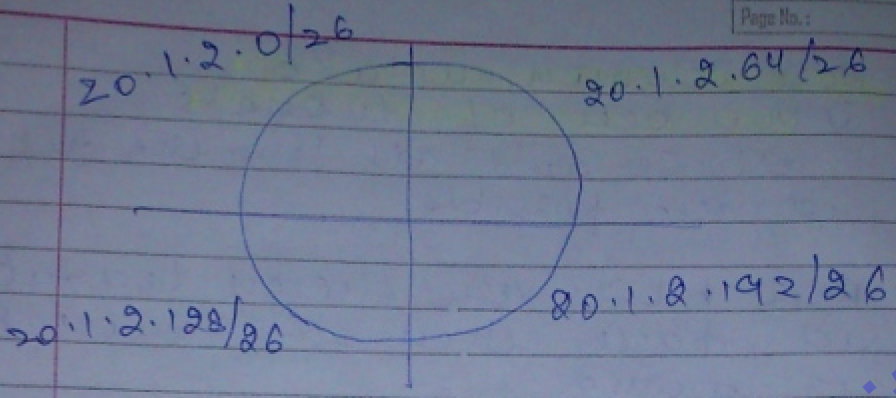
2) Theoretically, we can choose any bits from any position in the host id part for subnetting. Practically, we should always choose from first few bits.
We can have $^8C_2$ subnet masks.

Subnetting in classless



division into 2

Cosmos(Sajal) @ Techbits



division in 4 parts

Eg

15.20.198.100/20

↓

1100|0110

divide in 4 parts

N/w id → 15.20.192.0

1st → 15.20.192.0/22

2nd → 15.20.196.0/22

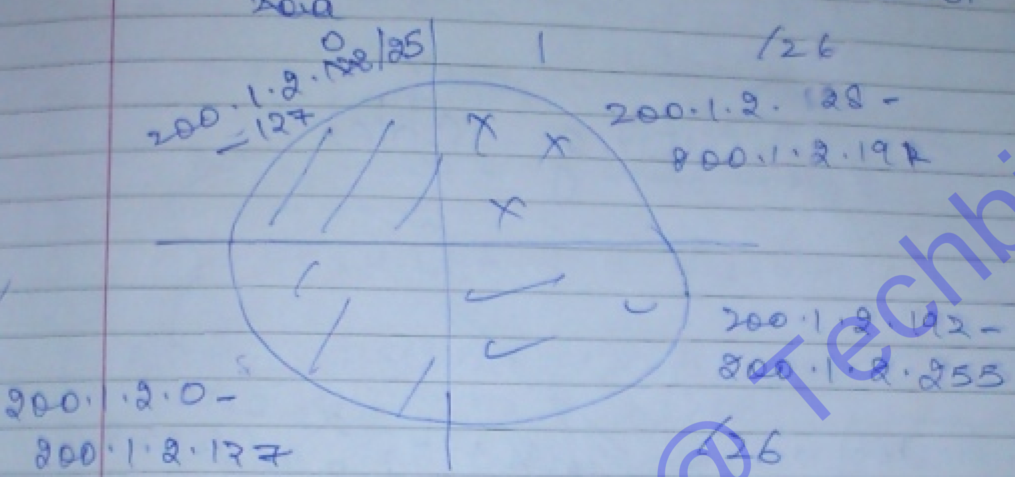
3rd → 15.20.200.0/22

4th → 15.20.204.0/22

Cosmos(Sajal) @ Techbits

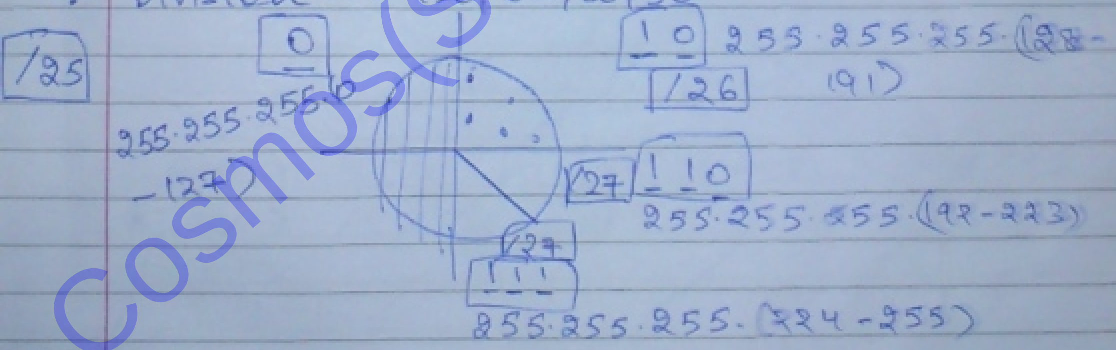
Variable length Subnet Masking (VLSM)

∴ 200.1.2.0/24 divide into 3 subnets such that we get 120,60 and 60.



* we can also divide it the other way.

∴ Division → 120, 62, 30, 30



20.1.198.100/20 divide into 1/2, 1/4, 1/4

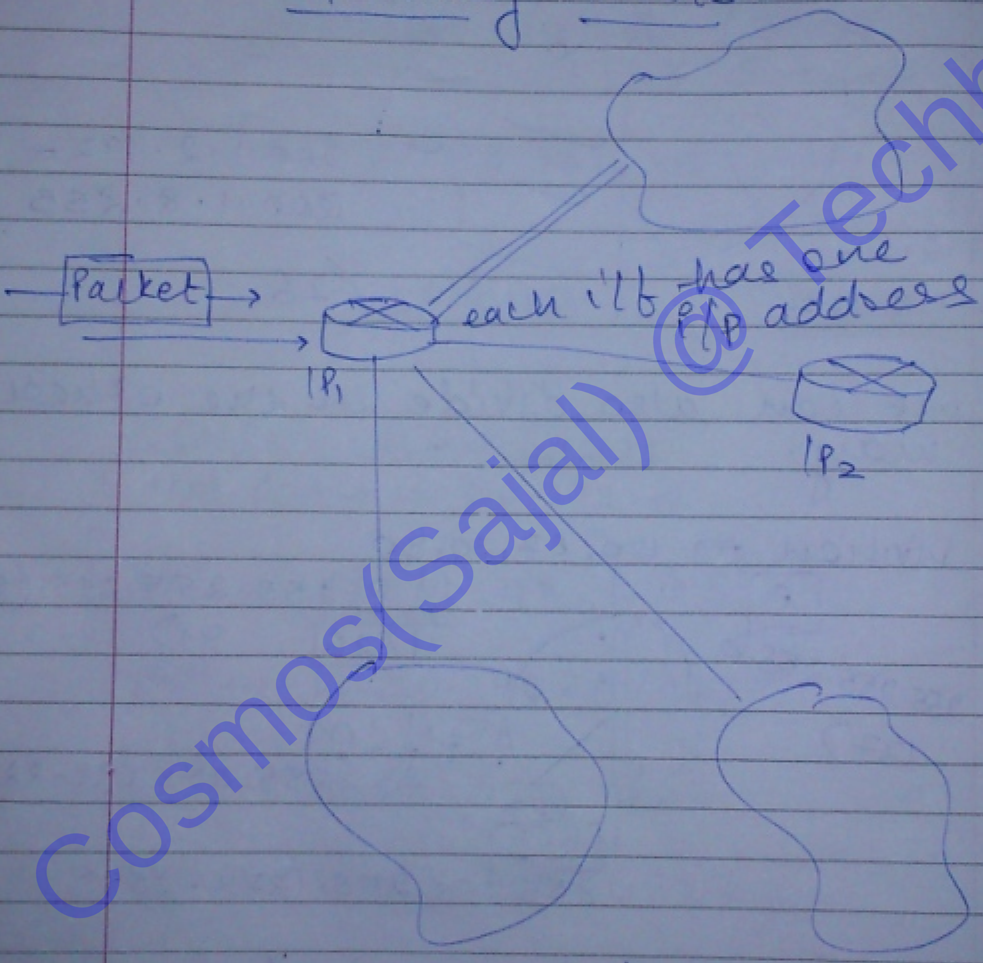
Cosmos(Sajal) @ Techbits

20.1.192.0/21

20.1.200.0/22

20.1.204.0/22

Routing Table

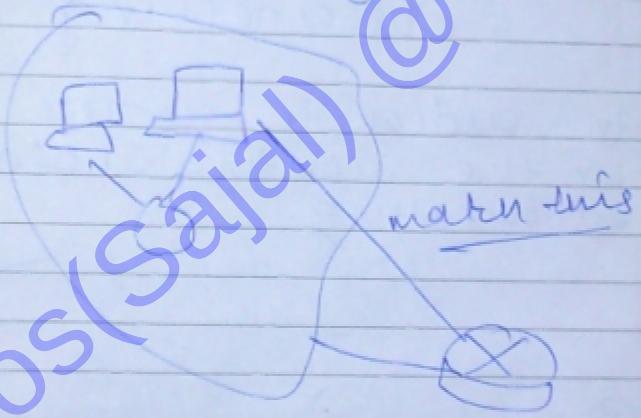


Cosmos(Sajal) @ Techbits

whenever a packet comes to the router, it masks the destination IP and mask, and searches the table.

NID	Subnet Mask	Interface
NID1	SM1	eth0
NID2	SM2	eth1
NID3	SM3	eth2
NID4	SM4	eth3
default		eth5

Note: largest mask should be matched first



Going for largest mask makes search easy.

Cosmos(Sajal) @ Techbits

Eg

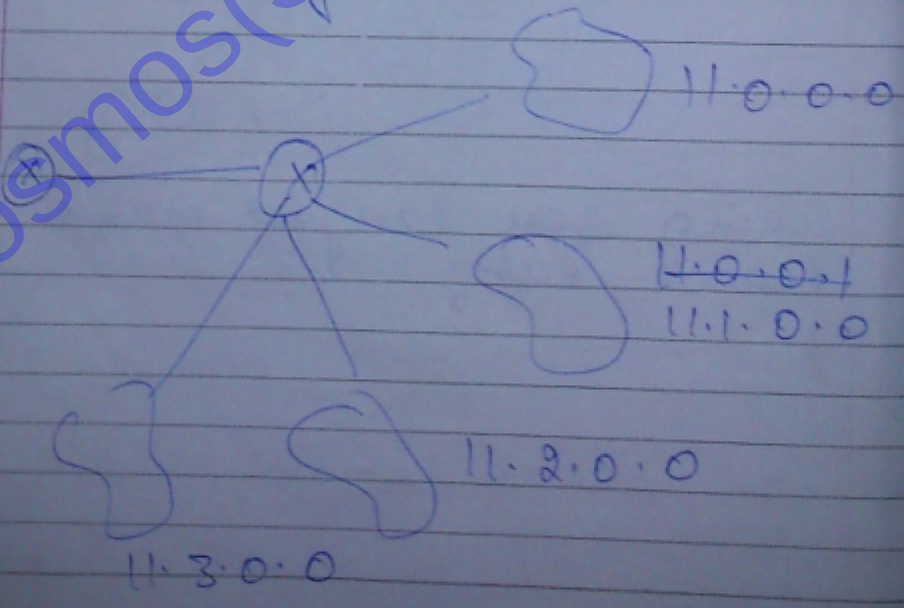
20.0.0.0	255.0.0.0	eth1
20.128.0.0	/9	eth2
20.128.0.0	/10	eth3
20.160.0.0	/12	eth4
	default	eth5

→ 20.168.3.1 matches all, forward to eth4

→ 120.x.y.2 matches none, sent to default.

Supernetting

- In order to reduce the entries in the routing table, we need supernetting.



Cosmos(Sajal) @ Techbits

Supernetting rules:

1. Network ids should be contiguous.

2. number of subnets should be of same size.

3. Number of networks should be a power of 2.

4. first n/w id should be a multiple of supernet size.

finding supernet ID

① find out supernet mask, AND with any IP address.

② AND all of them

③ first ID.

Supernet Mask

It is a 32 bit number in which number of 1s indicate fixed part and number of 0s indicate variable part.

here 173.0.0.0
173.1.0.0
173.2.0.0
173.3.0.0

~~255.255.2~~
255.252.0.0

Cosmos(Sajal) @ Techbits

1 7 199010000
8

10000.
12 16 8 4 2

Subnet mask:

$\boxed{255.252.0.0}$

Eg:

193.20.32.0
:
:
193.20.95.0

} 64

not possible because first address 32 is not div by size i.e 64

193.20.32
:
:
47

address

mask

$\boxed{255.255.224.0}$

↓

This AND with any IP should yield nwo id.

Cosmos(Sajal) @ Techbits

1 CA

10.0.0.0 — 10.255.255.255

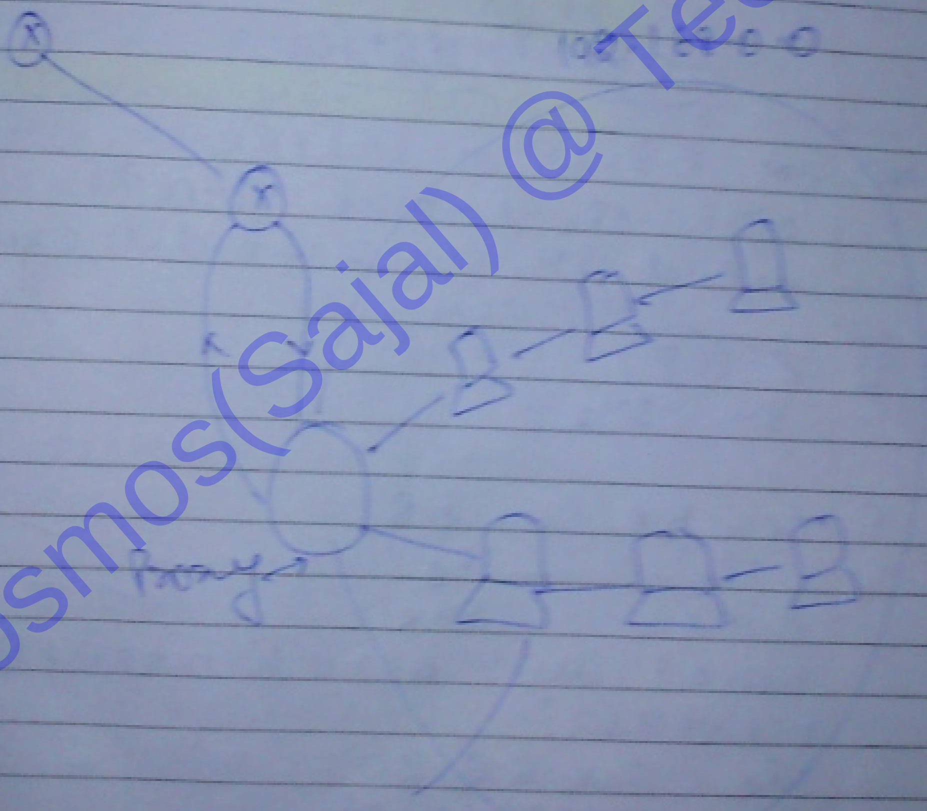
16 CB

172.16.0.0 — ~~172.16~~ 172.31.255.255

256 CC

192.168.0.0 — 192.168.

Network Address Translation



Private addresses can be assigned to all the nodes. Proxy does the job of deciding who takes

Cosmos(Sajal) @ Techbits

what. Depends on what is being requested.

— x —

IPV4 exhaustion

→ IPV4 addresses are getting over fast, this problem is called getting consumed fast'

Soln:

IPV6

NAT

Gate Questions

Q) SM

a) IP$_1$, IP$_2$ & same n/w?

→ And SM, check if nid is same.

Q) b) IP

SM$_1$, SM$_2$

Q) Comp A, Comp B

IP$_A$	IP$_B$
SMA	SMB

what will A think about B & vice versa?

IP$_A$: 200.1.2.20

SMA : 255.255.255.128

IP$_B$: 200.1.2.~~180~~70

255.255.255.192

Cosmos(Sajal) @ Techbits

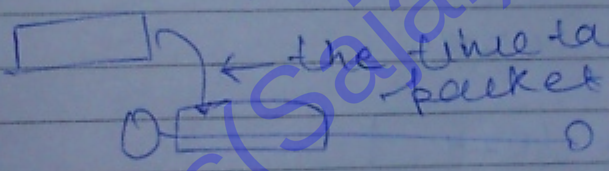
Date :
Page No. :

Q IP → NID
SM
SM

Q Note:

Delays in Computer Networks

- Transmission delay: Time taken to transfer a packet on to the outgoing link. This means



the time taken to put a packet on the line

factors : ✓ size
✓ BW

B bps

$1 \text{ sec} \rightarrow B \text{ bits}$

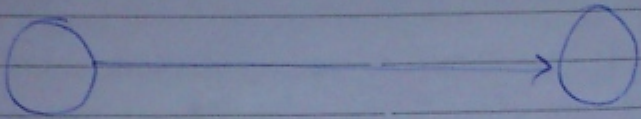
$B \text{ bits} \rightarrow 1 \text{ s}$

$1 \text{ bit} \rightarrow \frac{1}{B} \text{ sec}$

$$\boxed{L \text{ bits} \rightarrow \frac{L}{B} \text{ s}}$$

Cosmos(Sajal) @ Techbits

- Propagation delay: Time taken by a bit to travel from 1 end of the wire to other end of the wire.



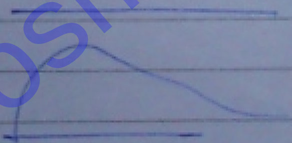
$$\boxed{T_p = \frac{d}{v}}$$

Q. If Bw is 1000 bps & L = 1000 bits then what is the Tframe?
→ 1s

Q If B = 1kbps & L = 1kb

V $T_t = \frac{1000}{1024}$

=> $\boxed{T_t = \frac{1024}{1000}}$



Q if d = 2 km, v = 2×10^8 m/s

$$\boxed{T_p = 10\ \mu s}$$

Cosmos(Sajal) @ Techbits

10^{-3} $\quad 2\times10$ $+10^{-5}$

$10^{-3}(1+0.01)$

Date:

Q $L = 1000$ bits, $B = 1$ mbps

$d = 2$

1.01 ms

T_t
↓
T_p
↓
~~Queue~~ ^{0}
↓
~~Processing~~ ^{0}
↓
~~$T_t(Ack)$~~ ^{0}
↓
T_p

$\boxed{T_t + 2*T_p}$

Time = $T_{del} + T_{trans}$

$$T = \frac{d}{V} + \frac{L}{B}$$

$$= \frac{2\times10^3}{2\times10^8} + \frac{10^3}{10^6}$$

$$= 10^{-3} + 10^{-5}$$

$$\boxed{T = 1.01\text{ms}}$$ Ans.

Flow Control Mechanisms

* A fast sender should never send more than what a receiver can receive.

STOP AND WAIT

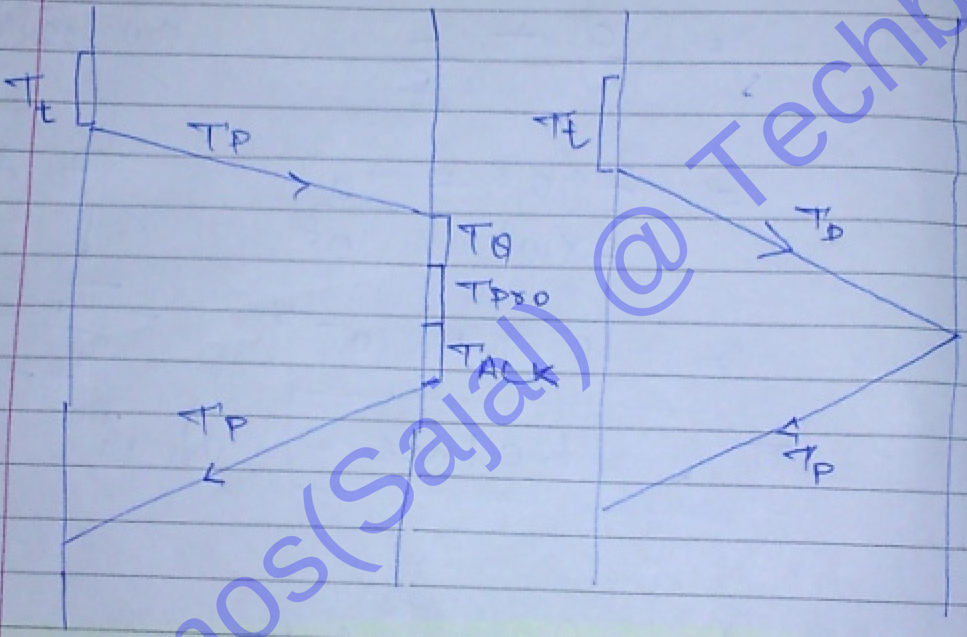
In this strategy, a sender will send data and wait for ACK, before sending next data.

Cosmos(Sajal) @ Techbits

Therefore, total time taken to send one data packet is

$T_{transfer}(data) + 2 \times T_{prop}$

→ Queuing, uncertain, assumed 0
→ Processing " "
→ $T_{transfer}(ACK) \simeq 0$



(a) (b)

(a): detailed timing diagram
(b): Timing when all extra delays assumed 0.

$$\eta = \frac{\text{Total time spent transmitting}}{\text{Total Cycle time}}$$

Cosmos(Sajal) @ Techbits

$$n = \frac{T_t}{T_t + 2 \times T_p}$$

$$\boxed{n = \frac{1}{1+2a}} \qquad \boxed{a = \frac{T_p}{T_t}}$$

Q if $n = 1/2$ in stop and wait, then what is reln between T_t and T_p.

Ans

$$\frac{1}{2} = \frac{1}{1+2a}$$

$$1 + 2a = 2$$

$$a = \frac{1}{2}$$

$$a = \frac{1}{2} = \frac{T_p}{T_t}$$

$$\boxed{T_t = 2 \times T_p}$$

$$\frac{1}{1+2a} \geq \frac{1}{2}$$

$$2 \geq 1 + 2a$$

$$a \leq \frac{1}{2}$$

$$\frac{T_p}{T_t} \leq \frac{1}{2}$$

$$\boxed{T_t \geq 2T_p}$$

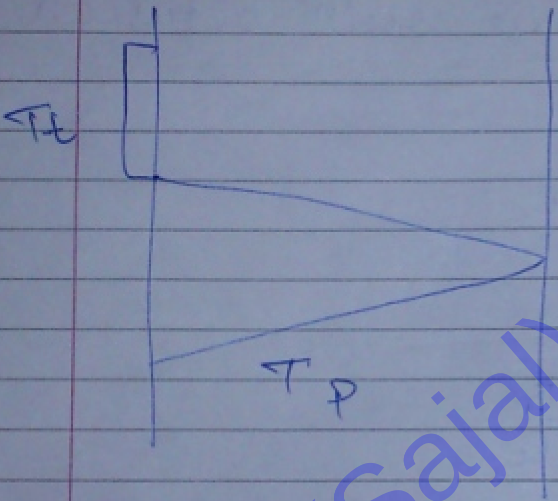
if T_t is very less and T_p is very large, more time will be spent travelling.

Cosmos(Sajal) @ Techbits

Q if $T_p = 1ms$ and $BW = 1Mbps$ what is min length of packet for 50% eff

Ans $$\frac{L}{10^6} \geq 2 \times 10^{-3}$$

$$\boxed{L \geq 2000 \text{ bits}}$$ Ans



to increase eff, you increase Tt, which can be done by increasing length.

Throughput:

Packets / Time

Cosmos(Sajal) @ Techbits

$$\frac{BL}{T_t+2T_p}$$

Link utilization
or
BW utilization $\Rightarrow \dfrac{(L/B)(B)}{T_t + 2\times T_p}$
or
Effective BW

$$= \eta B$$

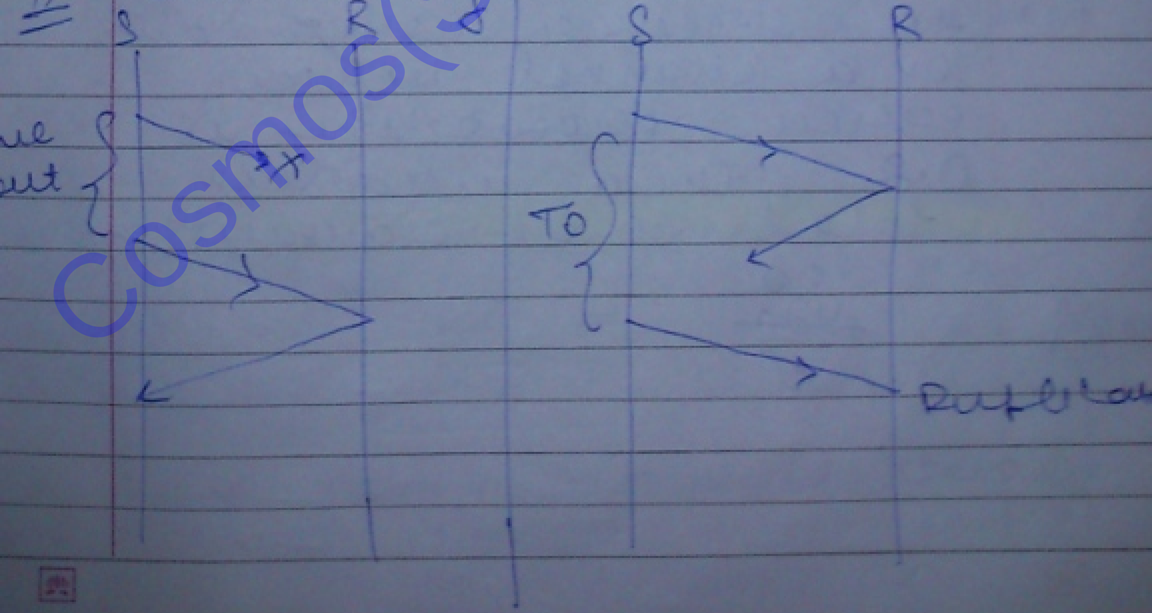
$$\boxed{\text{throughput} = \eta B}$$

Q if $T_t = 1ms$, $T_p = 1ms$ $BW = 3Mbps$, what is TP.

$$= \overset{\eta}{\left(\frac{1}{1+2\cdot 1}\right)}(3\,Mbps)$$

$$\boxed{\text{Ans} = 1\,Mbps}$$

Q Data missing



Cosmos(Sajal) @ Techbits

now, we need to add seq^n no in order to correctly identify packet.

$$S\&W\left[S\&W + TO + Seq^n \text{ number}\right]$$

Q If in stop and wait, a sender is sending 10 packets, in which every 4th packet is lost then what are the total number of retrans req

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

Q if 400 packets are transmitted from sender to receiver using S&W, on a channel where error probability is 0.2, then what is total no of transmission

A $\frac{\overset{80}{\cancel{400}}}{\cancel{5}}$

Cosmos(Sajal) @ Techbits

$$\boxed{n + np + np^2 + \ldots}$$

$$= \frac{n}{1-p}$$

$$= \frac{400}{1-0.8} = 500$$

$$\left[\eta = \frac{1}{1 + 2 \times \frac{d}{v} \times \frac{B}{L}} \right]$$

- As length increases, efficiency increases; stop and wait is suitable for frames of big size.
- As distance increases, efficiency decreases; stop and wait is efficient in LANs, but not in WANs

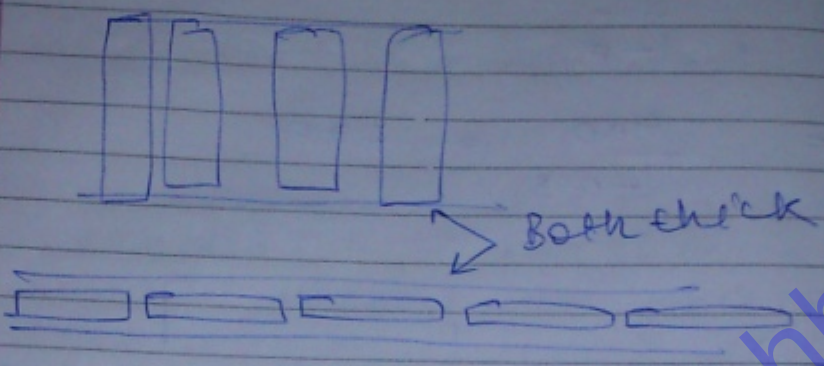
Capacity of a channel

→ Number of bits a channel can hold at any time is called capacity of the channel.

$$\left[\text{Capacity} = \text{Bandwidth} \times \text{Delay} \right]$$

Cosmos(Sajal) @ Techbits

if BW× delay product is high then it is called thick wire || thick channel.



- Basically a measure of how much can be "stuffed" into the wire.

low BW×delay → thin wire

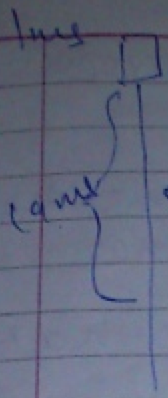
Note:
In thick wires, stop and wait fails, therefore, in order to increase efficiency we use pipelining.

Pipelining

Q if $T_t = 1ms$, $T_p = 9.5ms$, the what is efficiency of S&W

A $\eta = \frac{1}{1+2\times 9.5} = \frac{1}{20}$

Cosmos(Sajal) @ Techbits



← i could have sent additional packets here, this gives motivation for pipelining.

$1\,T_t \rightarrow 1p$

$1p \rightarrow T_t$ se

$1\,sec \rightarrow$

$$\left(\frac{T_t + 2 \times T_p}{T_t}\right) = w_s$$

we need $\lceil \log_2 w_s \rceil$

$T_t + 2 \times T_p$ → Total time spent b/w sending of the packet and receipt of ACK

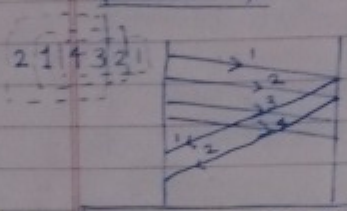
why $/ T_t$: gives us #packets that can be sent. each packet takes T_t to be placed on line

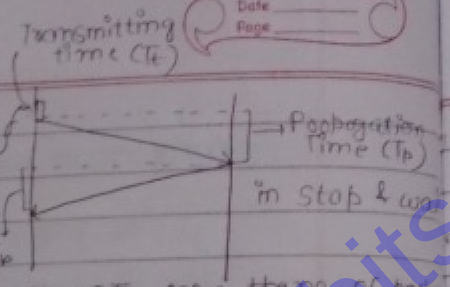
Cosmos(Sajal) @ Techbits

Date

23.09.12

- Quicklinks (Q.44 to 62)





This time period can be used to send more T_p packets, this time = $T_t + 2T_p$, now, the no of packets that can be put on the wire in this time are $\frac{T_t + 2T_p}{T_p}$ which is called the window size

window size $\boxed{W_s = \frac{T_t + 2\times T_p}{T_t}}$

W_s:- window size
T_t :- transmission time
T_p :- Propogation time.

now, the no of packets that can be sent the time $T_t +$ are $\frac{T_t + 2T_p}{T_t}$

so the no. bits in the sequence req. are $\log_2\left(\frac{T_t+2T_p}{T_t}\right)$

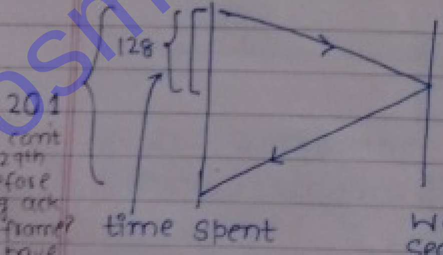
- the min no. of bits req. in sequence no. for window = $\lceil \log_2 W_s \rceil$

Q. If $T_t = 1$ ms, $T_p = 100$ ms, then in a sliding window protocol, then what is the min. no. of bits req. in sequence no. field.

Ans $W_s = \frac{201}{1} = 201$

no. of bits req = $\lceil \log_2 201 \rceil = \boxed{8}$.

★ If we have only 7 bits in sequence no. field, then we can send only 128 bits.



★ 128 ~~bits~~ frames will be sent (& not complete 201), so we can't send frames 129 to 201 in same window, because we have to repeat the sequence no. 0000000 for 129th frame before receiving ack for 0th frame, ∴ we have to wait for ~~20~~ ack of 0th frame which comes after $T_t + 2\times T_p$,

∴ Waiting time $= T_t + 2\times T_p - 128\times T_t$
$= 1 + 2\times 100 - 128\times 1$
$= 201 - 128$
$= 73$

Why we cant send 129th frame before receiving ack for 0th frame?
→ If we have sent 129th frame before receiving ack for 0th frame, then we have to repeat seq no 0000000 for 129th frame & if the 129th frame arrives at the receiver, ~~at~~ before 0th ~~frame~~ then receiver will not be able to distinguish that whether it is a dup frame or a new frame.

Cosmos(Sajal) @ Techbits

$$\boxed{W_{s} = \min\left(\frac{T_t + 2\times T_p}{T_t}, 2^n\right)}$$

n:- no. of bits req. in sequence no. field.

efficiency:- (of stop & wait). $\boxed{\frac{1}{1+2a}}$ $\boxed{a = \frac{T_p}{T_t}}$

sending only 1 frame in a period of 1+ 2a.

[efficiency is total time spent in transmission divided by total ~~time~~ cycle time $(T_t + 2\times T_p)$]

Sliding window protocol (efficiency):-

$\boxed{\frac{W_s}{1+2a}}$

efficiency :- $\boxed{\frac{W_s \times T_t}{T_t + 2\times T_p}}$ → t

total no of packets sent in the interval of $T_t + 2T_p$

$$= \frac{\frac{W_s \times T_t}{T_t}}{\frac{T_t}{T_t} + \frac{2\times T_p}{T_t}} = \frac{W_s}{1+2a}$$

Q. In above question, what is the efficiency.

Ans. $\frac{128 \times T_t}{T_t + 2\times T_p} = \frac{128\times 1}{1 + 2\times 100} = \frac{128}{201}$

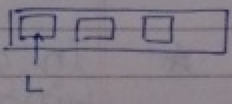
Bandwidth Utilization/

$\eta \times B$ [η:-efficiency B:-bandwidth]

Throughput:- no. of bits

derivation:- $(W_s \times L)$ → total no. of bits in each window

L:- ~~no. of b~~ no. of bits in each frame



$\left.\frac{W_s \times L}{T_t + 2\times T_p}\right\}$ → no. of bits sent per unit of time

$$\left(\frac{W_s \times L/B}{T_t + 2\times T_p} \times B\right) \quad \frac{L}{B} = T_t$$

$= \boxed{\eta \times B}$

Cosmos(Sajal) @ Techbits

★ Sliding window protocol is used for flow control only, if there are any errors, then we need error control also. In Sliding window protocol, error control is implemented in 2 ways:-

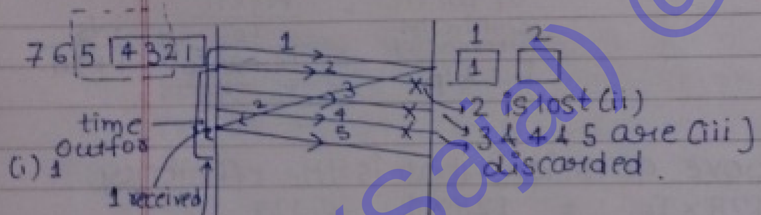
(i) GBN

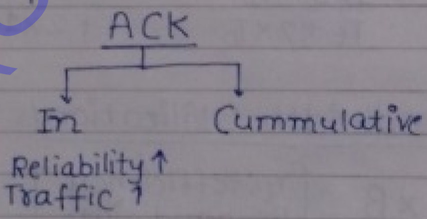
(ii) SR

for GBN:-

$$\frac{N}{1+2a} = \eta$$

$W_R = 1$





(iv) time-out for 2nd packet, so sender knows that packets in window 2,3,4,5 are lost, so sender will go back 4 from 5, (the window will go back N from the time out i.e. from the last frame sent, e.g. in this case from 5.)

★ In go back N, N indicates sender window size, if N=10, then it is go back 10.

★ efficiency of go back N = $\boxed{\frac{N}{1+2a}}$ [from sliding window protocol, $\eta = \frac{W_s}{1+2a}$ & $W_s = N$ in this case.]

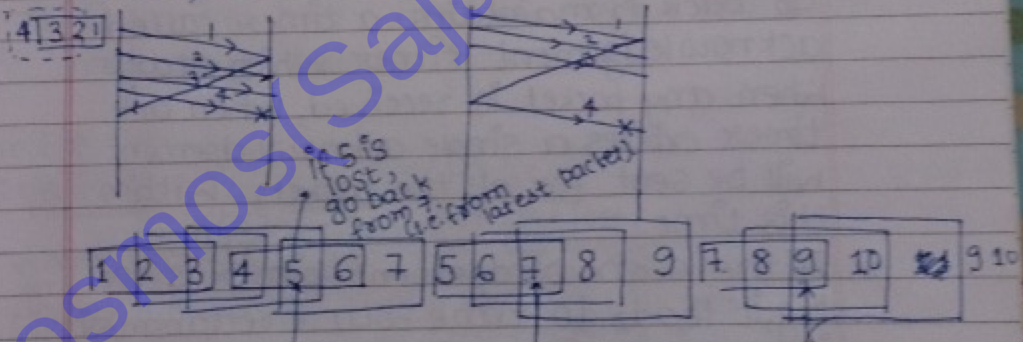
Cosmos(Sajal) @ Techbits

Q. If $T_t = 1ms$, $T_p = 19.5$ ms, then what is the efficiency of GB 10.

Ans $\eta = \frac{10}{1+2\times19.5} = \frac{10}{1+39} = \cancel{0.4}\ 0.25$.

Q. In GBN, receiver window size is 1, which always mean that receiver will be waiting for inorder packet, which means that any out of order packet will be discarded, so sender has to go back N & retransmit entire window if there is any time out.

Q. If in GBN, N=3, 10 packets are to be transmitted & every 5th packet is lost, then what is the total no. of transmissions req.


4 3 2 1
1
2
3
4
4
If 5 is lost, go back from 7 (i.e. from latest packet)
1 2 3 4 5 6 7 5 6 7 8 9 7 8 9 10 9 10

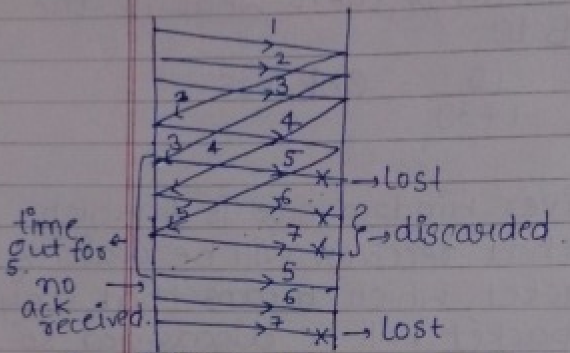
5 is lost, so go back N from 7
7 is lost

$\boxed{18}$ transmissions.

In case of stop & wait :- 1 2 3 4 5 5 6 7 8 9 9 10

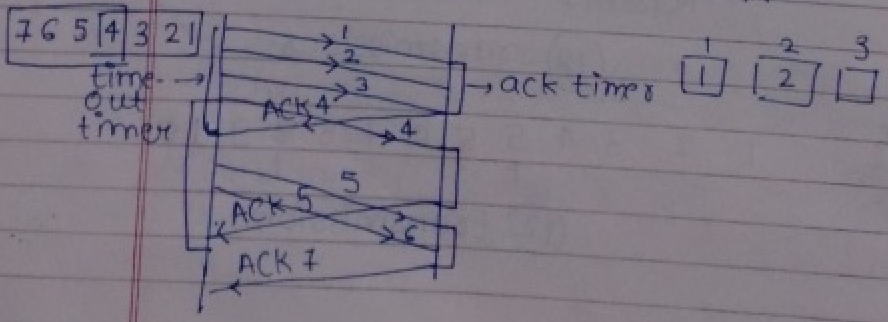
$\boxed{12}$ transmissions.

Cosmos(Sajal) @ Techbits



★ Acknowledgements are of 2 types:-
(i) Independent.
(ii) Cummulative.

★ In Go back N, the acknowledgements are cummulative.
Go back N maintains a timer called acknowledgement timer which starts when any packet is received, when ack timer expires a single acknowledgement will be sent for all the packets within this time.
If the acknowledgement timer is too big, it leads to time-out & retransmission, if the ack timer is too small, it becomes independent ack & more traffic.



Cosmos(Sajal) @ Techbits

★ There are 2 types of Acknowledgements:-

ACK

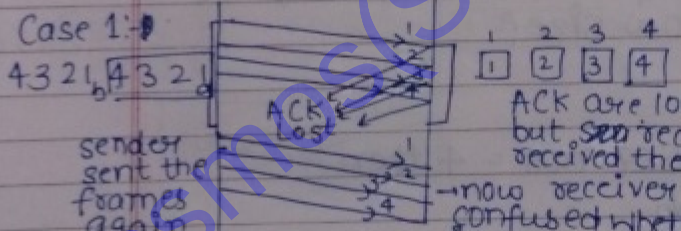
+ve
This indicates that a packet is received & there are no errors in the packet.

-ve
This indicates that a packet is received but there are errors, (detected by CRC).

★ Go back N receiver uses +ve ACK only, i.e. if a packet is corrupted, Go back N receiver will silently discarded & all subsequent packets will also be discarded, so sender will retransmit entire window after time-out.

★ Relation b/w window sizes & sequence nos. in go back N:-

Case 1:-

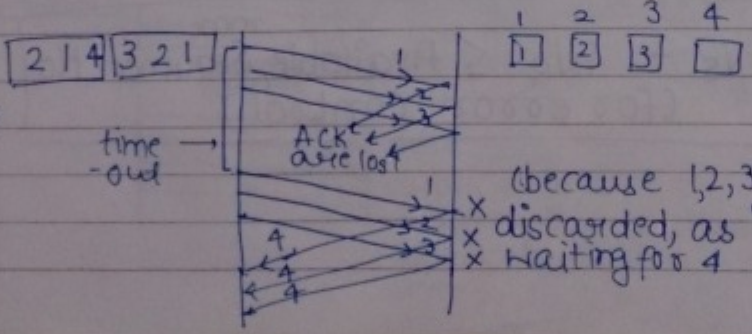


ACK are lost, but ~~sen~~ receiver received the frames

sender sent the frames again (window is not slided)

→now receiver will get confused whether it is from previous window or next window (i.e. if it is 1_a or 1_b).

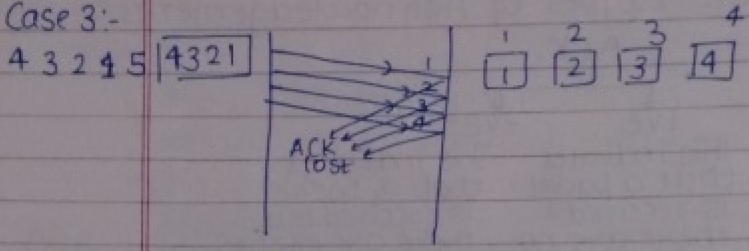
Case 2:- decreasing window size



discarded, as it was waiting for 4 (because 1,2,3 are from previous sliding window)

Cosmos(Sajal) @ Techbits

Case 3:-



Q1. If max. no. of Sequence no. available is N, then what is the max. window size?

Ans. $W_S = N-1$.

Q2. If Sender window size is N, then what is the min. no. of seq. no. req.?

Ans. $N+1$

Q3. If 'k' is max. no. of bits available in seq. no. field, then what is the max. window size?

Ans. $2^k - 1$.

★ if no. of seq. nos. = 4, then

W_S	W_R
3	1
2	1
1	1 → Stop & wait.

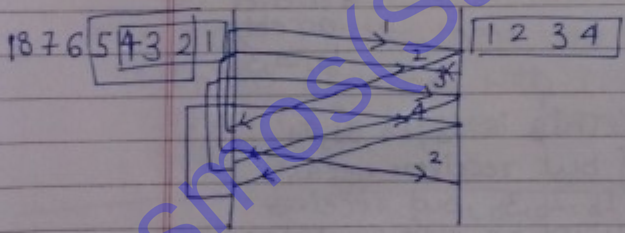
$W_S + W_R \le$ Available, $\overset{\text{max.}}{}$Sequence No.
(for error control.)

Cosmos(Sajal) @ Techbits

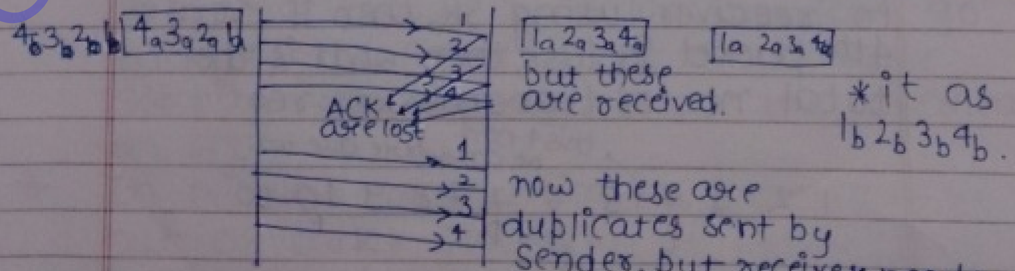
classmate
Date
Page

Selective Repeat

- ☆ In SR, sender window size is N (>1).
- ☆ efficiency of SR :- $\boxed{\frac{N}{1+2a}}$ N:- sender window size.
- ☆ ~~Wherever~~
In SR, receiver window size > 1 (equal to sender window), which implies a receiver can even accept out of order packets, so whenever a packet is lost there will be a time out at the sender & sender will send (or repeat) only lost packet selectively.
- ☆ In SR, acknowledgements are independent, so acknowoledgement timer is zero.
- ☆ In SR, a receiver will send -ve acknowledgement if a packet is received but it has 'bit errors'.



Reln. b/w sequence nos. & window sizes:-



now these are duplicates sent by Sender, but receiver needs $1_b, 2_b, 3_b, 4_b$, but sender sent $1a, 2a, 3a, 4a$, so receiver wont be able to distinguish & accept

classmate
Date
Page

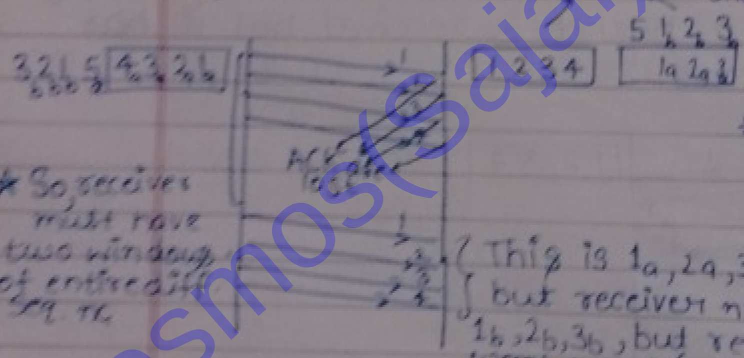
★ If sender window size = receiver window size = N, then what is the min. no. of seq. no. required

Ans. $\boxed{2N}$

★ If max. seq. no. is N, then sender &

★ If k is the max. no. of bits in the sequence no. field, then what is the max. W_S & W_R

$W_S = 2^{k-1}$
$W_R = 2^{k-1}$



these 2 windows should have completely diff. seq. nos.

★ receiver accepts 1a, 2a, 3a :

★ So, receiver must have two window of entire diff seq no

This is $1_a, 2_a, 3_a, 4_a$ but receiver needs $1_b, 2_b, 3_b$, but receiver won't be able to distinguish b/w 1a, 2a, 3a & 1b, 2b, 3b, so ★

Q. If 10 packets are sent from sender to receiver using SR, then if every 4th packet is lost, then what is the total no. of transmissions req.

this 4 can be anywhere else too.

1 2 3 4 4 5 6 7 7 8 9 10 10
↑ ↑ ↑

$\textcircled{13}$ transmissions

Cosmos(Sajal) @ Techbits

★ Comparison b/w Stop & wait, SR, Go back N.

(i) Sequence no. :-
2 in Stop & wait
N+1 in Go back N.
// → $2N^k$ in SR, k=0,1,2,.... [why k?]

(ii) buffers req :-
2 in Stop & wait
N+1 in GBN (N for sender & 1 for receiver).
2N in SR.

(iii) Retransmissions are less in S&W, & SR
more in GBN,
∴ B/w req. is more in GBN.

(iv) Sorting logic & Searching logic is req. in SR,
so more CPU time is req. is SR.

GBN→x S&W→x

Q. If B/w is moderate, buffers are sufficient &
SR✓ ← CPU's are powerful, then SR is preferrable.
→ If B/w sufficient, buffers are moderate &
SRx ← slow CPU's, then Go back N.
→ In a channel with high error probability, then SR is better because no. of retransmissions are less.

★ In wireless communication, out-of-order sequencing of frame arrival wont happen, & error probability is low, therefore go back N is preferred. (& not SR, because searching & sorting will increase the overhead on CPU).

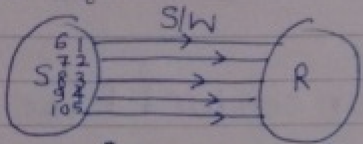
★ In wireless communication, there may be out-of-order sequencing of frame arrival & error probability is high, ∴ SR is preferrable.

Cosmos(Sajal) @ Techbits

classmate
Date
Page

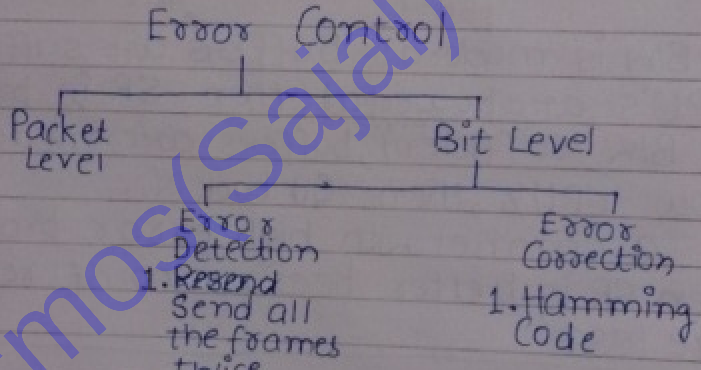
★ If there are N channels b/w sender & receiver & every channel is operated using stop & wait, then what is the overall effect equal to?

→ It is equal to SR.



if there is an error in receiving '1', then only frame 1 is resent & not all 1 to 5, ∴ SR.

★ Go back N is also called conservative protocol.



2. Parity
3. Checksum
4. CRC

→ These 2 are preferrables, because Hamming Code increases the overhead, & Checksum & CRC forces the sender to retransmit the packets only at the time of detection of errors

Cosmos(Sajal) @ Techbits

CRC (Cyclic Redundancy Check) :-

- Cyclic → Cyclic codes
- Redundancy → We are sending extra bits.
- Check → for checking purposes.

Exclusive- OR(XOR) (Modulo-2 sum)

e.g.

```
  1                          1
  1                          1
 ---   '10' mod 2 = 0        1    '11' mod 2 = 1
  10   (2)                  ---
                             11
```

CRC Generator : 1101 , if we have to send 101011

```
1101 ) 101011[000] → added 3 bits
       1101
       ---------
       011111000
        1101
       ---------
        0010100 0
          1101
          -------
          01100
           1101
          -------
           00110 → add this to 101011000
```

```
1101)101011110 → so this no.           in case of error
     1101          will be          1101) 111011110
     ---------     Sent.                  1101
     011111110                            --------
      1101                                 111110
     ---------                             1101
     0010111 0                            --------
        1101                               001011
       -------                               1101
        011010                             -------
         1101                               01100
       -------                               1101
         00000 ← remainder                  ------
                 is 0, so there                 1 ← remainder
                 is no error.                       is not
                                                    zero.
                                                    (so there
                                                    is an
                                                    error.)
```

Cosmos(Sajal) @ Techbits

classmate
Date
Page

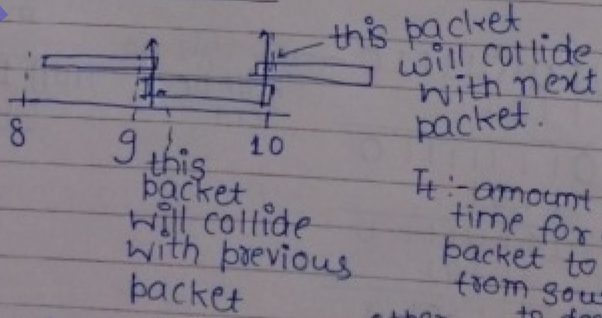
Access Control :-

In a shared link, many stations will share a common medium & try to transmit their data at the same time, ∴ some access control methods are required to control the access to the shared medium.

1. Aloha

In this protocol, any station can send data any time, ∴ collisions are possible. acknowledgements are used in aloha, so if an ack is not received, it indicates that the data might have collided & so retransmission is required. Before retransmitting, a sender must wait for random amount of time called backoff time.

Vulnerable time :-


this packet will collide with next packet.
8
9
10
this packet will collide with previous packet

Tt :- amount of time for a packet to go from source to destination.

→ So, during 9 & 10, no other packet should be there b/w time ~~period~~ >8 & <10.
So, vulnerable time is $\boxed{2 \times T_t}$

→ Vulnerable time means in this period, if there is some other packet, then collision will happen.

Cosmos(Saial) @ Techbits

$$\boxed{Load = \underset{\text{no. of req./sec.}}{\lambda} \times \underset{\text{time slot}}{T_{slot}}}$$

efficiency :- $\boxed{\eta = G \times e^{-2G}}$

where G :- no. of requests per time slot
where time slot = T_t.

$$\frac{d\eta}{dG} = e^{-2G} + G e^{-2G}(-2)$$

$$0 = \cancel{e^{-2G}} - 2G\cancel{e^{-2G}}$$

⇒ $\boxed{G = \frac{1}{2}}$ (so, max. efficiency is when $G = \frac{1}{2}$, i.e. 1 request per 2 time slots,

& max. efficiency $\eta_{max} = 0.184$).

★ B/W utilization = $\eta \times$ Bandwidth
$= 0.184 \times 100$
$= 18.4$

Q1. If B/W of a shared medium is 100 Mbps, then what is actual bandwidth available in Aloha.

Ans. 0.184×100
= 18.4 Mbps.

Q2. In the above ques., in that LAN if every station wants 1 kbps, then how many max. stations can be placed in the LAN.

Ans. $\frac{18400 \text{ kbps}}{1 \text{ kbps}}$ = 18,400 stations.

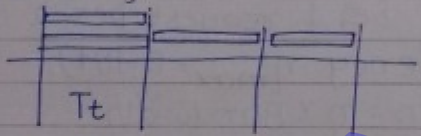
If every station wants 1 Mbps, then max. no. of stations = $\boxed{18}$.

Cosmos(Sajal) @ Techbits

classmate
Date
Page

Slotted ALOHA :-

Time is divided into slots where each slot is T_t & all the stations are forced to transmit only at the beginning of a time slot, ∴



Vulnerable Time = T_t

$\eta = G \times e^{-G}$

$\therefore G = 1$

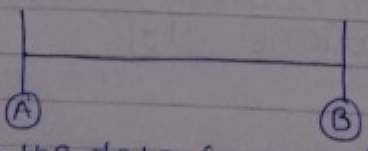
$\therefore \eta_{max} = 36.8\%$

Q1. If B/W = 100 Mbps in a slotted aloha & every station needs 1 Kbps, then what is the max. no. of stations that can be placed in the LAN.

Ans. 36,800.

Note :- Aloha is obsolette.

☆ In worst case :-



When the data from A is about to reach B, if at that pt. collision occurs then it will take another T_p collision time

Cosmos(Sajal) @ Techbits

to reach B.

so, $\boxed{T_t \geq 2 \times T_p}$

$$\frac{L}{B} \geq 2 \times T_p$$

$$\boxed{L \geq B \times 2 \times T_p} \quad \text{CSMA/CD}$$

CSMA/CD

In this, any station can transmit data at any time, but before transmitting the data a station should sense the carrier. If the carrier is free, then data should be transmitted, else the station should refrain.

There are no acknowledgements, ∴ a sender should detect a collision while transmitting the data (if there are any). The condition for collision detection is $\boxed{T_t \geq 2 \times T_p}$.

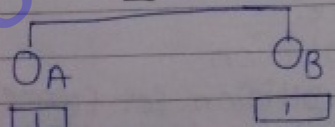
$\Rightarrow \boxed{L \geq 2 \times T_p \times B}$

if $T_p = 1$ ms & $B = 1$ Mbps, then what is min. L for collision detection.

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

$$\boxed{L \geq 2000 \text{ bits}}$$

☆ Exponential Backoff Algo:-



A is sending its 1st frame. B is sending its 1st frame.

both are sending together, so there will be collision, now,

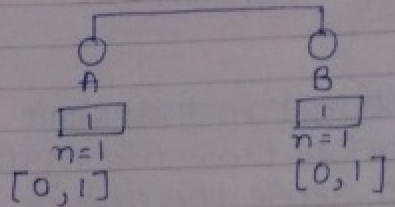
$n=1$ both for A & B (means both frames are collided once.)

- This algo gives waiting time for stations involved in collision.
- This algo works for only 2 stations, so it is called binary backoff algorithm,
- Waiting time for a station is K × Tslot. where K belongs to $[0, 2^{n}-1]$, where n is collision no. for a frame.

Cosmos(Sajal) @ Techbits

classmate
Date
Page

now, the algo will randomly choose K value for frame at station 1 in b/w $[0, 2^1-1] = [0,1]$ & $[0,1]$ for frame at station 2.

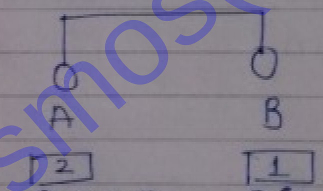


A	B		
0	0	→ Collision	$p(C) = \frac{1}{2}$
0	1	→ A	$P(A) = 1/4$
1	0	→ B	$p(B) = 1/4$
1	1	→ Collision	

$W_T = K \times T_{slot}$ — constant waiting time

↓ K value choosen from [0,1].

★



if A transmit it first.

A is sending 2nd frame.

B is sending 1st frame.

suppose there is a collision.
then it will be 2nd collision for frame 1 at station 2 & it will be 1st collision for frame 2 of station 1.

so $n = 1$ for A
& $n = 2$ for B

A
[0,1]

B
[0,1,2,3]

A will randomly choose b/w [0,1]
& B ,, ,, ,, ,, [0,1,2,3]

Cosmos(Sajal) @ Techbits

A	B
0	0
0	1
0	2
0	3
1	0
1	1
1	2
1	3

this means A will transmit in 0×Td

this means A will transmit in 1×Td

$p(C) = 25\%$
$p(A) = 62.5\%$
$p(B) = 12.5\%$

☆ So, collision probability decreases as no. of collisions increases.

☆ The main disadvantage is Capture Effect, in which 1 frame at one station collide again & again & won't be transmitted at all.

☆

The probability of successful transmission = $np(1-p)^{n-1}$ [When only 1 station transmit & other (n-1) stations doesn't.]

$Prob = np(1-p)^{n-1}$

$\frac{d(prob)}{dp} = 0$ (for max. p)

$\Rightarrow p = \frac{1}{n}$

now, max. prob $= \cancel{n} \times \frac{1}{\cancel{n}}\left(1-\frac{1}{n}\right)^{n-1} = \boxed{\frac{1}{e}}$

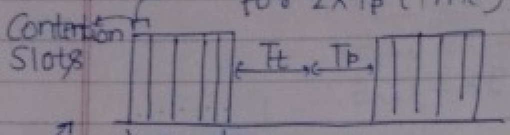
max. probability of success.

☆ So, e tries are required for 1st successful transmission.

Cosmos(Sajal)@ Techbits

Efficiency of CSMA/CD

$2 \times T_p$ (each ~~frame~~ station is sensing link for $2 \times T_p$ time)



e-times.

the frame will be sent e times & will suffer collision & successful ~~ce~~ transmission will take place after e tries.

during this time, the ~~medi~~ sender is transmitting its data for atleast $2 \times T_p$ time & collisions are taking place for 'e' times, ∴ total time = $2eT_p$

☆ If there are n stations, connected by shared medium, then medium will be successfully used only when one station transmits the data & remaining station refrain.

let 'p' be the probability with which a station ~~is sending~~ wants to send data, then prob. of success p

$$p_r = np(1-p)^{n-1}$$

the value of p_r is maximum when $p = \frac{1}{n}$,

$$\therefore \boxed{P_{r_{max}} = \frac{1}{e}}$$

∴ we need on average e no. of tries before 1st success.

∴ η can be analysed as follows

worst case time for contention slots = $2 \times T_p$

Cosmos(sajal) @ Techbits

$$\eta = \frac{T_t}{T_t + T_p + e \times 2 \times T_p}$$

$$= \frac{1}{1+(2e+1)a} = \boxed{\frac{1}{1+6.44a}}$$

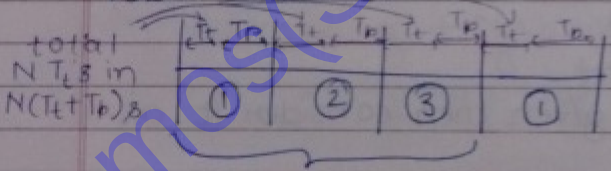
$$\eta = \frac{1}{1+6.44 \times \frac{d}{v} \times \frac{B}{L}}$$

★ if distance increases, efficiency decreases (no. of collisions are more.)

★ if ~~dist~~ Length increases (of packets), then no. of collisions decreases.
i.e. if we have small sized packets, no. of contention slots increases.

TDM (Time Division Multiplexing) :-

★ In TDM, time is divided into slots & each slot is given to one station in a round robin manner.



$$\eta = \frac{\cancel{N} \times T_t}{\cancel{N}(T_t+T_p)} = \frac{1}{1+a}$$

★ If $T_t = 1ms$, $T_p = 1ms$, then what is the η? ~~η~~ in TDM :-
η = 50%

★ If B/w = 4 Mbps, then what is B/w utilization?
→ 2 Mbps.

★ If every station wants 1 Kbps, then how many stations can be placed in the LAN at max.
→ 2000.

Cosmos(Sajal) @ Techbits

Date

29.09.12

Q1.(i) In a TDM n/w if $T_p = 2ms$ & $T_t = 1ms$, then what is the efficiency? (33.33%)

(ii) If B/W = 3Mbps, then eff. b/w.

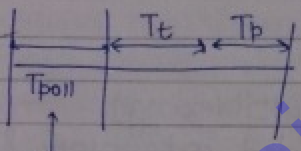
(iii) If every station needs 1 Kbps, then how many stations?

Ans.(i) 33.3%

(ii) eff. b/w = 1 Mbps

(iii) no. of stations = $\frac{1 \text{ Mbps}}{1 \text{ Kbps}} = 1000$

★ –



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

time taken by algo to decide which station to transmit next

Note:- If T_p is not given, then consider it as zero.

★ Delays :-

→ 10 bit time

it means that the time it takes for 1st bit to reach the destn, we can transmit 10 bits.

Cosmos(Sajal) @ Techbits

Token passing in Token ring:-

- **Bit Delay:-**
  If time is given in bits, we can convert into seconds by dividing with b/w,
  b bit delay indicates the time taken to transmit b bits.
  Conversions:-

- $$\begin{tikzcd}\text{bit delay} \arrow[r, "\text{divide by b/w}"'] & \text{delay (in sec.)} \arrow[l, bend right, "\text{multiply by b/w}"']\end{tikzcd}$$

- $$\begin{tikzcd}\text{delay (in meters)} \arrow[r, "\text{divide by velocity}"'] & \text{delay (in sec.)} \arrow[l, bend right, "\text{multiply by } v"']\end{tikzcd}$$

- **Ring Latency:-**
  It is the time taken by a bit to go around the ring & return to the same point

ring latency $= \frac{d}{v} + \frac{N \times b}{B}$ sec.

$= \frac{d}{v} \times B + N \times b$ bits

d:- total length of the wire
v:- velocity
N:- no. of stations.
B:- Bandwidth
b:- bit delay at each station (i.e. it takes for each station to transmit the bit back to the wire).

Cosmos(Sajal) @ Techbits

Time taken for the token to come back to its initial position:-

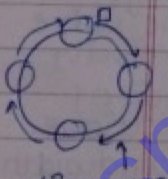
(i) Time taken for 1 station to hold the token:-
time taken for all the bits of that station to come back to the sender station = $T_t + T_{RL}$

T_t → transmission time

T_{RL} → Ring Latency

(ii) If we assume all stations are willing to transmit, then:-
time taken for all stations to hold it = $N \times (T_t + T_{RL})$

(iii) Now, token has to travel from one station to other station & come back to original position:-
= T_p (Propogation Time)
= $\frac{d}{v}$
d → ~~dis~~ length of the wire
v → velocity,



time taken for token to travel from one station to next along the wire (sum up all the time.)

So, total time = $N(T_p + T_{RL}) + T_p$
if $\boxed{b=0}$
∴ $N(T_p + T_t) + T_p$.

∴ efficiency = $\frac{\text{total transmission time}}{\text{total cycle time}}$

$$= \frac{N \times T_t}{N(T_p+T_t)+T_p} = \frac{1}{1+\left(\frac{N+1}{N}\right)a}$$

Cosmos(Sajal) @ Techbits

Delayed Token Reinsertion

In this strategy, data is transmitted & allowed to take a round & then removed & only after that token is released.
In this case, token holding time = $\boxed{T_t + T_{RL}}$

→ if ~~bit~~ we assume bit delay (b) = 0.
$T_{RL} = T_p \left(\frac{d}{v}\right)$

$\therefore \boxed{THT = T_t + T_p}$

→ Total cycle time :- is the time taken by the token to be seen by all the stations & coming back to the same point :=
$N \times (THT) + T_p$

→ Total Transmission time in this total cycle time = $\boxed{N \times T_t}$

$$\therefore \boxed{\eta = \frac{N \times T_t}{N \times (THT) + T_p}} = \boxed{\frac{1}{1 + \left(\frac{N+1}{N}\right)a}}$$

Early Token Time :-

In this strategy, a station will hold the token, & transmit the data & immediately release the time.

→ Token holding time = T_t

→ Total cycle time = $N \times T_t + T_p$

$$\therefore \eta = \frac{N \times T_t}{N \times T_t + T_p} = \boxed{\frac{1}{1 + a/N}}$$

Cosmos(Sajal) @ Techbits

Q1. If $T_p = 1\,ms$, $T_t = 1\,ms$, $N = 1$, then what is the efficiency in early & delay?

Ans. ~~In delay:~~

In early token reinsertion:-

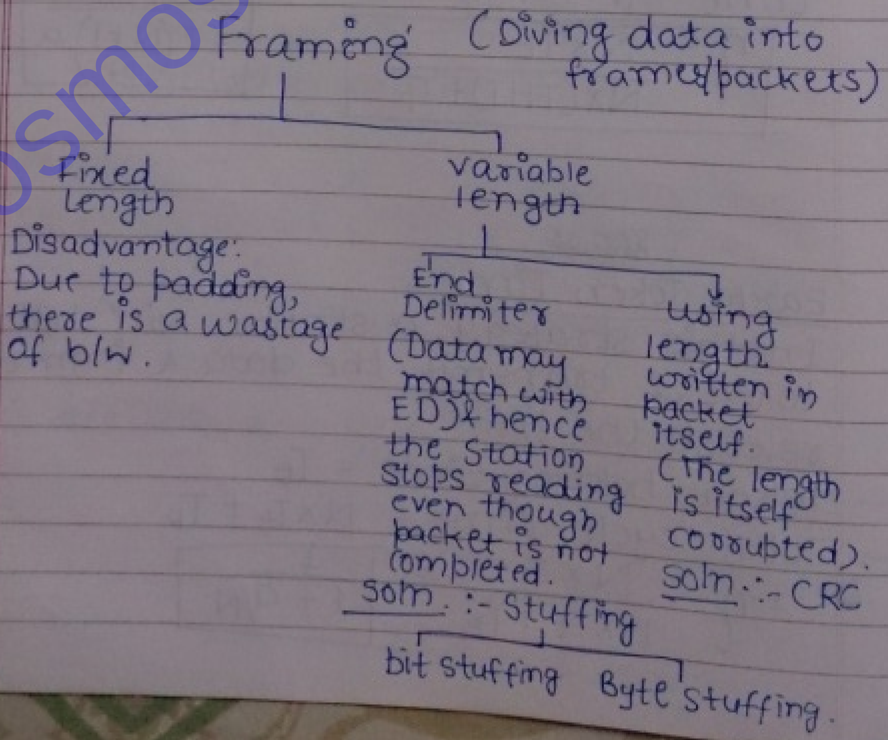
$$\eta = \frac{1}{1 + a/N} = \frac{1}{1 + 1/1} = 50\%$$

In delay token reinsertion:-

$$\eta = \frac{1 \times 1}{1 \times (1+1) + 1} = \frac{1}{3} = 33\%$$

Note:- Default strategy is early token reinsertion
Under heavy load condn. (when all are transferring data) early is better.

Framing (Diving data into frames/packets)



Fixed length — Disadvantage: Due to padding, there is a wastage of b/w.

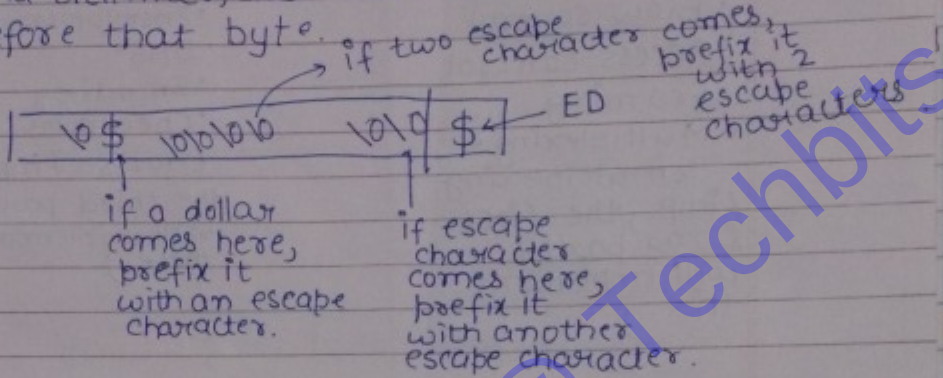
End Delimiter (Data may match with ED) & hence the station stops reading even though packet is not completed.
Soln. :- Stuffing

Using length written in packet itself. (The length is itself corrubted).
Soln. :- CRC

Cosmos(Sajal) @ Techbits

Byte Stuffing:-

Whenever data matches with the byte used for end delimiter, then add an escape character before that byte.


if two escape character comes, prefix it with 2 escape characters
\0$
\0\0\0\0
\0\0
$
ED
if a dollar comes here, prefix it with an escape character.
if escape character comes here, prefix it with another escape character.

if two dollar character comes, then prefix both of them with escape character.

\0$0\$.

☆ Byte stuffing is obsolete.

Bit Stuffing:-

if any pattern matches with end delimiter, then break the pattern by stuffing 1 bit

e.g.(i) ED = 01111

then add a 0 after 3 ones.

(ii) ED = 0111

Message = 01110110 0

Message sent = 01101011000

[add a zero after a 011, no matter whether sequence is 0111 or 0110]

Cosmos(Sajal)@Techbits

Functions of CN

- Error Control
- Flow Control
- Access Control
- Framing
- Multiplexing & Demultiplexing

(imp., the first & 2nd party will implement this.)

- Compression
- Encryption
- DNS
- Encoding
- Checkpoint

(not so imp., the third party will implement these.)

ISO-OSI :-

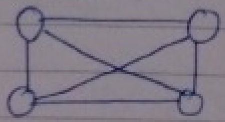
user ← { ~~Phy~~ Application Layer → user
Presentation " → optional
Session " → Thin
Transport " → Thick }

Interface ← N/W " → Complicated

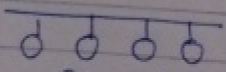
N/W ← { Data Link " → H/W & S/W
Physical " → Pure H/W }

Physical Layer :-

It deals with electrical, mechanical, procedural & functional characteristics of physical links.



Point-to-Point



Broadcast

will take care whether to add start delimiter (preamble).

Cosmos(Sajal) @ Techbits

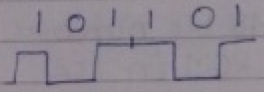
classmate
Date
Page

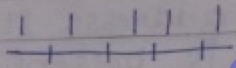
Modes of transmission :-

① Simplex e.g T.V. service provider
② Half Duplex e.g. HAM radio
③ Full Duplex e.g. Mobile Communication

Encoding :

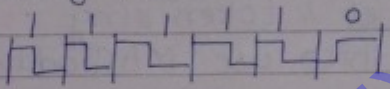
- Simple encoding :-



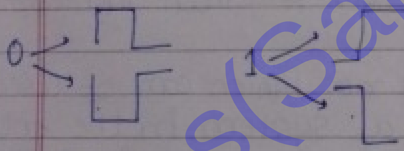


[unable to detect the no. of 1's.]

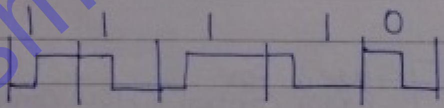
- Using Manchester encoding :-



- Using Differential Manchester :-



e.g.



2. **Data Link Layer :-**

(i) Flow Control :- Sliding Window Protocol
(ii) Error Control :- CRC
(iii) Access Control :- Alloha, Slotted Aloha, Polling, CSMA/CD
(iv) Framing :- putting SD & ED
(v) Physical Addressing

Cosmos(Sajal) @ Techbits

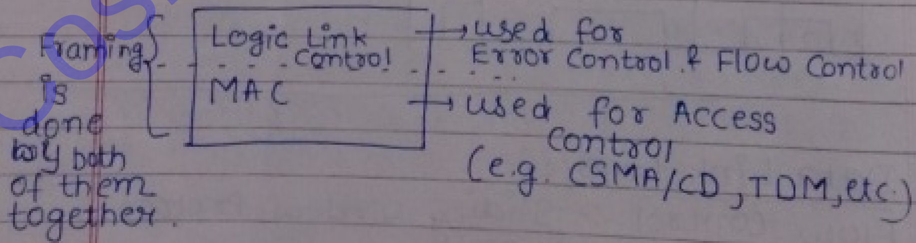
- Flow Control:-

Physical Address:- Any no. which can be used to identify a station uniquely in a LAN is called Physical address.

MAC address:- It is a 48-bit number which is present in the ROM in the NIC which is unique globally. MAC address can be used as physical address. e.g. ethernet & token ring are the LAN's which use MAC address as physical address.

Apple Talk is a LAN which uses randomly generated nos. as physical address.

Logical Address:- Any no. which can be used to uniquely identify a system in the entire world (or globally) is called Logical Address. e.g. IP address is used address in TCP/IP.


Framing is done by both of them together.
Logic Link Control
MAC
used for Error Control & Flow Control
used for Access Control (e.g. CSMA/CD, TDM, etc.)

Cosmos(Sajal) @ Techbits

Network Layer :-

- Routing
- Logical Addressing
- Congestion Control
- Fragmentation

Transport Layer :-

- End to End connectivity.
- Service point addressing
- Segmentation.
- Error Control
- Flow Control

→ Service point address :- any no. which can be used to identify a process uniquely within a host is called service point address, e.g. port number.

Session Layer :-

- Synchronisation / Checkpointing
- Dialog Control :-
  Even though the channel is full duplex, we use it as half duplex.
  e.g. web conference.
- Checkpointing :-

Cosmos(Sajal) @ Techbits

Presentation Layer

- Encryption
- Compression
- Translation
  (e.g. ASCII → EBCID)

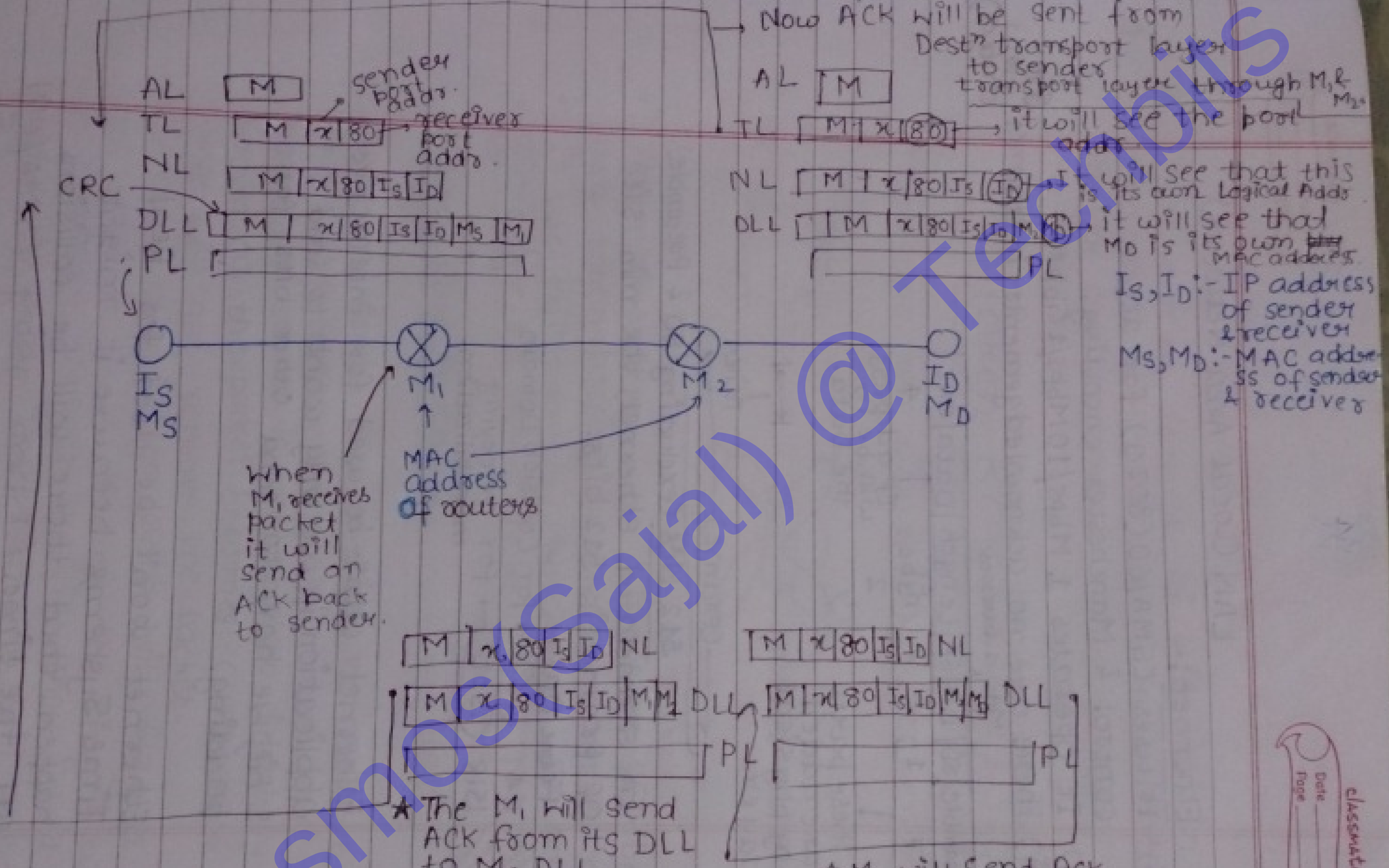
Mainly Session & Presentation layer functions are optional & not needed by all the applications ∴ these are implemented at Application Layer by the concerned application.

- Application Layer :- Message
- Transport " :- Segment
- Network " :- Datagram
- Data Link " :- Frame
- Physical " :- Single PDU.

☆ Diff. b/w flow control of Transport layer & Data link layer :-

→ Let assume if the packet is lost at M_2, though M_2 have sent Ack to M_1 depicting it has received the packet, but sender's transport layer runs a timer which times out if it doesn't receive Ack from receiver's transport layer.

Cosmos(Sajal) @ Techbits



Now ACK will be sent from Destⁿ transport layer to sender transport layer through M_1 & M_2.

it will see the port addr

It will see that this is its own Logical Addr

it will see that M_D is its own ~~by~~ MAC address.

I_S, I_D :- IP address of sender & receiver

M_S, M_D :- MAC address of sender & receiver

When M_1 receives packet it will send an ACK back to sender.

MAC address of routers

★ The M_1 will send ACK from its DLL to M_S DLL.

★ M_2 will send Ack from its DLL to M_1 DLL.

Cosmos(Sajal) @ Techbits

classmate
Date
Page

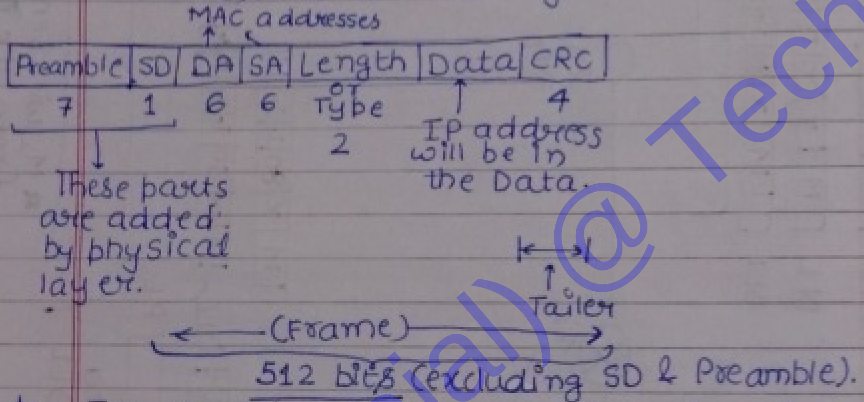
LAN (Local Area Network)

Ethernet:-

(i) It uses CSMA/CD (802.3) for access control & Manchester encoding.

(ii) It operates 1 Mbps/10 Mbps/1 Gbps.

(iii) There are no acknowledgements in ethernet. (no flow control)



MAC addresses

Preamble	SD	DA	SA	Length or Type	Data	CRC
7	1	6	6	2		4

These parts are added by physical layer.

IP address will be in the Data.

Tailer

(Frame)

512 bits (excluding SD & Preamble).

★ In standard ethernet, the min. size of frame is 512 bits.

	Frame	Data	
Min.	64	46	→ for Collision Domain
Max.	1518	1500	→ for removing monopilization.

?

★ Ethernet can't be used for interactive application, if we only want to send 1 bit, we have to send other bits for padding.

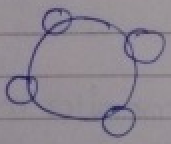
★ Ethernet won't be used for Real Time Systems because it might happen that there will be collisions all the time. (When using CSMA/CD)

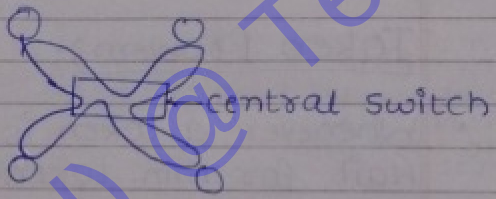
Cosmos(Sajal) @ Techbits

★ There are no concept of priorities in ethernet, so we can't use it in client-server architecture.

Token Ring (802.5) [not used for practical purposes.]

There are two diagrams for token ring:-





- Token ring operates at 4 Mbps or 16 Mbps, it uses token passing as access control method.
- It uses differential Manchester encoding.
- There are no ACK in token ring.

Token Ring Problem:-

1. When the sender is down & is not able to remove the packet from the ring.
2. When the sender is not able to identify the packet as the packet becomes currupted & hence will not remove the packet.

→ To solve this, Master comp. will flag a bit 1st time it passes through the ring & when it sees that bit set, it will know that the packet is doing 2nd round & will remove it.

Cosmos(Sajal) @ Techbits

	Sender	Receiver	
	Available	C	
• Initial bit pattern	0	0	→ Initial bit
• sender has sent, but receiver didn't receive .	1	0	check errors bit — if it is set, then packet is currobted — if not, then receiver might be busy.
• sender has sent & receiver has received	1	1	→ copied at sender
• sender has not sent & receiver has received .	0	1	→ Invalid

Token Problem :-

- Whenever a token is lost, monitor will wait for min. token return time to max. token return time.
- Min. token retuon time = RL (when no station transmits.)
- Max. token return time = Cycle time = R.L. + N(T.H.T.)

Monitor Problem :-

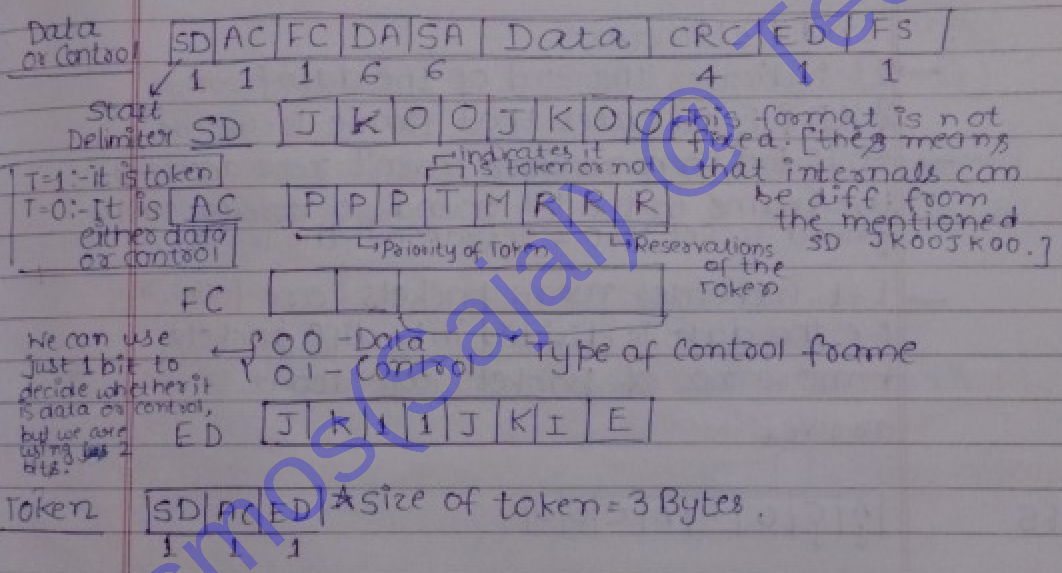
- When monitor itself is down or corrupted.
- Monitor should send AMP packet at regular intervals of time & if AMP packets are not received for sometime then all stations will conduct election & elect the next monitor.

Cosmos(Sajal) @ Techbits

30.09.12

- The s/w of a monitor could get corrupted & hack in such a way that monitor will be sending just AMP packet & will not do any other task.
- For this problem manual intervention is required.

Frame format (Token ring)



Data or Control

SD	AC	FC	DA	SA	Data	CRC	ED	FS
1	1	1	6	6		4	1	1

Start Delimiter SD

J	K	0	0	J	K	0	0

This format is not fixed. [this means that internals can be diff from the mentioned SD JK00JK00.]

AC

P	P	P	T	M	R	R	R

T=1:-it is token
T=0:-It is either data or control
indicates it is token or not
Priority of Token
Reservations of the Token
FC
00 -Data
01 - Control
Type of Control frame
We can use just 1 bit to decide whether it is data or control, but we are using ~~bas~~ 2 bits.

ED

J	K	1	1	J	K	I	E

Token

SD	AC	ED
1	1	1

*Size of token = 3 Bytes.

SD:-
Start Delimiter which indicates the beginning of a frame. J & K are line codes which are not used for any valid encoding.

AC :-
This byte is used for access control.
Even though a station has a token, it can't send the data because another station with high priority wants to send data.
M:- indicates that about to a stamp by monitor, if M=1, it indicates monitor has stamped on the packet(i.e. the packet has already made a round

Cosmos(Sajal) @ Techbits

around the ring & is now making a 2^{nd} round).
if M=0, then packet will be making its 1st round & monitor will stamp it to '1'.

Frame Control:-

End Delimiter:-

→ It indicates the end of the dataframe & ED & E indicates that frame is corrupted.

→ So if E=1, then receiver haven't ~~rece~~ accepted the frame in the 1st round, so ~~monitor~~ sender need to set M=0 & retransmit the packet.

→ I=1 indicates more packets are following. i.e. the data is divided into diff. packets & more no. of packets are about to arrive.

FS

A	C	0	0	A	C	0	0

Q1. Why two copies of A & C in FS?
Ans. Because FS is not included in CRC computation

Q2 Why FS is not included in CRC?
Ans. Because CRC is computed at sender & FS is computed/changed at receiver

Q3. If b/w of a token ring is 4Mbps & token holding time is 1 ms, then what is the max size of frame that can be sent

Cosmos(Saiaj) @ Techbits

Ans. ~~4×2^{29}~~ $\frac{4\times10^{6}\,bps}{\cancel{10}}\times 10^{-3}s$ $= 4\times10^{3}$ b
$= 4000$ bits

& max size of data $= 4000$ bits $- 21\times8$ bits
$= 500B - 21$
$= \boxed{479B}$

now for 16 Mbps
$16\times10^{6}\,bps\times10^{-3}s = 16\times10^{3}$ bits
$= 2000$ Bytes (of max frame size).

& max. data size = 1979 Bytes (2000 − 21).

★ Min. data size in token ring could be zero bytes (because there will not be any collisions).

$\boxed{\text{Capacity of a wire} = \text{Bandwidth}\times T_p}$

★ Now, min. length of the wire in token ring can be calculated using capacity of wire
A token ring should be capable of holding atleast 1 token, ∴ capacity ≥ token size.
∴ length ≥ 24 bits
$B/W \times T_p \geq 24$ bits
or $B * \frac{d}{v} \geq 24$ bits.

Q4 If a token is of 24 bits, b/w is 4 Mbps & velocity of signal in the wire is 2×10^{8} m/s, then what is the min. length of token ring

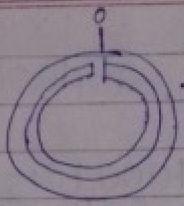
Ans. $\cancel{24}\times\cancel{10^{6}} * \frac{d}{\cancel{2\times10^{8}}\,10^{2}} \geq \cancel{24}\ 12$

$d \geq 1200\,m$

$1s \to 4\times10^{6}$
$10^{-6} \to 4$ bit 2×10^{8}m − 1s
4×10^{6} b → 1s   200m → [illegible]
$1b \to \frac{1}{4\times10^{6}}\times10^{6}$ $10^{-6}s$

Cosmos(Sajal) @ Techbits

classmate
Date
Page



- This means that atleast 1200 m of wire is req. for the 1st bit to reach the sender & last bit to be transmitted from the sender.
- If wire is less than 1200m, then the 1st bit will come back to sender even when the last bit is not transmitted & hence it will be an overlap & hence error takes place.

Q. If we have only 1 km wire, then what is the bit delay that has to be introduced in order to compensate 200m?

Ans. The time req to travel 200m = $\frac{\cancel{200}^{100}}{\cancel{2}\times 10^8} = 10^{-6}s.$

now, 4×10^6 bits takes 1s

$10^{-6}s$ will transfer 4 bits.

∴ 4 bits of buffer has to be introduced in b/w the wire.

Cosmos(Sajal) @ Techbits

Sender

Transport Layer

TCP (reliable)

Network Layer

IP (unreliable)

Receiver

★The main responsibity of n/w layer is switching.

★The transport layer will first send a notification to receiver telling about the ~~frames~~ packets that has to be arrived in future.

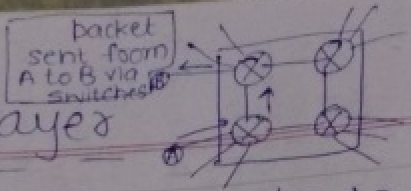
★The IP which is an unreliable protocol will fragment the packets & send them via the n/w, they may or may not arrive & many-a-times arrive out of order.

★In this case, the transport layer at receiver will send a +ve or -ve ACK about the data received & the transport layer at sender will send the packets if there was a -ve ACK.

The packets at receiver ~~will~~ can arrive -
- out of order
- currobted
- duplicated
- delayed

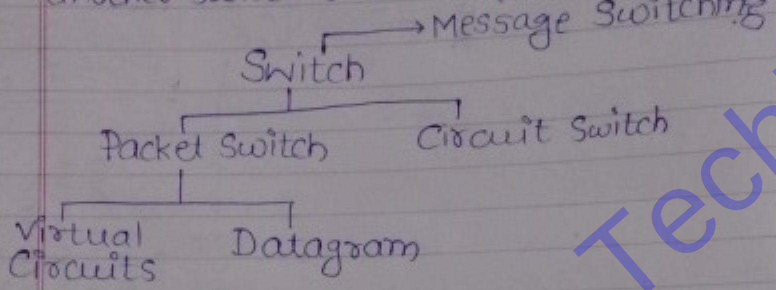
Cosmos(Sajal) @ Techbits

classmate Date Page



N/W Layer

★ To send data from one n/w to another switches are required.



Circuit Switching :-

Total time taken for a packet to be sent from sender to receiver:-

$$S + \frac{m}{B} + \frac{(x+1)d}{v} + T$$

S → time req. to set up the connection (i.e setting up of the wire path)

m → message length

B → B/w (time req. to put the message on the path.)

x → no. of switches

v → velocity

d → distance b/w two switches (time req. for packet to travel from sender to receiver)

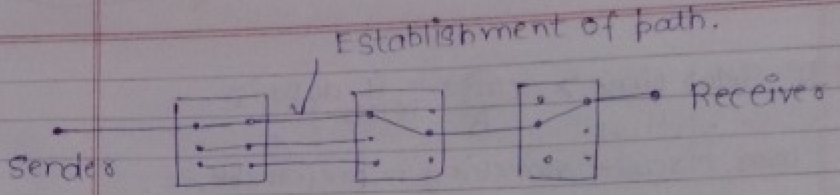
T → tear-up time (to tear up the path).

★ Header is only req. in Setting up time. when we need Sender & Receiver Address to switch & establish the path & header is no longer req. after that.

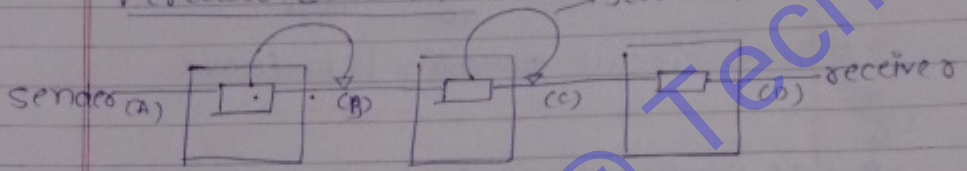
★ ~~We dont~~ The packets will arrive in-order because there is only one path.

★ Circuit switching is implemented at physical layer.

Cosmos(Sajal) @ Techbits



Virtual Circuits (ATM)



- ☆ Whenever the 1st packet goes, it will contain header with sender & receiver address & will establish a connection & will tell the routers to allocate reserve some part of buffers for the packets to be arrived in future.
- ☆ Header is req. only for the 1st packet & all the remaining packets will follow the same route.
- ☆ All the packets will take the same route.
- ☆ Out-of-order is not possible.
- ☆ If we have a connection-oriented service at network layer, we dont need connection-oriented service at transport layer.

because of store & forward

$$\boxed{(x+1)\frac{m}{B} + (x+1)\frac{d}{v}}$$

setup time & Tear-up time is negligible.

distance b/w one end of (B) to another end of (B).

velocity.

if we have x routers, then it will take $(x+1)\frac{m}{B}$ time to put on (A) & (B) & (C) & (D) combined together.

time req to put the message on (A) or (B) or (C) or (D).

there are (x+1) wires, ∴ time req is $(x+1)\frac{d}{v}$.

time req. to travel the packet from say one end of (B) to other end of (B).

Cosmos(Sajal) @ Techbits

★ If Setup time > $x\frac{\textcircled{m}}{B}$ → ie. if data is if less

then, virtual circuit ~~switching~~ is preferrable.

★ if setup time < $x\frac{m}{B}$ i.e. data is more

then circuit switching is preferrable.

★ If we have to send bursty data, then circuit switching is better.

★ If we have to send small amounts of data, virtual circuits are better.

Datagram Circuits (IP)

★ No resource reservation is done, i.e. buffers are not reserved for future packets

★ All packets contain header (as they may take diff. paths, so they must contain sender & receiver address for routers.)

★ Packets may or may not take same route.

★ No ~~reso~~ Reordering may be required.

Total time - $\boxed{(x+1)\frac{m}{B} + (x+1)\frac{d}{v}}$

★ It is unreliable, because it may discard the packets if the buffers are full.

Cosmos(Sajal) @ Techbits

32 bits

4 bits	4	8	16
Version	IHL	Type of Service	Total length
Identification (16)		▨ D F, M F	Fragmentation offset (13)
Time to live (8)		Protocol (8)	Header checksum (16)
Source Address (32)			
Destination Address (32)			
Options (0 or more protocol) Header			

20 Bytes

(0-40) Bytes.

IP header

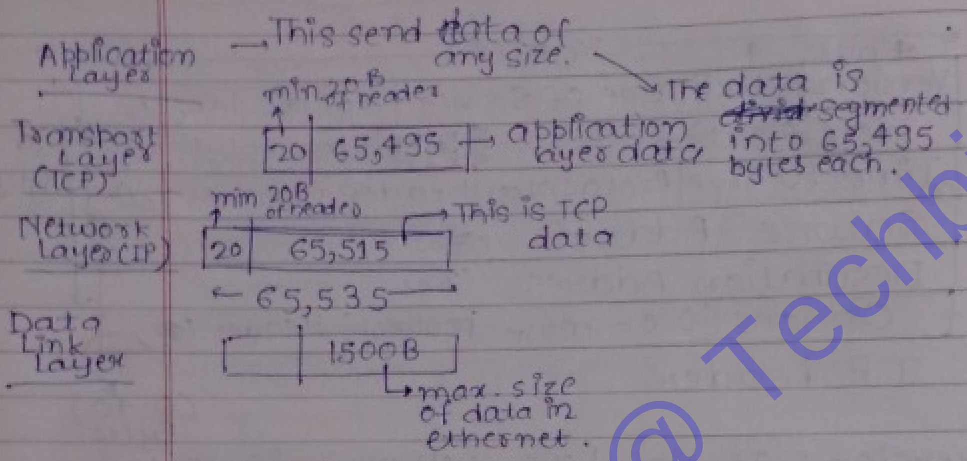
(i) Version :- It ~~gives~~ tells whether it is IPv4 or IPv6.

(ii) IHL (IP header length) :- 1 bit indicates 4 Byte length, because max. header size = 60B, & 15 bits are req. to represent them, ∴ each bit indicates 4B.
∴ IHL = 1010 means header is of 10×4 = 40 bytes.
This field indicates size of the header in terms of 4 bytes.

- if HL = 26, IHLF = 7
- if HL = 24, IHLF = 6
- if IHLF = 10, HL = 40
- if IHLF = 7, HL = 28.

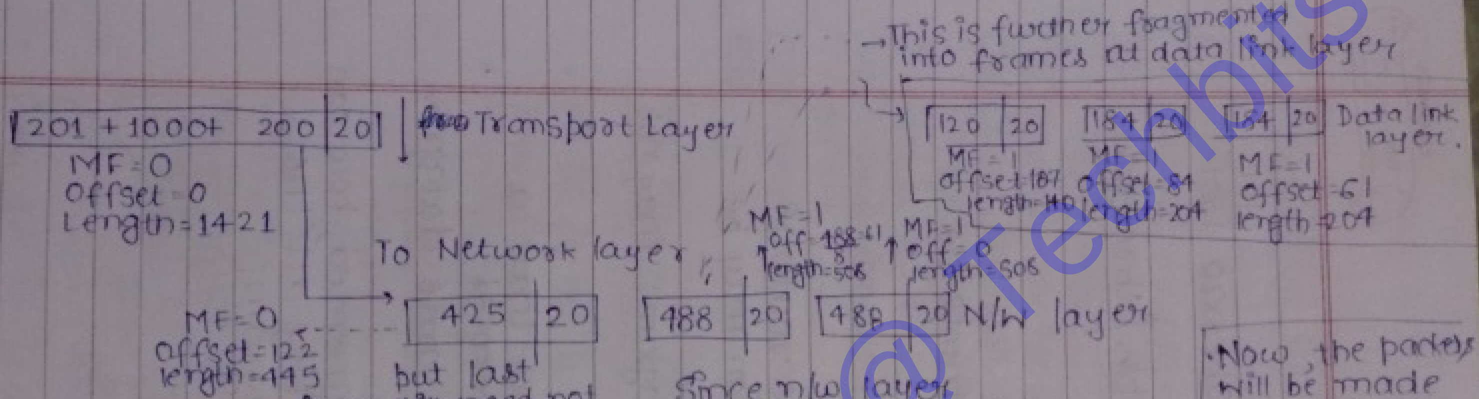
(iii) Total Length :- it is a 16 bit field which indicates total size of IP header + IP data which can be a maximum of $2^{16}-1$.

Cosmos(Sajal) @ Techbits



★ If we The max. no. that ~~[illegible]~~ can be put into offset is 65,514, ~~i.e.~~ when the last frame size is just 1B & 65,514 B is ahead of it,
so, we need to store 2^{16} B data in 13 bit field,
so using scaling $\frac{2^{16}}{2^{13}} = 8$.
so, take the actual

Cosmos(Sajal) @ Techbits



but last frame ~~bit~~ need not to be multiple of 8, as there is no frame after it, & hence its size wont be written in any frag. offset.

Since n/w layer has IP implemented in it, & IP has fragmentation offset of just 13 bits & the max size it can hold is 65,514, so we need 16 bits, but we have only 13 bits,

$$\frac{2^{16}}{2^{13}} = 8 \text{ bits, of frag. offset}$$

So 1 bits, will depict 8 bits of data.

∴ we have to divide the data in the multiples of 8 only.

- Now, the packets will be made in-order at receiver using offset no.

e.g, if we have

0 84 61 107

Overhead of fragmentation

1401+20 at transport layer at sender & at receiver we have 1401+20×5

.overhead =

1401+20×5−1401−20

= 4×20B

Cosmos(Sajal) @ Techbits

- Efficiency (η) =

$$\frac{\text{Total useful bytes}}{\text{Total bytes received}} = \frac{1401}{1401+5\times20} = \frac{1401}{1501}$$

- B/W utilization/effec. b/w / throughput :-

$\eta \times B/W$

Q. Where should the fragments be reassembled?

Ans. At the destination.

Q. Why not at immediate routers?

Ans. ① Further fragmentation may be required.

② Since, it is datagram service ~~every packet~~ datagrams may not take same route.

Q. How can a receiver know that a datagram is not fragmented?

Ans. If MF=0 & offset=0 for same datagram.

Q. If a datagram is fragmented, how can a receiver ~~underst~~ identify all the fragments of a datagram?

Ans. Identification no.

	MF	off
not fragmented ←	0	0
first fragment ←	~~0~~ 1	0
last fragment ←	0	10
intermediate fragment ←	1	!0

Cosmos(Sajal) @ Techbits

Reassembly Algorithm:-

(i) Identify that the datagram is fragmented (MF≠0 , or, Offset ≠0 , or, both ≠ 0) .

(ii) Collect all the fragments having same identification no.

(iii) Identify the 1st fragment (offset = 0)

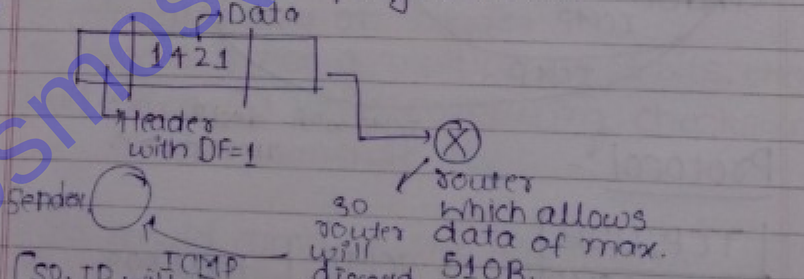
(iv) Count the no. of data bytes in that fragment (Total length - Header Length) . Divide it by 8. (Let it be x).

(v) Search for the fragment having x as its offset.

(vi) Repeat the above two steps until MF = 0.

DF (Do not fragment)

- If DF is set, it indicates that the datagram should not be fragmented.
-



so router will discard it & send an ICMP packet to sender telling about the discard.

(the datagram need to be fragmented, but DF = 1, so it will not be fragmented)

[So, IP with ICMP is reliable?]

- Why IP is still unreliable even with the support of ICMP?

Ans. Because if ICMP is discarded/lost, then no ICMP for it is generated.)

Cosmos(Sajal) @ Techbits

Time to Live:

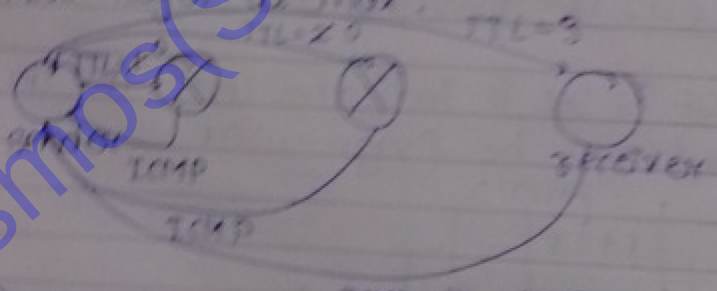
- It is used to prevent a packet from infinite looping.

This two

→ tracert www.google.com
in cmd

Tracert will give all the intermediate routers b/w a source & a destination.

→ Keep incrementing TTL until we get ICMP packet with destination unreachable message (when we give wrong port no.) & port no. will be read by transport layer, & intermediate routers won't be able to read because it has N/w layer at max.



ICMP with destn unreachable.

Protocol:

TCP, UDP
ICMP, IGMP IP

1 - ICMP
2 - IGMP
6 - TCP
17 - UDP

→ these nos. will tell IP is carrying which protocol.

Cosmos(Sajal) @ Techbits

classmate
Date
Page

Checksum

0000 0001 | 0001 0001 | 00011000 | 11010101

1   17   24

add them together

1+17+24 = 42

$(42)_{10} = (00101010)_2$

now take its 1's complement

$(11010101)_2$

append it to the data

now, sum up these

```
  00101010
  11010101
  --------
  11111111 ← all 1's (so no error)
```

★ It is called header checksum because checksum is calculated only on header.

★ If header is not a multiple of 16 bits, then we pad extra 0's while computing checksum but we will not transmit it.

Q. Who should compute the checksum?

Ans. ① Senders, Receivers
② All the routers on the way

Q. Why should routers calculate checksum?

Ans. Because TTL changes at each router & some other fields like offset, MF, Total length & Options may change at the routers.

Cosmos(Sajal) @ Techbits

NID	HID	
valid	valid	→ IP
"	all 0's	→ NID
"	all 1's	→ Direct broadcast addre
all 1's	all 1's	→ Limited "
all 0's	valid	→ Host within a n/w
all 0's	all 0's	→ I dont have IP.
127	!0, !1	→ loopback.

★ Ping 127.0.0.1

★ Ping 127.0.0.0 }
127.255.255.255 } ?

Cosmos(Sajal) @ Techbits

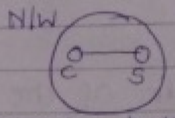
Date

10.11.12

ARP (Address Resolution Protocol)

It is used to find out the physical address of machine whose IP address is already known
We have 4 cases where ARP is used :-

Case 1:

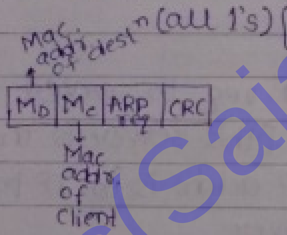


• when both client & server are in same ~~ch~~ n/w.

To check whether they are in same n/w, we check the subned id of client acc. to client & subnet id of server acc. to client (when both subnet id are same, they are in same n/w)
When both client & server are in same n/w, client will forward message directly to server in a frame. For this client has to find out physical address of the server & so it generates ARP request

ARP Note:- ARP request is always broadcasted at data link layer.
ARP reply is always unicasted.

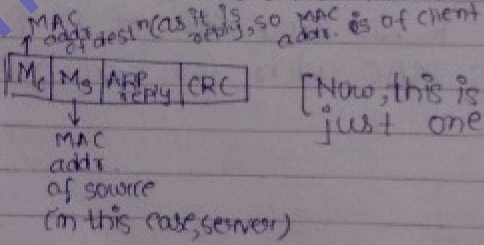
1.



[so it is broadcasted to all nodes in the n/w along with router]

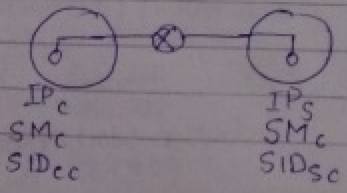
2 The node having the IP addr. of destn. will accept it & put its MAC addr. in ARP reply.

3.


MAC addr of destn (as it is reply, so MAC addr. is of client
M_c
M_S
ARP reply
CRC
MAC addr of source (in this case, server)

[Now, this is unicasted to just one node.]

Case 2:-



When subnet id of client acc. to client ≠ Subnet id of server acc. to client [then client & server are in diff n/w.]

Cosmos(Sajal) @ Techbits

classmate
Date
Page

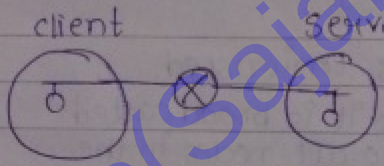
In this case frame has to be 1st forwarded to the router, ∴ client should find out MAC addr of the router

Note :- Any broadcast message at DLL can never cross n/w boundaries.

So, to obtain the MAC addr of the router the ARP req. is broadcasted, & the router will reply with its MAC addr.

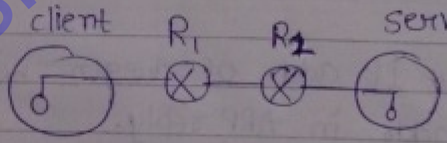
→ Though the default router is same always, but being so much loaded with traffic, so NIC cards are changed many-a-times ∴ we need to send ARP req. periodically.

Case 3 :-



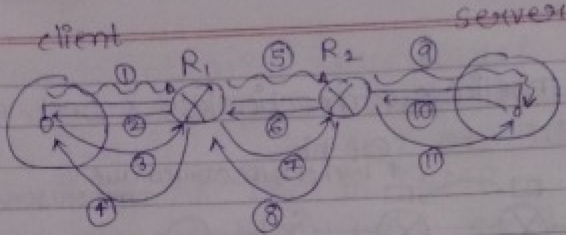
when router will send a req. to server to know its MAC address. [this server is the ultimate $dest^n$ whose IP addr. is in IP packet.]

Case 4 :-



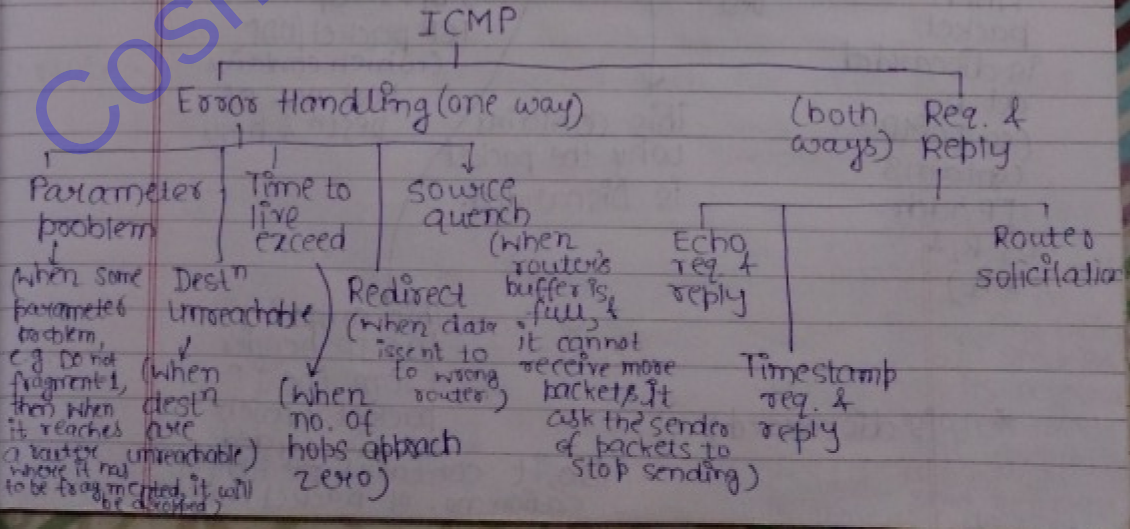
when router R_1 will send ARP req. to R_2 to know its MAC addr. for next hop.

Cosmos(Sajal)@Techbits



① ARP req. to next router R_1 for its MAC addr.
② ARP rep from R_1 along with its MAC addr.
③ Data sent to buffers of R_1.
④ Ack sent back to client from R_1.
⑤ R_1 send ARP req. to R_2 for its MAC addr.
⑥ R_2 send ARP reply to R_1.
⑦ Data sent to buffers of R_2.
⑧ Ack sent to R_1
⑨ R_2 send ARP req. to server for its MAC addr.
⑩ server send its MAC addr. to R_2 via ARP reply.
⑪ Data sent to server from R_2.

★ ICMP :- It is a n/w layer protocol. It is used for
★ error handling & feedback messaging at n/w layer. (It doesn't use any protocol at transport layer.)

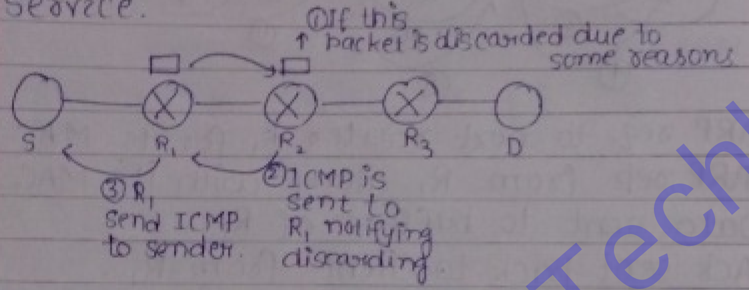

ICMP
Error Handling (one way)
(both ways) Req. & Reply
Parameter problem
(when some parameter problem, e.g. Do not fragment 1, then when it reaches a router where it has to be fragmented, it will be dropped)
Dest^n unreachable
(when dest^n are unreachable)
Time to live exceed
(when no. of hops approach zero)
Redirect
(when data is sent to to wrong router)
source quench
(when router's buffer is full, & it cannot receive more packets, it ask the sender of packets to stop sending)
Echo req. & reply
Timestamp req. & reply
Router solicilation

Cosmos(Sajal) @ Techbits

★ For both TCP & UDP, ICMP packets will be generated.

classmate
Date
Page

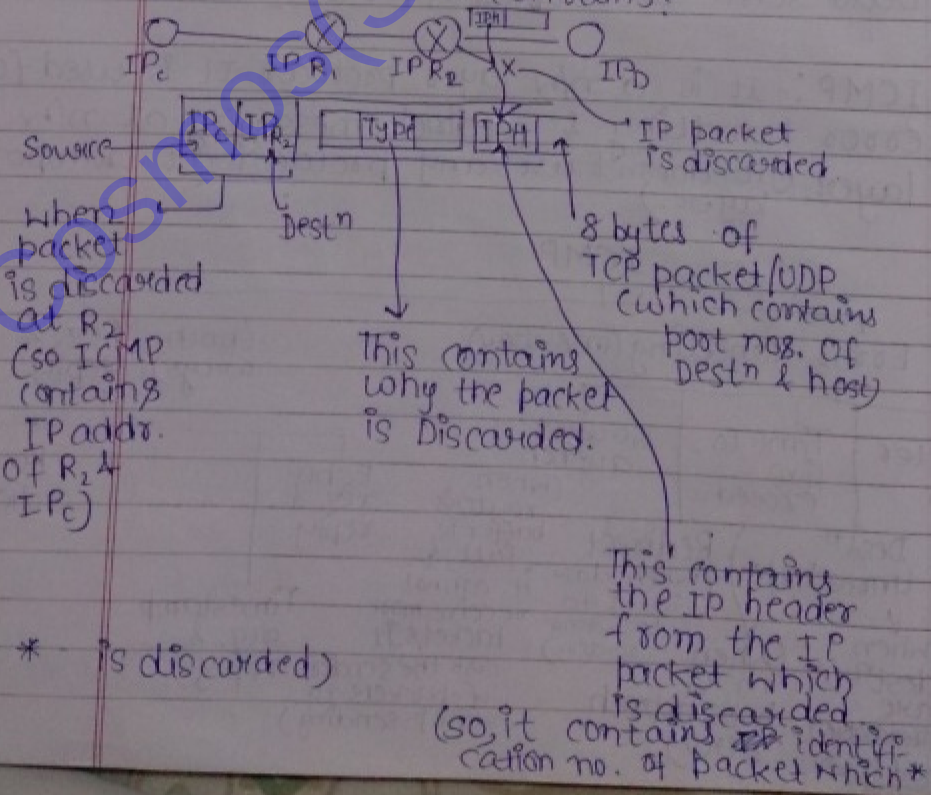
★ IP is unreliable, connectionless & best effort service.


①If this packet is discarded due to some reasons
S
R1
R2
R3
D
③R1 send ICMP to sender.
②ICMP is sent to R1 notifying discarding

★ Though IP send ICMP packets, but still it is unreliable, because if ICMP itself is lost, no ICMP's are generated for it.

Trace Route :-

→ What the ICMP contains?


IPH
IPc
IPR1
IPR2
X
IPD
IPc
IPR2
Type
IPH
Source
Destn
IP packet is discarded
where packet is discarded at R2 (so ICMP contains IP addr. of R2 & IPc)
This contains why the packet is Discarded.
8 bytes of TCP packet/UDP (which contains port nos. of Destn & host)
This contains the IP header from the IP packet which is discarded
(so, it contains ~~IP~~ identification no. of packet which*
* is discarded)

Cosmos(Sajal) @ Techbits

classmate
Date ______
Page ______

How to obtain trace route?

① First send a packet with TTL = 1, so R_1 will discard it & will send an ICMP packet specifying the IP_{R_1} in ICMP.

② Now, increment TTL by 1, so R_1 will forward it to R_2, & R_2 will discard it & send ICMP to ~~R1~~ Client via R_1 (specifying its IP_{R_2}).

③ Now, increment TTL by 1, so TTL = 3, & it will reach the Destⁿ, no ICMP will be sent, in this case, we specify destⁿ port no. as one which is wrong, so destⁿ will send a destⁿ unreachable ICMP to sender.

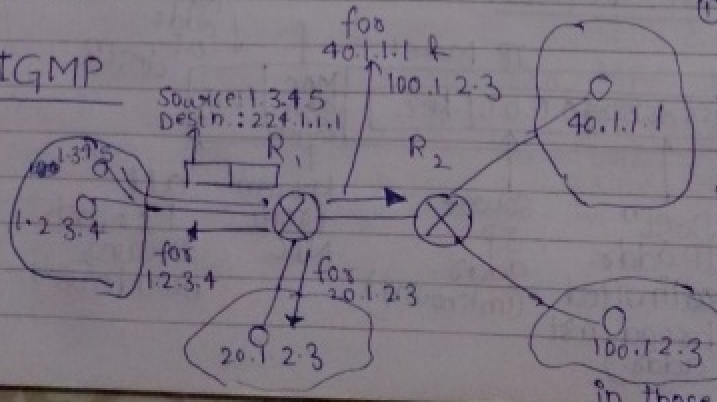
Algo for Traceroute:-

① Generate a UDP packet (UDP is used because header size of UDP is only 8 Bytes.) with TTL as 1 & keep incrementing TTL till we get destⁿ unreachable message.

Note: UDP packet must be sent to a port which doesn't exist

Note:- ICMP will be generated both for TCP as well as UDP.

IGMP



① R_1 will see its routing table for the group ID, but when it doesn't found it in its routing table it will send ask its neighbou routers abou the group ID & then will send the packet in those diff directions.

Cosmos(Sajal) @ Techbits

classmate
Date
Page

Class D is used for Group messages

(i) Can create a group.
(ii) Can join the group.
(iii) Can unjoin the group.
(iv) Transfer info. about the groups to all the routers.

GID:224.1.1.1

1.2.3.4
20.1.2.3
40.1.1.1
100.1.2.3

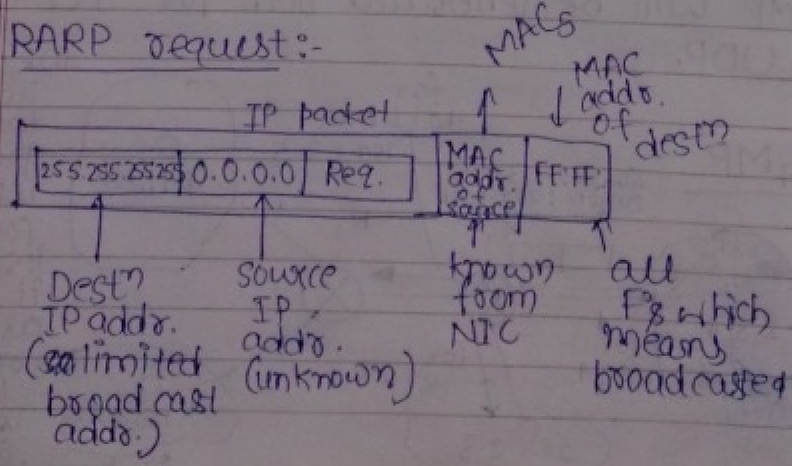
★ 256 million (2^{28}) Class D addresses are reserved for group id's, but till date we are using only few thousands of groups.

Cosmos(Sajal) @ Techbits

RARP

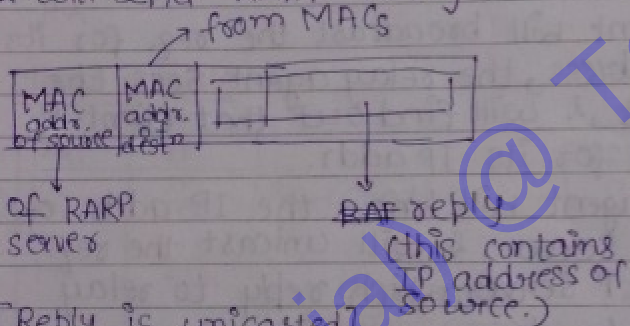
→ When the source doesn't know the IP address of itself, so it ask the RARP server about its IP address.

RARP request:-


MACs
MAC addr. of destn
IP packet
255.255.255.255
0.0.0.0
Req.
MAC addr. of source
FF:FF
Destn IP addr. (limited broadcast addr.)
source IP addr. (unknown)
known from NIC
all F's which means broadcasted

This req. is seen by all nodes in the same n/w, the router will not allow it to leave the n/w.

→ The RARP server finds out that its a RARP req & consult its table.
The table will have an IP address of source corresponding to source MAC addr.
& will send RARP reply.



MAC	IP
MAC,	IP,
MACs	IPs

RARP server table.

[Reply is unicasted]
[Request is broadcasted]

Problem:-

① Don't know my IP address (so ~~$~~ IP_{source} = all 0's)
② Don't know whom to ask (so IP_{Dest^n} = all 1's)
& MAC_{Dest^n} = all 1's)

★ Disadvantage of RARP:-

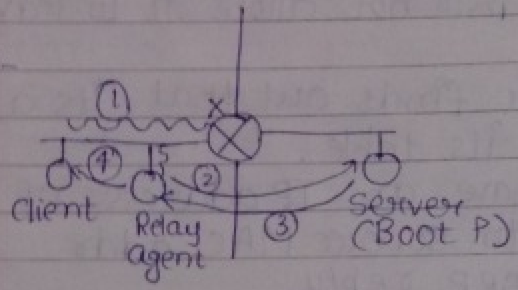
- If there are sub n/w in the same n/w, then we must have RARP server for each sub n/w.
- The table of RARP server is static, i.e. one IP addr. for a particular MAC address. (So, if we have 200 machines; then we need 200 IP addresses). [if we have ~~only~~ 100 machines working at a time, then we need only 100 IP address]
- We should have RARP server in all n/w.

no. of IP ≥ ~~no.~~ of machines

Cosmos(Sajal) @ Techbits

- RARP is obsolette.

BOOTP:-



The client will broadcast the req. for its IP address, the relay agent sees the request, & will find out that client is asking for its IP addr.
Relay agent will know the IP addr. of Boot P Server & will unicast the req. to Boot P Server, which reply to relay agent, & relay agent will unicast the reply to client.

Advantage:-

- For a large no. of n/w, we can have only one Boot P server.

Disadvantage:-

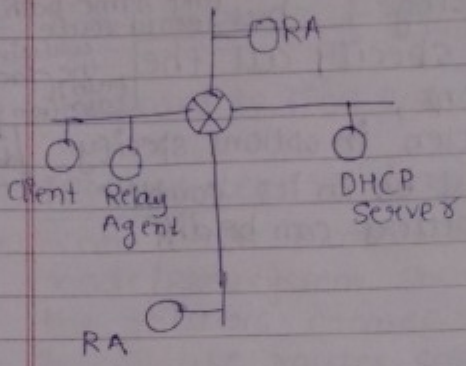
- The Boot P server table is static.

Format:-

DHCP (Dynamic Host Configuration Protocol)

Cosmos(Sajal) @ Techbits

classmate
Date
Page

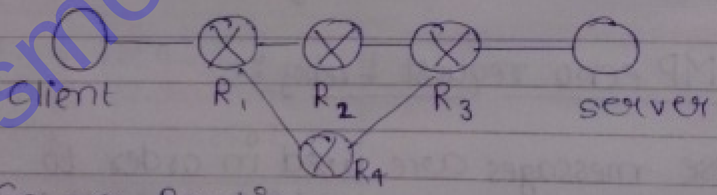


Mapping table:-

MAC	IP
M_1	IP_1
M_2	IP_2
M_K	IP_K

→ Static [static IPs are assigned to various servers.

→ dynamic (~~also~~ this contains pool of IP addr, whenever a machine asks for IP addr, it will be allocated to that machine with a particular lease period.)



- Source Routing:-

When at the source site, the route to the dest^n is fixed.

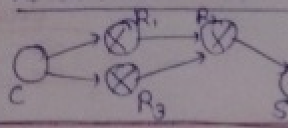
→ Strict Source routing:-

when the complete route is mentioned in the Options field of IP.

- Max. no. of IP addr. that can be specified in options field is 9. (as options is 40 bytes max. ∴ 40/4 = 10, but 4 bytes are used for inter gap b/w 2 IP).

Cosmos(Sajal) @ Techbits

Record Route is diff from Trace route :-



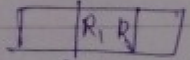
TTL = 1, to R_1 then to
TTL = 2, to R_3 & R_2

[Trace routes doesn't alway take same path.] but record route will give the exact path it taken from source to dest.

Loose Source Routing :-

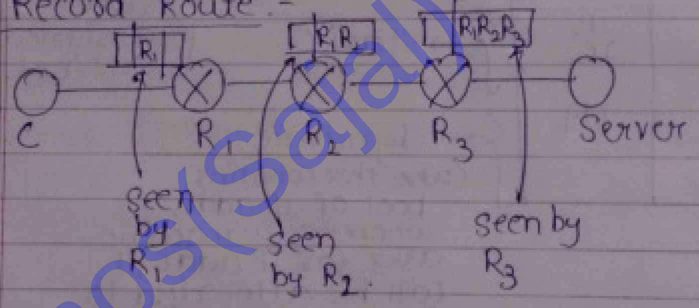
When we doesn't specify all the routers in options,
the routers written in options specify those routers must be in its complete path, the other routers can be diff.

e.g.



now intermediate can be R_2 or R_4.

Record Route :-

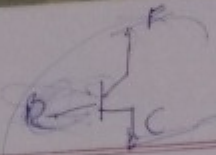


but we need trace route, because record route is not received by source.

ICMP echo request & reply :-

- These messages are used in order to test whether the n/w layer of the destn & all the routers on the way are working or not.
- Ping ~~users~~ uses echo request & reply.

Cosmos(Sajal) @ Techbits



Timestamp req. & reply :-

- It is used to find out time as well as delays.

ICMP router Solicitation:-

- When a n/w is connected to many routers, a node/~~[illegible]~~system should know what are the routers connected to the n/w, for this it will use router solicitation req. & all the routers will reply to this request.

ICMP router advertisement :-

- Whenever any new router come up, everyone should know about it & so the router advertises itself.

Special IP address (127.)

★ To check whether the sender's NIC is working properly, we use loopback address.

★ 127 is loopback addr. which is used to test self connectivity.

Ping 127.0.0.1 ✓
Ping 127.0.0.0
Ping 127.255.255.255

	S.A.	D.A.
Data	1.2.3.4	127.0.0.1

↳ other than
127.0.0.0
or
127.255.255.255

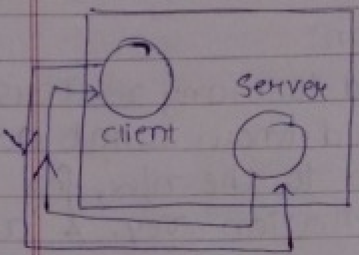
★ if we write S.A. & D.A. same, then the packet will go to the router & then come back to same machine.

★ interprocess comm. within the same machine.

Cosmos(Sajal) @ Techbits

classmate
Date
Page

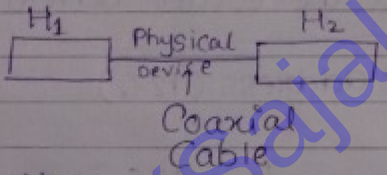
* In order to test client & server, which are running on same machine, we use special address 127.

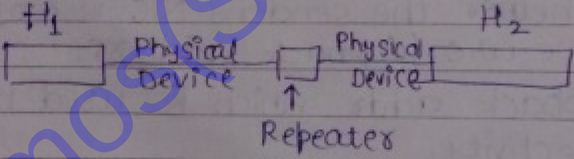


← on same machine.

Hardware in Comp. N/W (Devices)

1 Coaxial Cable:-

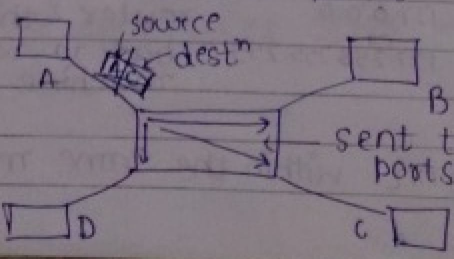




Repeater is used to decrease attenuation when coaxial cable is too long.

2. Hub:-

- Hub is multiport repeater.
- It is a pure electronic device with no S/W associated with it.



sent to all ports except from where it came.

Cosmos(Sajal) @ Techbits

Disadvantage of Hub:-

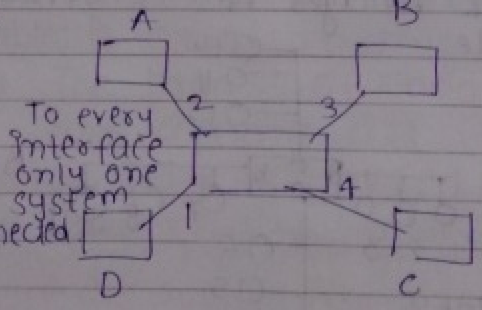
- It doesn't have a lookup table,& ~~[illegible]~~ ∴ it will have a lot of traffic.
- Collisions are possible inside a hub because it is not store & forward device, ∴ collision domain doesn't change.
- Hub has only physical layer, it doesn't have DLL or NL.
- If a device has to stop broadcasting done
- The broadcast domain is also not changed in hub because it has only physical layer.

Switch :-

- Switch is an active device (~~[illegible]~~ s/w), using the s/w a switch will construct lookup table. A Switch is a store & forward device

lookup table

MAC	interface
A	2
B	3
C	4
D	1



To every interface only one system is connected

★ Switch contains Physical layer & data link layer.
★ Doesn't contain n/w layer.

- Since, switches have a lookup table, the traffic will be less.
- Since, Switch is a store & forward device, there will be no collision. ∴ (collision domain is used.)

Cosmos(Sajal) @ Techbits

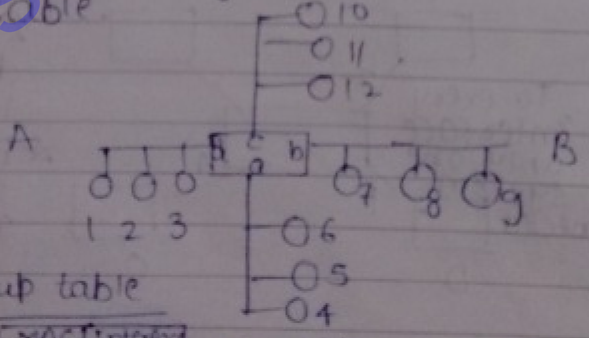
- It Will not stop the broadcasting done at data link layer because switch doesn't contain n/w layer.

Disadvantage:-

- Switch is 4-5 times costlier than hub.

Bridge :-

- Bridge is a switch with less no. of ports. It is used to connect many LANs (instead of system)
- Bridge contains physical layer & data link layer
- Broadcast domain is not changed by a bridge because it doesn't contain n/w layer
- Colision domain is decreased because it is store & forward device
- Even bridges will construct lookup table



lookup table

MAC	Interface
1	a
2	a
3	a
.	
.	

- but if we move ③ from A to B, lookup table becomes

Cosmos(Sajal) @ Techbits

- Bridge will perform 3 tasks:-

(i) Forwarding :- take a packet & send to other interface.

(ii) Filtering- when both source & dest^n are on same n/w, the packet will be filtered.

(iii) Fill the lookup table.

Router :-

- Router is a device which is used to connect various n/w or subnets.
- Router will contain physical layer, DLL, & n/w layer.
- Router is a store & forward device.
- Broadcast domain & collision domain are reduced. by routers.
- Responsibilies of routers are :-

(i) Forwarding.

(ii) Filtering

(iii) Routing.

- Routing :- The process of preparing the routing tables is called routing.
- Forwarding :- The process of choosing one outgoing links among all the available outgoing links is called forwarding.

[if the device have routing table, forwarding means choose one interface among all, but if the device doesn't have routing table forwarding means send to all the interfaces except from which it comes, also known as flooding.]

- Advantages of flooding :-

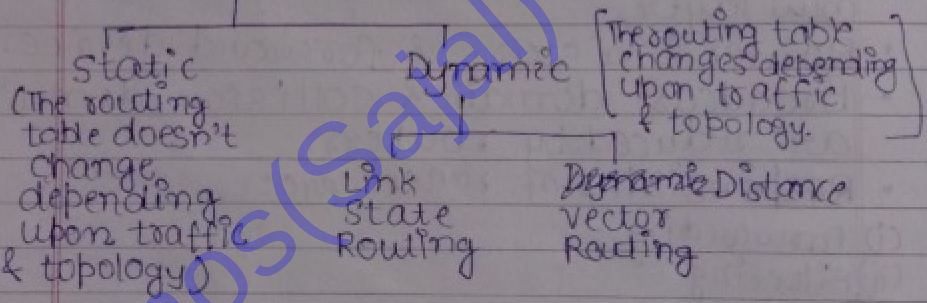
Cosmos(Sajal) @ Techbits

- High reliability (packet delivery is guaranteed even if there is atleast one path.)
- ~~V~~ Shortest path is guaranteed (always the 1st packet is the one which has taken shortest path.)

Disadvantages:-

- Lot of traffic & duplicate packets are generated.

Routing algorithms



Static

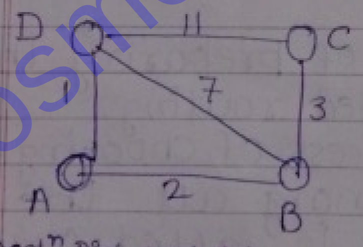
(The routing table doesn't change depending upon traffic & topology)

Dynamic

[The routing table changes depending upon traffic & topology.]

Link State Routing

~~Dynamic~~ Distance Vector Routing



At A

Destⁿ	Dist	Next Hop
A	0	A
B	2	B
C	∞	—
D	1	D

Distance vector

At C

Destⁿ	Dist	Next Hop
A	∞	—
B	3	B
C	0	C
D	11	D

At B

Destⁿ	Dist	Next Hop
A	2	A
B	0	B
C	3	C
D	7	D

At D

Destⁿ	Dist	Next Hop
A	1	A
B	7	B
C	11	C
D	0	D

Cosmos(Sajal) @ Techbits

classmate
Date
Page

- In the 1st step, create the routing table for all the routers (when they know only about their adjacent neighbours.)

Step 2:- All the nodes will exchange distance vectors with their neighbours. At every node new routing table will be constructed using the new information from neighbours.

At C:-

length of Shortest path of max. edge 1

A	∞	−
B	3	B
C	0	C
D	11	D

from B (distance vector)

A	2
B	0
C	3
D	7

from D (distance vector)

A	1
B	7
C	11
D	0

new routing table:-

length of Shortest path of max. ~~hops~~ 2 edge

A	5	B
B	3	B
C	0	C
D	10	B

C to A = { C→B to A = 3+2=5 ✓
C→D to A = 11+1=12

C to B = { C→B = 3 ✓
C→D→B = 11+7 = 18

C to C = 0

C to D = { C→D = 11
C→B→D = 3+7 = 10 ✓

At A

A	0	A
B	2	B
C	∞	−
D	1	D

A	2
B	0
C	3
D	7

from B

A	1
B	7
C	11
D	0

from D

Cosmos(Sajal) @ Techbits

45
×7
315

new table

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

$A \to B = \begin{cases} 2 ✓ \\ A \to D \to B = 1+7=8 \end{cases}$

$A \to C = \begin{cases} A \to D \to C = 1+11=12 \\ A \to B \to C = 2+3=5 ✓ \end{cases}$

$A \to D = \begin{cases} A \to B \to D = 2+7=9 \\ A \to D = 1 ✓ \end{cases}$

- Even though we have calculated new routing table for C in Step 2, we will use old routing table of C in this step & will use the new table in step 3. [the step 2 will complete when new routing tables for all routers will be made.]

★ Compute Step3 similarly.

Other method:-

At A

A	0	A
B	2	B
C	∞	—
D	1	D

from B

2
0
3
7

AB = 2

from D

1
7
11
0

AD = 1.

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

Cosmos(Sajal) @ Techbits

classmate
Date
Page

3rd method: from diagram (do directly).

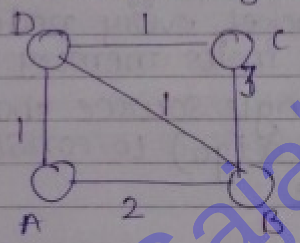
at ~~A~~D (final routing table).

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

Q. In the above question, how many edges are not used?

Ans. 2 (CD & BD).

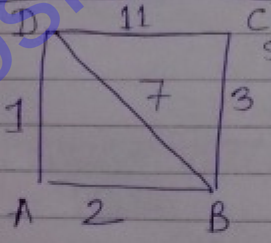
Q. If those unused edges are ~~made~~ changed to 1.



only BC is not used.

★ Disadvantage of Distance Vector Routing is count-to-infinity.

Link State Routing :-



Step1: Every node will construct link state packets using local knowledge (knowledge about the neighbours)

Step 1:- Link State packet at A:-

Seq No.	
Age	
B	2
D	1

at B:-

Seq No.	
Age	
A	2
C	3
D	7

at C:-

Seq No.	
Age	
B	3
D	11

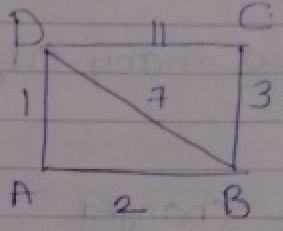
at D:-

Seq No.	
Age	
A	1
B	7
C	11

Cosmos(Sajal) @ Techbits

Step 2:- All Link state packets will be flooded to all other nodes.

At B:- B will get link state packet from A,C,D (adjacent neighbour)



[B will know the topology of the entire n/w & similarly other nodes will know about the entire topology.]

Step 3:- Using link state packet, every node will construct a graph in its memory. Every node will apply single source shortest path (or Dijkstra algo) to construct the routing table

★ In link state routing, there is no count-to-infinity problem.

Cosmos(Sajal) @ Techbits

Date

11.11.12

Gateways

Gateways

It is a connecting device which has all the 5 layers & so a gateway is capable of Deep Packet Inspection(DPI) i.e. at gateway we can even look into the application layer.

Transport Layer:-

- Main responsibility of transport layer is end-to-end connectivity.
- If N/w layer is providing unreliable & connectionless service, then transport layer should provide reliable connection oriented service. Two popular protocols used at Transport layer:

(i) TCP
(ii) UDP

TCP

Header Format:-

<table>
<tr><td colspan="4">Source Port address
(16 bits)</td><td colspan="5">Destination port address
(16 bits)</td></tr>
<tr><td colspan="9">Sequence Number(32 bit)</td></tr>
<tr><td colspan="9">Acknowledgement Number (32 bit)</td></tr>
<tr><td>Header length
(4 bits)</td><td>Reserved
6 bits</td><td>U R G</td><td>A C K</td><td>P S H</td><td>R S T</td><td>S Y N</td><td>F I N</td><td>Window size [adv window]
(16 bits)</td></tr>
<tr><td colspan="4">Checksum
(16bits)</td><td colspan="5">Urgent pointer (16 bits)</td></tr>
<tr><td colspan="9">Options(if any) (0-40 byte)</td></tr>
<tr><td colspan="9">data</td></tr>
</table>

- Min. size of TCP header is 20 Bytes.
- Max. " " " " " 60 Bytes.

Cosmos(Sajal) @ Techbits

Wireshark
ethreal

classmate
Date
Page

(1) Port Numbers:-

0 to $2^{16}-1$,
Out of which 0 to 1023 are well known,
& 1024 to 49,151 are reserved, &
49,152 to 65,536 are available.

Well known ports:-

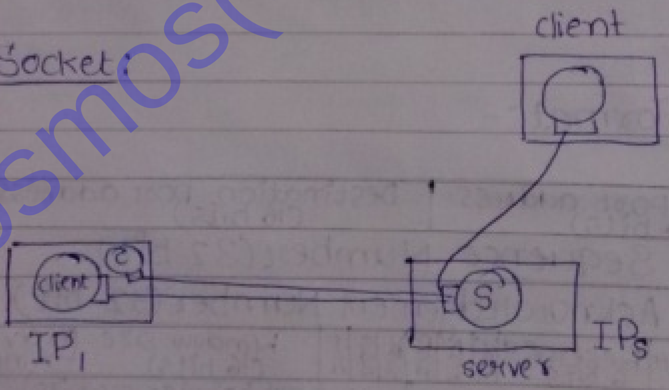
All popular services runs on well-known port numbers & these port nos. are fixed.

Reserved ports :-

These port nos. are with IANA (Internet Assigned Authorithy) & they can be used for any new protocols that will come up in future.

★ TCP is connection oriented protocol.

Socket:



client wants a web service, so it connects to port no. 80 at server.

- diff. port nos. are req. to distinguish b/w diff. processes.
- If two clients connects to same server's port no. (e.g. 80 in this case) & choose same port at client's site (e.g. x), then port no. alone can't distinguish b/w two clients.

Cosmos(Sajal)@Techbits

classmate
Date
Page

- So, we need IP address.
- But, if the same machine sends req. to same server, then IP address alone can't distinguish b/w the 2 requests.
- So combination of IP addr. & port no. is req. for distinguishing them.

- A socket is 48 bit no. (IP + port).

- TCP is byte stream protocol, i.e. every byte is numbered in TCP.

Sequence No. :-

- Since every byte in the stream is numbered, the sequence no. of the segment is seq. no. of the first byte in that segment. Sequence no. is 32 bit field which means 2^{32} sequence nos. are possible, ∴ we can send out only 2^{32} bytes with unique sequence nos.
- Wrap around :- The process of using up all the sequence numbers & repeating a previously used sequence no. is wrap around.
- (WAT) Wrap around time :- The time taken to wrap around is called wrap around time.

Q. If b/w is 1 BPs, then what is the wrap around time?

Ans. 1 Byte → 1s

~~$\frac{2^{32}}{2^3}$ Byte → $\frac{2^{32}}{2^8}$ s = 2^{29} s.~~

1 seq. → 1 s

2^{32} seq. → 2^{32} sec.

- Lifetime :- It is the time for which a packet can be there in the internet before being discarded. (practically lifetime = 3 min.)

So $\boxed{\text{WAT} \geq \text{Lifetime}}$

[illegible]

Q. If B/W is 1 MBps, then what is WAT?

Cosmos(Sajal) @ Techbits

★ Every byte takes one sequence no.

Ans. 1M Bytes → 1s

1M seq no → 1s

1 seq. no. → $\frac{1}{1M}$ s

2^{32} seq. no. → $\frac{2^{32}}{1M(10^6)}$ s = 4294.967296 s.

> 180 sec
(3 min)

Q. B/w 1 GBps
WAT = ?

Ans. 10^9 Bytes → 1s

10^9 seq. no. → 1s

1 seq. no. → $\frac{1}{10^9}$ s

2^{32} seq. no. → $\frac{2^{32}}{10^9}$ s

= 4.294967296 sec.

< 180 sec

[So, we are sending packets frequently]

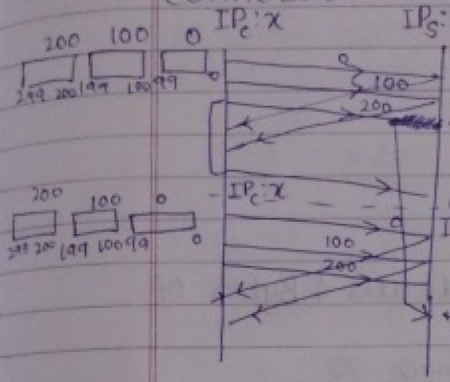
★ Since, wrap around time < lifetime, in order to distinguish b/w 2 packets with same sequence no., we use time stamp.

- Timestamp:- is used in the options field

★ All the segments made by Transport Layer need not be of same size.

Cosmos(Sajal) @ Techbits

- We use random initial sequence nos. in order to avoid accepting packets from previously closed connection as a packet from current connection.



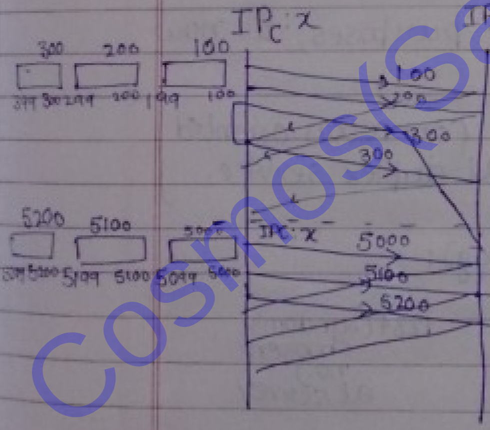
when always 0 is taken as starting no.

← not arrived

connection closed

← now the previous packet arrived & receiver has a confusion that whether packet is from current or prev. connection.

To avoid this problem, we use random initial sequence no.



IP_S:80

The data with 300 seq. no. is not of current connection, ∴ discarded. (as current connection has initial random no. of 5000.)

★ The probability of two processes on same computer to pick same seq. no. = $\frac{1}{2^{32}}$ (very small).

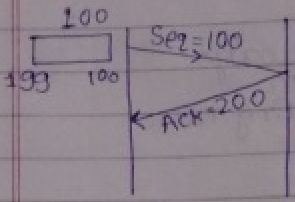
★ WAT will not change even if we use random initial sequence no.

Cosmos(Sajal) @ Techbits

Cosmos(Sajal) @ Techbits

Acknowledgement No. :-

It is the sequence no. of the byte that the receiver is expecting next.



Header Length :-

Every no. in this field indicates 4 Bytes of header.

If HLF = 5, then header length = 20

If header length = 21, then HLF = 6
$+3$ ← padding (in options)
24

Reserved :-

It is reserved for future purposes, till now it doesn't fail.

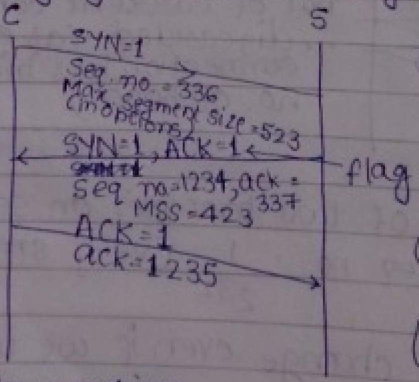
Flags :-

[TCP is connection oriented & full-duplex service.]

(i) SYN Flag (Synchronisation Flag):

336 (random no. choosen) at client

*Every SYN packet will take one sequence no.



Connection establishment phase

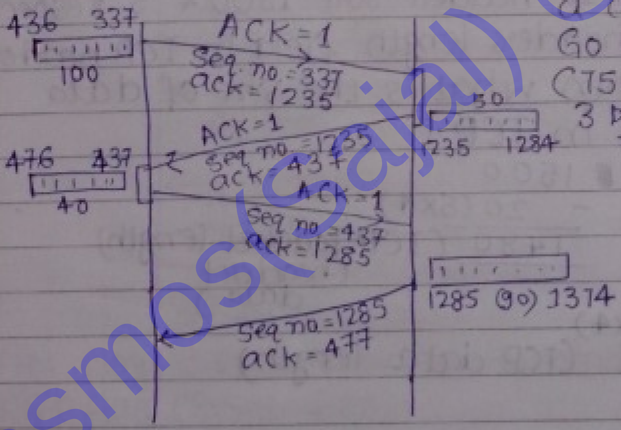
1234 (randomly choosen no.) at server

Connection Establishment (three way handshaking)

(ii) ACK flag This flag indicates that acknowledgement field is being used & it is valid.

Note:- Only the request segment will have ACK = 0 & all other segments will contain acknowledgements (ACK = 1).

SYN	ACK	
1	0	– Request (First packet)
1	1	– Reply
0	1	– Pure & Piggybacking
0	0	– X (Not possible)



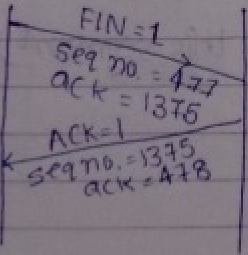
TCP uses a combination of Go back N & SR (75% SR + 25% GBN)
3 principles from SR & 1 principle from GBN

~~Haa~~ 2to ' Data transfer phase.

(iii) FIN Flag: It is used to close the connection.

SYN→1
FIN→1
ack→0
Data→1

- SYN will take 1 Seq. no.
- FIN will take 1 Seq. no.
- Every Data byte will take 1 Seq no.
- Pure ACK wont take any seq. no.



← FIN is sent
← FIN is acknowledgement
[so connection b/w client to server is closed.]

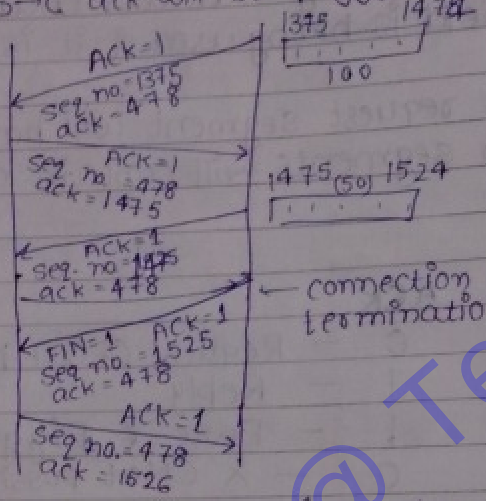
C —X→ S

now, Data can't be sent from C→S
" " can be sent from S→C
Ack can be sent from C→S
Ack can be sent from S→C

Cosmos(Sajal) @ Techbits

but S→C ack will be piggybacked & not pure.

★ All packets ~~are~~ other than the first SYN packet will have ACK=1.



Q. If total length field & header length field in IP header are 1500 & 5 respectively & header length field in TCP header is 5, then what is the size of data present in TCP?

Ans. ~~1500 − (5) = 1495~~

1500
− 20 (5×4)
1480 (TCP packet length) (header + data)

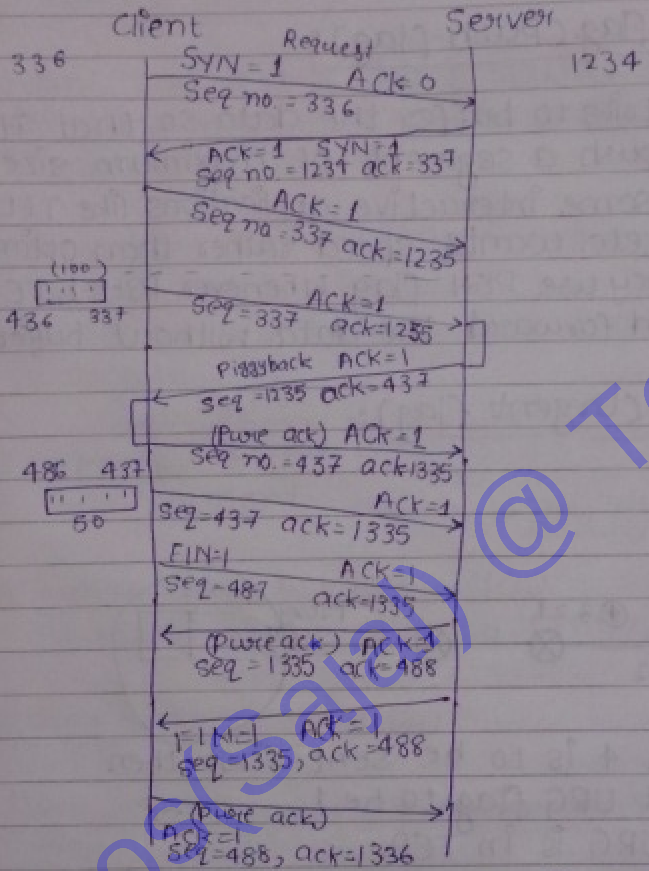
1480
− 20 (5×4)
1460 (TCP data length)

Q. If in above question, seq. no. of the TCP segment is 1234, then what is the ack no.?

Ans. 1234
+1459
2693 (last byte of this segment)

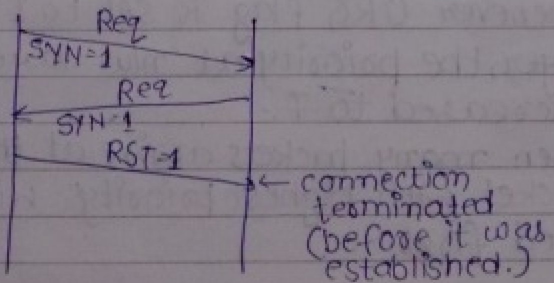
2694 is the ack no.

Cosmos(Sajal) @ Techbits



- FIN flags : It is used to terminate the connection.
- RST flag (Reset flag):

Reset is used to terminate the connection during the connection establishment phase.

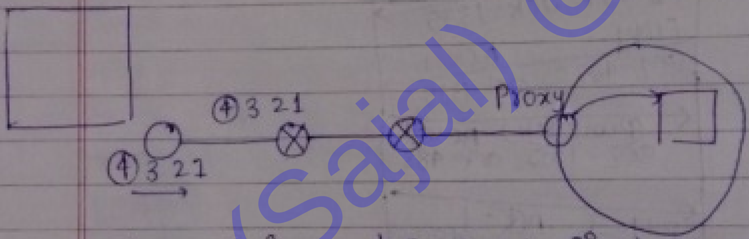


Cosmos(Sajal) @ Techbits

- PSH flag (Push flag) :-

TCP tries to buffer the data so that it can push a segment of maximum size, but some interactive applications like TELNET, chat, etc. wants speed rather than optimality so they use PSH flag. Whenever PSH=1, TCP should forward the data without buffering.

- URG (Urgent flag) :-



- When 4 is to be sent first, then we set URG flag to be 1.
- But, URG is in TCP.
- So, routers won't be knowing it as it works at n/w layer max., & URG is in Transport layer, so to tackle it, whenever URG flag is set to 1 at transport layer, the priority at n/w layer will be increased to 7.

When many packets arrive at the router, the packet with highest priority will be forwarded first.

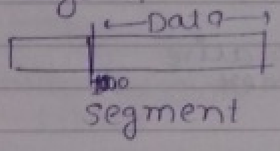
Cosmos(Sajal) @ Techbits

- ## Urgent Pointer:-

- When URG=1, this field is valid.
- This field indicates till what part of segment is the data urgent.

Q. If urgent pointer = 100 & sequence no of the segment is 1000, then what is the sequence no of the last byte in the segment which is urgent.

Ans.

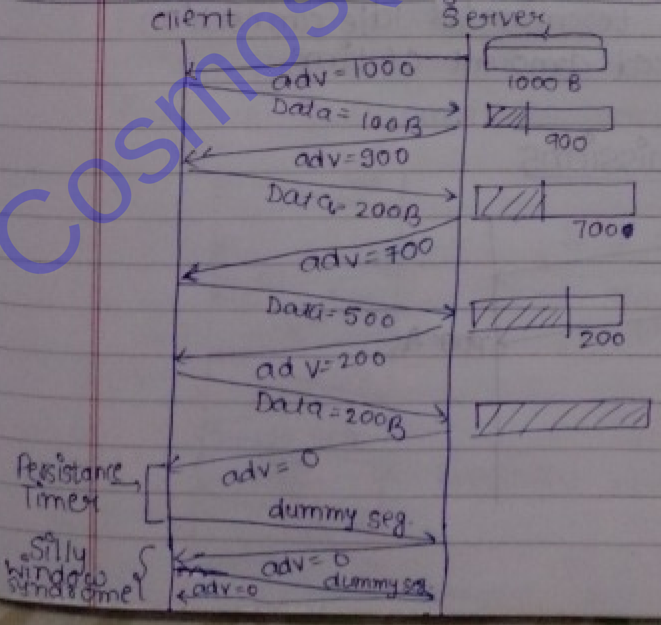


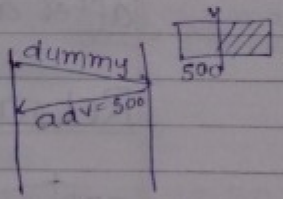
if urg ptr = 100,
then ~~no.~~ no of urgent bytes
$= \boxed{101\text{ B}}$

last urgent bytes = 1100
urgent data = 1000 to 1100 (101 B)

- Advertisement Window:-

TCP Flow control using advertisement window:-



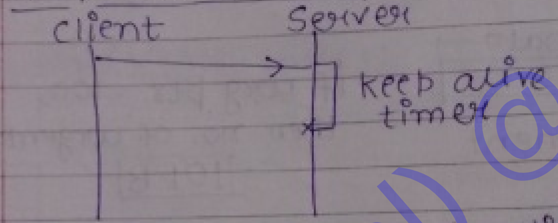


- Dummy segments are ~~[illegible]~~ sent when client can't send normal segments

Cosmos(Sajal) @ Techbits

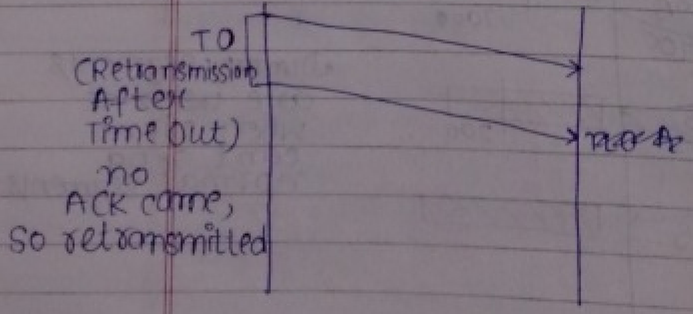
- Since advertisement window is 16 bits, a server can't advertise more than 64 KB even if it has free buffer, ∴ to overcome this to this field 14 bits are added (appended) to make it 30 bits (1 GB). These bits are in Options

Keep alive timer

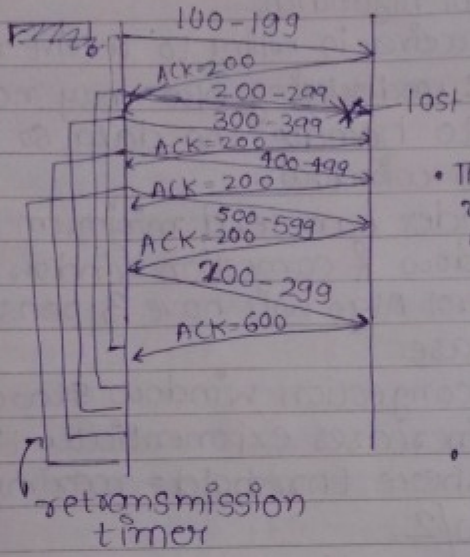


- In this case, whenever the client establishes a connection with server, the server starts keep alive timer, if ~~we~~ client doesn't send any data / or perform any activity within the timer expiration period, then connection will get terminated.
- This timer terminates idle connection after a fixed amount of time.

Retransmissions


TO
(Retransmission After Time out)
no ACK came, so retransmitted

Cosmos(Sajal) @ Techbits

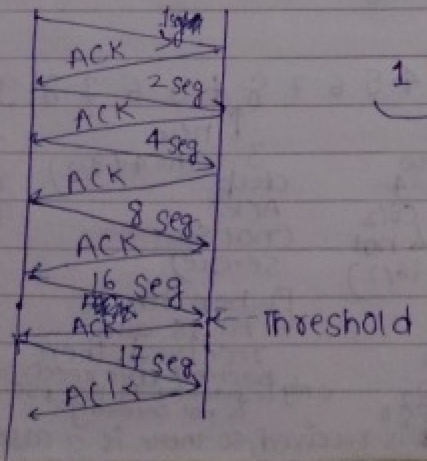


- Three duplicate ACKs are received, so it is a "fact" that if 3 duplicate ACKs are received for a packet, then that packet might be lost in the the n/w, so retransmit it before time out.
- If last packet is lost, then it will be retransmitted after time out.

- TCP Congestion Control:-

Buffer size ~~MSS~~ = 32000 B (Receiver)
MSS = 1000 B

- Now, we can send 32 segments at once w/o waiting for ACK.
- But we can't send all 32, as the n/w might get congested due to it (the routers may cause timeout) & hence TCP controls congestion.



$\underbrace{1\ \ 2\ \ 4\ \ 8\ \ 16}_{\text{slow start phase}}\ \ \underbrace{17\ \ 18\ \ 19\ \ 20.}_{\text{congestion avoidance}}$

Cosmos(Sajal) @ Techbits

classmate

Date ______
Page ______

Congestion Control Algorithm:-

- Even though a receiver is wiling to receive more than 1 MSS, the underlying n/w may not be in a position to handle the data, so TCP uses congestion window.

Therefore, a sender can send minimum of advertise window & congestion window.

- Congestion Control Algo will have 3 phases:-

(i) Slow start phase.

In this phase congestion window starts with 1 MSS & increases exponentially till the threshold where threshold = maximum sender window/2.

(ii) Congestion avoidance phase:-

In this phase, congestion window will grow linearly till it reaches maximum window size.

e.g. let receiver's buffer size = 160,00B, MSS is 1000 B, then after how many RTT's (Round Trip time)/Rounds. sender can send 16 MSS in one window

Ans. ~~We~~ after 11 rounds.

e.g. Max = 32 MSS

Th = 16

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

Time Out (severe) → new Th = 4 (8/2 & not 16/2)

[Time out occurs when there is congestion in the n/w, as no ack for lost packets is received, so there is a case that various packets are lost.]

3 dup ACKs (not so severe) → new Th = 4 (8/2)

[When 3 dup ACKs are received, then only packets are received, but 1 packet is lost, so congestion is not severe.] so congestion in n/w.

TO new Th = $\lfloor \frac{9}{2} \rfloor = 4$

Cosmos(Sajal) @ Techbits

classmate
Date
Page

Congestion Detection Phase:-

Congestion could be detected in 2 ways:-
(i) 3 duplicate ACKs.
(ii) Time Out.

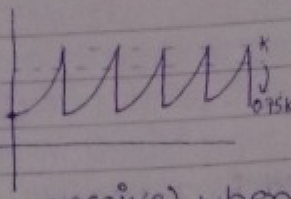
- 3 duplicate ACks:- whenever congestion is detected because of 3 duplicate ACKs, it will indicate that congestion is not severe, ∴ new threshold is set to half of current congestion window size & algo enters congestion avoidance phase.
- Time Out :- this indicates that congestion is severe & so new threshold is set to half of the current congestion window size & algo enters slow start phase.

Time Out Timer at link-to-link protocols ~~in~~ at data link layer like "HDLC" uses static time out timer, but end to end protocols like TCP should not use static time out timers as it may lead to n/w congestion when there is heavy traffic.

~~Tim~~ RTT at 4:00 A.M. is less than that at 6:00 PM.

Cosmos(Sajal)@Techbits

Congestion Control



- If the sender is sending data at rate of 1Gbps, but user is allocated only 100Mbps.
- In this case we set a value k (max. limit ~~of~~ of no. of packets that receiver will receive), when k is attained, we simply starts discarding the packets, (we dont send ACK's for them), so timer will time out at server, so the server will again start from 1, & hence in this way we can set k & set the receiver to receive data at 100Mbps (by setting k.)

★ Second soln. :-
In this soln., we send adv. window size acc. to 100 Mbps from client to server.

Checksums

1. TCP checksum is calculated ~~at~~ for TCP header, TCP payload & pseudoheader.
2. IP Layer put checksum calculation for IP header.
3. If in transit, the IP header gets currupted & the checksum for IP gets modified in such a way that the router/receiver can't ~~pe~~ catch the error.
In this case, TCP will catch the error by checksum on pseudoheader, so TCP will discard the packet as the IP header gets curropted & sent to wrong machine.

★ The TCP doesn't calculate checksum for entire IP header, just a part of the header, as the IP header changes through the transit.

Cosmos(Sajal) @ Techbits

classmate
Date
Page

The fields that change during transit in IP header:-

- TTL
- Offset
- Checksum
- Options
- MF

Q. Why should routers compute the checksum of IP for every packet?

Ans. Because TTL changes at every router with each hop. In this case if there is fragmentation, fragment offset, MF & total length may change & options could change.

Q. Why TCP is computing checksum only on pseudoheader from IP & not on actual header?

Ans. Because many fields in IP header may vary.

☆ We need ~~to~~ CRC at DLL even though we use checksum at TCP & IP because sometimes we can send data ~~b/w~~ ~~from~~ b/w two machines only, so we dont need n/w & transport layer, so errors will be detected by DLL's CRC only as TCP & IP layers are absent.

☆ Why can't use static round trip time?

Ans. Because the round trip time changes ~~is~~ at different time of day, ∴ we need ~~du~~ round trip time timer to ~~be~~ change from time-to-time.

Cosmos(Sajal) @ Techbits

Q. Why should we guess first RTT?

Ans. Because the packet will be sent via a gateway & gateway serves millions of users, so if we send a packet just for actual calc. of initial RTT, then a large traffic will occur while getting

How to set time out timer? (Basic Algorithm)

- Initially we set the ~~RTT~~ Round Trip Time (RTT) to a guess value, e.g. IRTT = 10 ms. so we set ~~to~~ Time out timer = 2×IRTT = 20 ms
- ~~Let the Pac~~
  So, now we sent the packet & it returns in 15 ms,
  then next RTT (NRTT) = α(IRTT) + $(1-\alpha)$ARTT
  [α can be value b/w $0 \le \alpha \le 1$] ↑ actual RTT

let ARTT = 15 ms.

∴ NRTT = 12.5 ms, [$\alpha = 1/2$]

so, ~~next~~ Time Out Timer (TOT) = 25 ms (12.5×2)

☆ practically α is taken to be $\frac{1}{3}$.

☆ Disadvantage of Basic algorithm is computing Time out as 2×NRTT.

Jacobson's Algorithm

① Initially, we guess IRTT, let it be 10 ms
& ID (Initial Deviation) = 5 ms (assumption).
now, we calculate initial Time Out

$$TO = IRTT + 4 \times ID$$
$$= 30\text{ms}$$

② In next step, when we get the packet, let the actual RTT (ARTT) = 20 ms
then the actual deviation (AD) =

$$|IRTT - ARTT|$$
$$= 10 \text{ ms}$$

then, we calculate next deviation (ND)

Cosmos(Sajal) @ Techbits

$ND = \alpha(ID) + (1-\alpha)(AD)$
$= 7.5$ — ②

$NRTT = \alpha(IRTT) + (1-\alpha)(ARTT)$
$= 15ms$, — ①

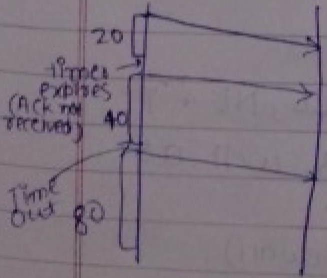
So ~~Next~~ Time Out (TO) = NRTT + 4 × ND
= 45ms.

③ In next step,
we take IRTT = 15ms (from ①)
& ID = 7.5ms (from ②)
& let ARTT = 25 ms
∴ $AD = |IRTT - ARTT| = 10ms$
& $ND = \alpha(ID) + (1-\alpha)AD$
$= 8.75ms$.
& $NRTT = \alpha(IRTT) + (1-\alpha)ARTT$
= ~~[illegible]~~ 20ms
& TO = NRTT + 4 × ND
= 55 ms.

Options (in TCP)

KARNS soln.

If we dont get ACK either in basic algorithm or in Jacobson's algorithm, the timeout for the next retransmission acc. to KARN is twice the previous time-out.



Cosmos(Sajal) @ Techbits

classmate
Date
Page

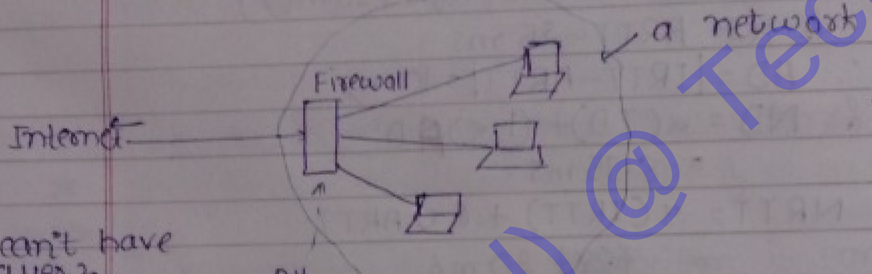
LAN connecting Devices:-

① Wires
② Hub
③ Switch
④ Bridge

} → These devices can't stop a broadcasting message

☆ Routers will stop the broadcasting.

firewalls



All the devices in the n/w will be connected to the firewall (so all packets reaching the hosts in the n/w, & packets from hosts will pass through firewall.

We can't have a layer 2 firewalls, because the packet from internet will be coming ~~from~~ through gateway, (as all the packets will be coming from gateways so all the packets will be discarded)

Types of Firewall :-

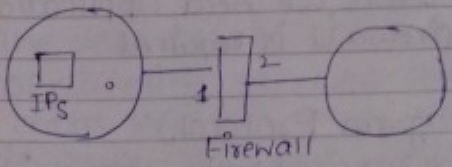
1. Layer 3 firewall :- (Packet filtering firewall) This firewall will contain till n/w layer & can make a decision depending on the IP address. (It can filter out a host with a particular IP address.)

2. Layer 4 firewall :- This contains physical layer, DLL, NL & TL, ∴ it can filter both host as well as particular service on the host.

3. Layer 5 firewall :- (Proxy firewall)

Cosmos(Sajal) @ Techbits

This contains all 5 layers. It can filter host, particular service on a host & particular user (user ID & password).



Firewall :-

Destⁿ IP	Source IP	Destⁿ Port	Source Port	Usertype	Interface
–	IP_s	–	–	–	1
IP_s	–	23	–	–	2
–	IP_{FB}	–	–	–	–

if the sender with IP addr. as IP_s is requesting for some services through interface 1, then the firewall will block it.

if the destⁿ is a particular host with IP addr. as IP_s, & we dont want anyone to connect to ~~its~~ [illegible] also port 23 (for telnet services) & the req. coming from interface 2, so firewall blocks it.

(when we want to block any packet coming from FB, then ~~we~~ firewall will block it (no matter from which interface it comes from.)

Q. What is the smallest firewall needed to block ICMP packet?

Ans. ICMP works at n/w layer, so we need Layer 3.

Q. What is the smallest firewall that can be used to block HTTP traffic?

Ans. Layer 4, we have to block port no. 80, ∴ we need layer 4.

Cosmos(Sajal) @ Techbits

Q What is the firewall capable of blocking some of the users?

Ans. proxy firewall

In order to block users, we need application layer, so proxy firewall is required.

UDP (User Datagram Protocol):-

whenever speed is required rather than reliability we use UDP.

Source port no.	Destn port no.
Checksum	Total Length

& not the header length.

- Multimedia
- DNS
- NTP

TL ─ Reliable → (TCP)
TL ─ Unreliable → (UDP)

NL ─ Connectionless (Datagram → IP)
NL ─ Connection Oriented (Virtual Circuits → ATM)

DLL

PL

Q.☆ If the Datagram received at n/w layer has to be handed over to user at application layer w/o providing any reliability at transport layer, we use UDP at transport layer.

~~Ad~~ Need for UDP:-

(i) If an application needs speed rather than reliability, then UDP is better. (e.g. Multimedia applications)

(ii) If an application needs one request & one reply kind of communication, then connection

Cosmos(Sajal) @ Techbits

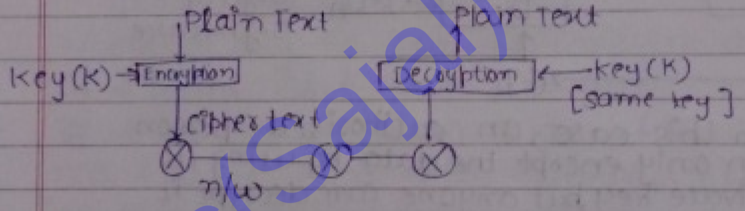
establishment is not required, ∴ UDP is better. (e.g. DNS, NTP (N/w Type Protocol), ~~Port of the~~ Quote of the day}, n/w news

Note- UDP is connectionless, unreliable protocol.

(iii) The data rate in TCP is not uniform because of differing ~~size of advertisement wind~~ data rate (diff. no. of packets sent) during Congestion Control if application needs uniform data rate, then UDP can be used

Cryptography

Symmetric-key Encryption



Disadvantage:

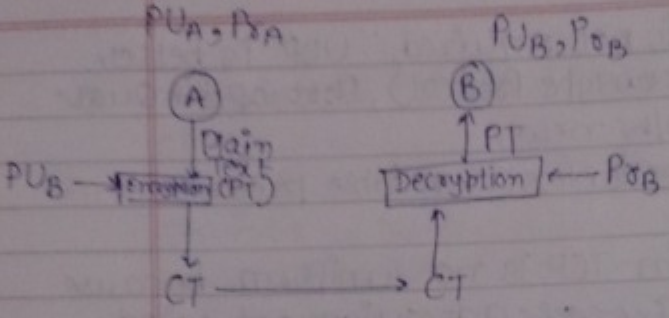
① Key transfer is not secure.

② If there are 'n' parties who wants to communicate securely, then we need $^nC_2$ keys.

Public Key, Private Key Encryption

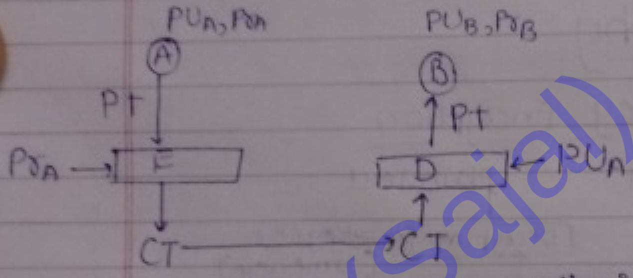
Cosmos(Sajal) @ Techbits

classmate
Date
Page



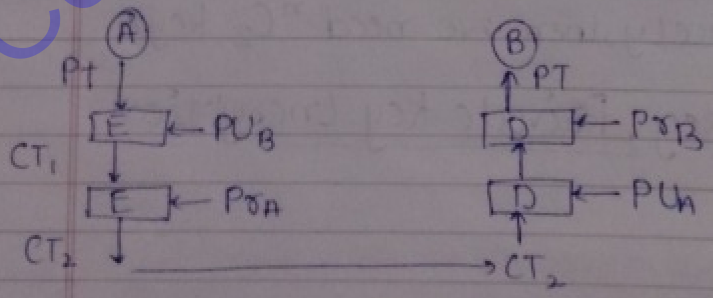
Encryption

In this case, anyone can send the data to B as everyone has PUB, so we can't identify whether packet comes from authorised person or not.



authorization & Digital signature

In this case, an authorised person can only encrypt the data by using its private key, but anyone can decrypt it by using the public key of A & hence no security,
but in this case, authorization can be guranteed.



In this case, the packet can only be sent by A & no other can send it (as only A has its Private key) & only can also be encrypted by public key of B, so that only B can decrypt it using its private key & no other.

Cosmos(Sajal) @ Techbits

Basics Of Cryptography

① Euler's Theorem:-

If 'p' is a prime no. & 'a' is any positive no. not divisible by p, then $a^{p-1} \cong 1 \pmod p$.
[a < p] → must

means $\frac{a^{p-1}}{p}$ gives 1 as remainder.

Euler-Totient no. (ϕ):-

It represent no. of +ve integers < "n" which are relatively prime ~~divisible~~ 'n'.

Relatively prime:- Two ~~prime~~ nos. whose gcd is 1.

$\therefore \phi(5) = \{1,2,3,4\} = 4$

$\phi(10) = \{1,3,7,9\} = 4$

$\phi(35) =$ [illegible]

Whenever any no. can be written as product of 2 prime nos. & the nos. are diff.

Note:- When $n = p \times q$, such that p & q are 2 prime nos. & $p \neq q$, then $\phi(n) = \phi(p) \times \phi(q)$

If p is a prime no., the $\phi(p) = p-1$

Discrete Logarithms:-

If 'α' & 'n' are relatively prime nos., then there exist atleast one integer 'm', which satisfy $\alpha^m \cong 1 \pmod n$

Q. If $\alpha = 7$ & $n = 19$, then find m?

Ans $7^m \bmod 19 = 1$

Cosmos(Sajal) @ Techbits

Q. Find out the period of 3 mod 7

Ans.
$$\left.\begin{aligned} 3^1 \bmod 7 &= 3 \\ 3^2 \bmod 7 &= 2 \\ 3^3 \bmod 7 &= 6 \\ 3^4 \bmod 7 &= 4 \\ 3^5 \bmod 7 &= 5 \\ 3^6 \bmod 7 &= \boxed{1} \end{aligned}\right\} \rightarrow \text{period} = 6$$

it becomes 1.

& $3^7 \bmod 7 = 3^1 \bmod 7$ [as period is 6]

☆ If period of a mod b is $\phi(b)$, then a is called primitive root of b.

☆ 3 is a primitive root of 7, 2 is not a primitive root of 7.

☆ The period of a mod b will definitely divide $\phi(b)$.

RSA Algorithm

(to generate public key & private).

rsa -keygen

Step (i) Select 2 prime nos. 'p' & 'q' such that $p \neq q$.

step (ii) Calculate $n = pq$

step (iii) Calculate $\phi(n) = \cancel{pq}\,(p-1)(q-1)$

step (iv) Select an integer 'e' such that gcd of $\phi(n)$ & e is 1 & $1 < e < \phi(n)$.

Step (v) Calculate 'd' such that
$$d \cong e^{-1} \bmod (\phi(n))$$

Cosmos(Sajal) @ Techbits

$ed \cong 1 (\bmod \phi(n))$

Public key (e,n)
Private key (d,n)

RSA algorithm can be used to send a small no. for security & then it can be used as symmetric key for the subsequent communication

Diffie-Hellman Key Exchange

(i) If A,B wants to exchange a key then there are 2 publically known nos. e.g. a prime no. 'p' & an integer α which is primitive root of 'p'.

A selects a random integer $x_A < p$ & compute Y_A as $Y_A \cong \alpha^{x_A} \bmod p$.
B selects a random integer $X_B < p$ & computes Y_B as $Y_B \cong \alpha^{X_B} \bmod p$.
Each side (A & B) keeps X as private & declares Y as public key.

At A key = $(Y_B)^{X_A} \bmod p$
At B key = $(Y_A)^{X_B} \bmod p$] → both of these nos. are same.

Cosmos(Sajal) @ Techbits

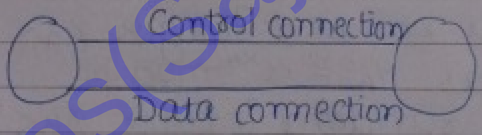
Application layer

HTTP

It is used for web service. Port no. is 80.
HTTP is stateless. (i.e. ~~it do~~ HTTP server doesn't remember the connection info, it asks client to store the info in cookies)
HTTP uses TCP at transport layer (reliability is required).

FTP (File transfer Protocol)

① It is used to transfer files b/w client & server.
② FTP requires reliability, so it uses TCP at transport layer.
③ Port Nos. used are 20, 21.

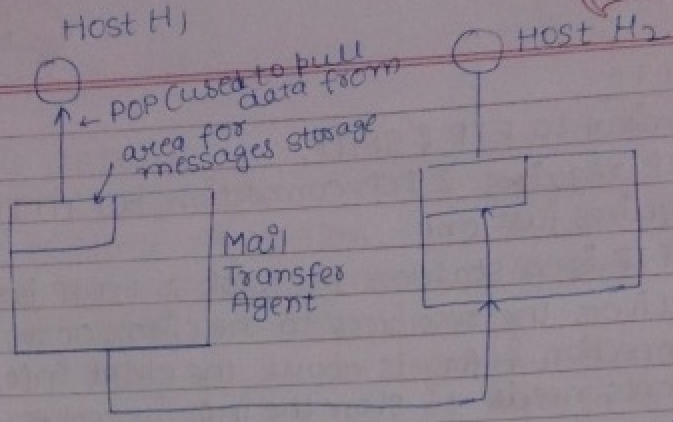


Using control connection, we can browse the file system & using data connection we can transfer the data.

④ FTP is out of band connection, i.e. data & control information follows 2 connections.

SMTP (Simple Mail Transfer Protocol)

Cosmos(Sajal) @ Techbits



① SMTP is used to push the emails & POP is used to pull the emails.

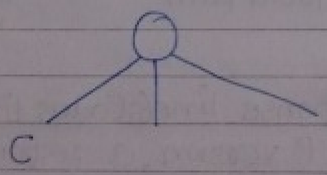
② Both the protocols are pure text based.

③ MIME is a set of s/w programs which will assisst SMTP & POP in sending & receiving data which is not pure text.

④ Both SMTP & POP needs reliability & so they use TCP at transport layer.

DNS (Domain Naming Server)

① DNS is a one request one reply protocol, ∴ it uses UDP at transport layer.



Cosmos(Sajal) @ Techbits

HTTP

- Similar to FTP & SMTP.
- FTP requires 2 TCP connection, but HTTP requires just one.
- HTTP is a stateless protocol, so HTTP just delivers the resources to the client, closes the connection & forgets about the client info so clients needs to store the info. in cookies

HTTP request/response format

Initial Line
Headers
Blank Line
Body

- The initial line differs for both request & response.

initial request line:-

method name URL HTTP version
(local path)

e.g.

$$\underbrace{\text{GET}}_{\text{method name}}\ \underbrace{\text{/path/to/file/index.HTML}}_{\text{local path}}\ \underbrace{\text{HTTP/1.0}}_{\text{HTTP version}}$$

initial response line(status line):-

- it contains HTTP version, a response status code that gives the result of the request & an English reason phrase describing the status code,

e.g. HTTP/1.0 200 OK
or HTTP/1.0 404 NOT FOUND

Cosmos(Sajal) @ Techbits

$\frac{60}{(1.7)^2}$ $\frac{60}{2.89}$

FTP

1. It is stateful
2. Uses TCP for reliability
3. Out of band connection (which means that FTP uses 2 different ports for control & data connection)

The FTP client sends an FTP request to FTP server on port 21 of TCP (this occurs through a command connection), initially authorization is required which takes place through username & password.

After the authorization, some command is sent through ~~common~~ control connection (e.g to download a file from server), the FTP server in response opens a data connection with the client on port 20, & dowloading takes place.

After that the connection terminates (the server closes the connection, but remembers about the client i.e authorization, etc & hence is stateful), so whenever client ask for next file transfer, he/she dont need to start the authorization step again.

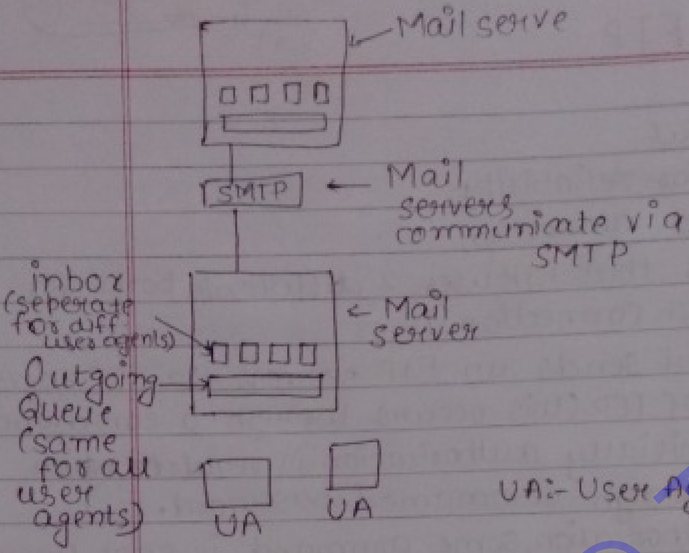
It is called Out of band connection because control & data connection takes place through 2 different ports

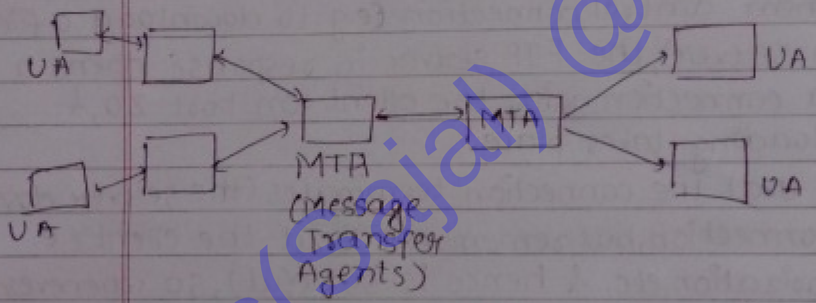
SMTP

- Supported by TCP/IP suite.

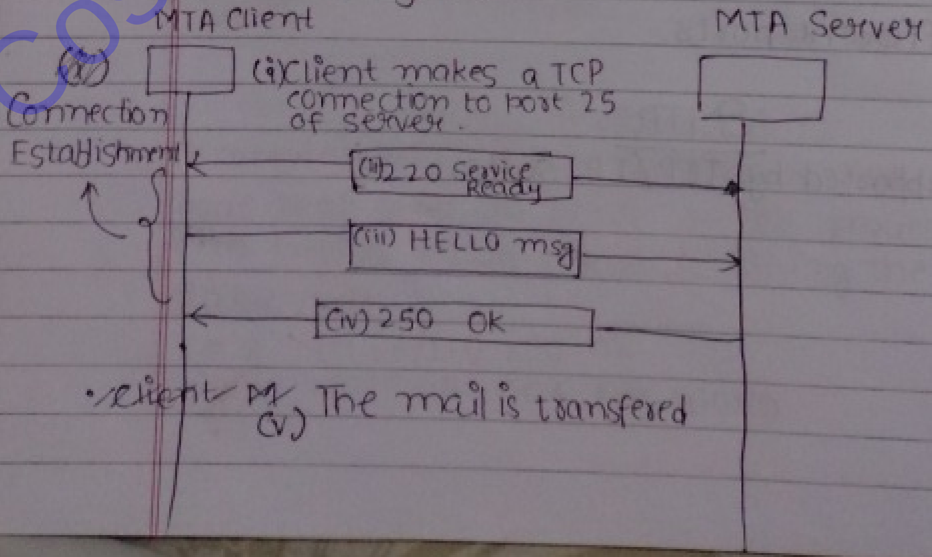
Cosmos(Saial) @ Techbits

classmate
Date
Page


Mail serve
SMTP
Mail servers communicate via SMTP
inbox (seperate for diff user agents)
Mail server
Outgoing Queue (same for all user agents)
UA
UA
UA:- User Agents



- MTA's are used to transfer email from one n/w having some format say f1 to another n/w having same or different format (say f2).



(i) Client makes a TCP connection to port 25 of server.

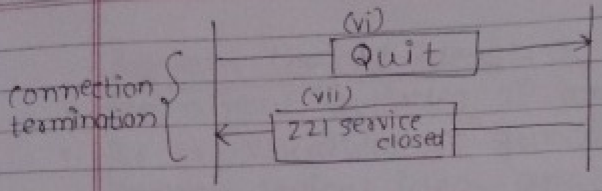
(ii) 220 Service Ready

(iii) HELLO msg

(iv) 250 Ok

• ~~client~~ ~~M~~ (v) The mail is transfered

Cosmos(Sajal) @ Techbits



- SMTP doesn't allow non-textual data to be sent via a n/w.
- But MIME(Multipurpose Internet Mail Extensions, an extention to SMTP) can be used to transfer non-textual data to be transferred via Internet. (non-ASCII)

POP3

- Used for interacting with the mail box
- used for downloading the mails from mail server to the user machine.
- Users can't create folders on mail server.

IMAP4

- More features than POP3.
- Can check email header prior to downloading.
- Can search contents of email prior to downloading.
- Can partially download email.
- Can create, delete or rename mailboxes on mail server.
- Can create hierarchy of mailboxes in a folder for email storage.

Cosmos(Sajal) @ Techbits