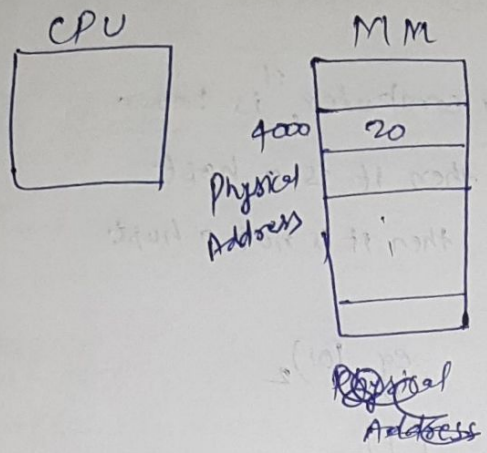
Date : 18/07/22

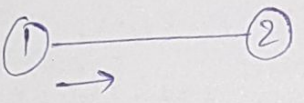


NIC Card (Network Interface Card)
OR
Physical Address
or
Ethernet Address
or
Implicit Address
or
MAC Address

48 bit Address
↳ Hexadecimal Notation
14:1A:12:13:12:16 } → 8×6 = 48 bit
In CN
16
0001 0110 → 8 bit

In Mobile,
IMEI No ≡ MAC A
Mob. No. ≡ IP Addr
IP Address
↳ Explicit Add

Any system in internet can be identified by IP Address.



Sender Add(SA) Destination Add (DA)

S.MAC, D MAC
Scope is Local (LAN)

Scope of MAC Address is local
i.e; we can uniquely identify the device within the LAN only not globally.

IANA → Internet Assigned Number Authority (Classful Addressing) → Logical Addressing

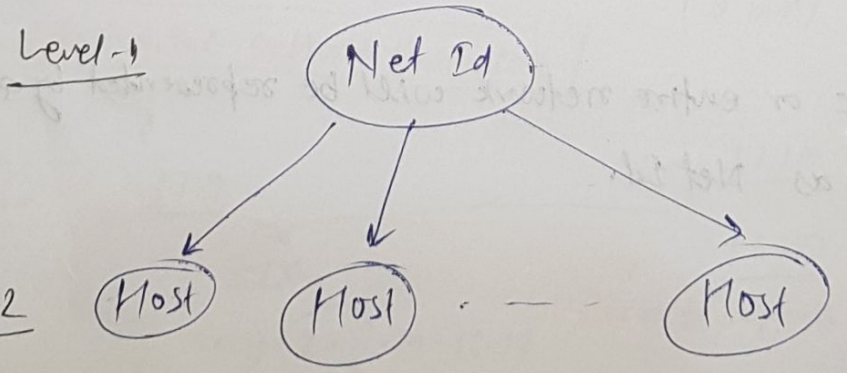
Class (IPv4)

A, B, C, D, E
↳ Research Purpose

Unicasting (one to one)
Multicasting (one to many)

Our aim is to assign IP addresses to the computer.

Two Level Hierarchy :



⇒ (Two level Hierarchy)

eg: www.google.com
↑ Host-name

Host :

Whenever an IP address is assigned to a computer, it is known as Host. eg. Mobile with SIM Card: then it is a host
" without " " : then it is not a host

Classful Addressing :

$(xy)_2$; $x < 2$, $y < 2$ eg $(01)_2$ $(7)_{10}$

1) Binary Notation$_2$ (System Friendly)

01010111 10101111 10101010 11111111 → Octet

ii) Dotted Decimal Notation$_{10}$ (User Friendly)

41.89.99.121

$(41)_{10}$ = $(0\ 0\ 1\ 0\ 1\ 0\ 0\ 1)_2$

$(89)_{10}$ = 0 1 0 1 1 0 0 1

$(99)_{10}$ = 0 1 1 0 0 0 1 1

$(121)_{10}$ = 0 1 1 1 1 0 0 1

128 64 32 16 8 4 2 1

$(189)_{10}$ = 1 0 1 1 1 1 0 1

$(194)_{10}$ = 1 1 0 0 0 0 1 0

$(183)_{10}$ = 1 0 1 1 0 1 1 1

Net Id :-

Every network or entire network will be represented by a number, is known as Net Id.

→ In Binary Notation, Starting few bits will decide the type of class

→ In Dotted Decimal Notation, first octet will decide the type of class

Total : 32 bits.

Class A: ~~0–127~~ (1–126)

0 $(2^7 - 2)$ No of Networks — Net bits [8 bits]

$(2^{24} - 2)$ no of hosts (each network has) — Host Bits [24 bits] (as per IANA)

8 bits + 24 bits = 32 bits

0 0000000 = 0
⋮
0 1111111 = 127 (~~0~~ to 127) → 1 – 126

0.0.0.0 → DHCP Client Sp. IP Add

127.x.y.z → Loop Back Address Sp. IP Add.

Two Level Hierarchy
→ L-1 : Net Id
L-2 : Host Id

eg: 40.50.60.70 ← Class A

Dotted Decimal → Octet 1 = 40 ∈ (1,126) → Class A

→ In Class A, Starting bit is '0'.
→ 0 & 127 are Special IP addresses so we don't include them in the range of Class A IP add. → Range = [1 to 126]

→ Any no. of cont. 1's is an odd no. eg 11 → 3, 111 → 7, 1111 → …

Class B : (128–191)

10 2^{14} — Net Bits (16 bits) + $2^{16} - 2$ — Host Bits (16 bits) = 32 bits [as per IANA]

10 000000 = 128
⋮
10 111111 = 191

eg. 136.41.93.89 ← class B

Class C : (192–223)

110 2^{21} — Net Bits (24 bits)

$2^8 - 2$ — Host Bits (8 bits)

110 00000 = 192
⋮
110 11111 = 223

[Class A, B, C supports Unicasting]

Class D : (224–239)

1110

1110 0000 = 224
⋮
1110 1111 = 239

225.

eg 225.14.16.17 ← class D

∵ Class D supports Multicasting ⇒ No network & host bits

Class E : (240–255)

1111

1111 0000 = 240
1111 1111 = 255

Used for Research Purpose

Summary:

Class A : [0...] 1 - 126
Class B : [10. .] 128 - 191
Class C : [110. . .] 192 - 223
Class D : [1110 . . .] 224 - 239
Class E : [1111 . . .] 240 - 255

Q Which of following is true in classful address:
① Class 'A' Range is (1 to 128).
② No. of N/ws of class B are 2^{16}
③ No of hosts in each n/w of class A is $(2^{24}-2)$ hosts
④ none
Ans: 1, 3

(i) Network Mask or Default Mask :-

(allows something, restrict other things)

Network Bit = All 1 bits
Host Bit = All 0 bits

Class A ⇒ 11111111 00000000 00000000 00000000
↳ 255.0.0.0 // Network Mask for Class A

Class B ⇒ 11111111 11111111 00000000 00000000
↳ 255.255.0.0 // N/w Mask for Class B

Class C ⇒ 255.255.255.0 // N/w Mask for Class C

Class D Class E

eg. $IP_1 = \underbrace{201.44.89}_{N}.\underbrace{99}_{H}$ // Class C IP add.
Net ID = ?

All Host bits are 1s → Direct Broadcast Address of N/work, 201.44.89.255

IP_1 = 201.44.89.99
Mask = 255.255.255.0 ← // Class C N/w Mask.
Net ID = 201.44.89.0

↓ Bitwise AND op

eg

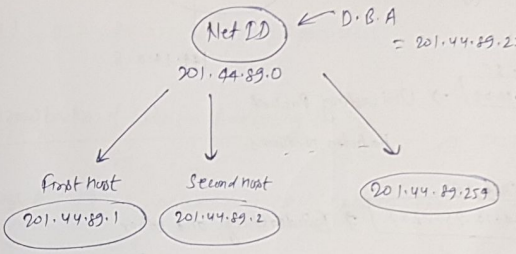
x	y	AND
0	0	0
0	1	0
1	0	0
1	1	1

201 = 1100 1001
255 = 1111 1111
201 = 1100 1001

99 : 0110 0011
0 : 0000 0000
0 00000000

Net ID :

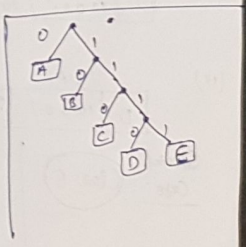
By performing bitwise 'AND' b/w IP Address and Network Mask, we will get the Network ID (Net ID).



DBA: Direct Broadcast Address } to communicate between other network

We are subtracting two addresses (2) in the number of Hosts in each network because one of them is used for Net ID and the other one is used for the DBA.

eg. IP_1 = 144.89.99.142 → ← class B
Net Id = ? 144.89.0.0
DBA = ? 144.89.255.255



Summary:

Class A : [0 ...] 1 - 126

Class B : [10 - -] 128 - 191

Class C : [110 ...] 192 - 223

Class D : [1110 ...] 224 - 239

Class E : [1111 ...] 240 - 255

Q Which of following is true in classful address:

① Class 'A' Range is (1 to 126).

② No. of N/Ws of class B are 2^{16}

③ No of hosts in each n/w of class A is $(2^{24} - 2)$ hosts

④ none

Ans: 1, 3

(i) Network Mask or Default Mask :-

allows something restrict other things

Network Bit = All 1 bits Host Bit = All 0 bits

Class A ⇒ 11111111 00000000 00000000 00000000

→ 255.0.0.0 // Network Mask for Class A

Class B ⇒ 11111111 11111111 00000000 00000000

→ 255.255.0.0 // N/w Mask for Class B

Class C ⇒ 255.255.255.0 // N/w Mask for Class C

Class D Class E

eg: IP_1 = 201.44.89.99 // Class C IP add.

Net ID = ?

All Host bits are 1s → Direct Broadcast Address of Network, 201.44.89.255

IP_1 = 201.44.89.99

Mask = 255.255.255.0 ← // Class C N/w Mask.

Net ID = 201.44.89.0

↓ Bitwise AND op

x	y	AND
0	0	0
0	1	0
1	0	0
1	1	1

eg 201 = 1100 1001

255 = 1111 1111

201 = 1100 1001

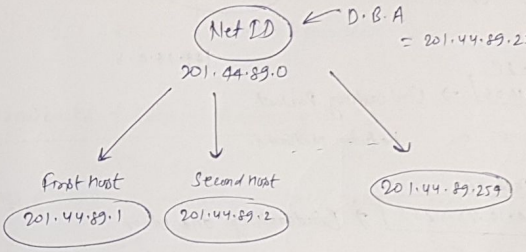
99 : 0110 0011

0 : 0000 0000

0 00000000

Net ID :

By performing bitwise 'AND' b/w IP Address and Network Mask, we will get the Network ID (Net ID).



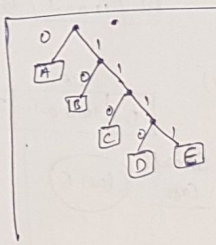
We are subtracting two (2) addresses in the number of Hosts in each network because one of them is used for Net ID and the other one is used for the DBA.

eg. ← Class B

IP_1 = 144.89.99.142

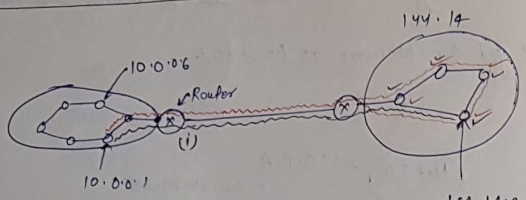
Net Id = ? 144.89.0.0

DBA = ? 144.89.255.255



Pseudo Approach of Network :-

Net ID cannot be given to host.



(i)	S.IP	D.IP
D	10.0.0.1	144.14.0.8 ⇒ Unicasting Packet between Networks.

(ii)	Source IP	Dest IP
D	10.0.0.1	144.14.255.255 ⇒ Broadcasting one other network.

(Possible)

| S.IP | D.IP |
---|---|---|
D | 144.14.255.255 | 10.0.0.1

X (Not Possible)

(iii)	S.IP	D.IP
D	10.0.0.1	10.0.0.6 → Unicasting in same network.

(iv)	S.IP	D.IP
D	10.0.0.1	255.255.255.255 → Broadcasting within the same network.

Special Case: Class E

LBA
Limited Broadcast Address
(Scope is Local).

| S.IP | D.IP |
---|---|---|
D | 255.255.255.255 | 10.0.0.1

X

msq

Q. Which of the following is used as destination IP only :-

(a) 10.255.255.255 only D is possible

(b) 176.16.0.1 both S & D possible If any comp. is acting like both source & dest.

(c) 192.168.1.3 " "

(d) 255.255.255.255 only D possible

Drawbacks of Classful Addressing :-

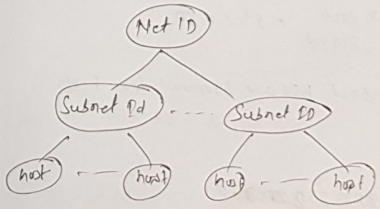
Class A : $(2^7 - 2)$ networks ⇒ each network has $(2^{24} - 2)$ hosts (analogy)
(req. eg 5000) (many eg 90,000,000 → many IPs are wasted)

Class B : 2^{14} networks ⇒ each network has $(2^{16} - 2)$ hosts
(req. eg 5000) (available = 65534)

Class C : 2^{21} networks ⇒ each network has $(2^8 - 2)$ hosts
(req. 1000) (available only 254)

} Subnetting Concept is used.

} Supernetting Concept is used



Subnetting → Dividing a network into some small parts for effective utilization of IP addresses, is known as Subnetting.

(i) In Class C,

If subnet mask = 255.255.255.224

No of subnets = ?

No. of host in each subnet = ?

Soln:

Class C,

Default mask : 255.255.255.0

= 11111111 11111111 11111111 00000000

Net bits | Host bits

Subnet mask : 255.255.255.224

11111111 11111111 11111111 111 00000

Net bits | S | H

∴ No. of Subnets = $2^3 - 2 = 6$

No of host in each subnet = $2^5 - 2 = 30$

During the subnetting, subnet bits are borrowed from host.

eg: In Class B,

subnet mask : 255.255.252.0

No of subnets =

No of hosts in each subnet = ?

Class B, Default mask,

255.255.0.0

= 11111111 11111111 00000000 00000000

Subnet mask : 255.255.252.0

11111111 11111111 111111 00 00000000

N | S | H

∴ Total no. of subnet = $2^6 - 2 = 62$

No of ho = $2^{10} - 2 = 1022$

← Class C → Net bit =

eg: IP : 201.44.89.99

Subnet Mask : 255.255.255.224

99: 01100011

224: 11100000

01100000

= 96

① Subnet Id = ?

② Subnet no = ?

11111111 11111111 11111111 111 00000

N | S | H

for Class C, Net bits = ~~16~~ 24 bits

∴ Subnet Id : 201.44.89.96 → Host bits → All zeros

Subnet no : 3rd subnet

① for a subnet ID Host bits will always be zeros.

② Subnet mask will give the info that how many are the subnet bits & h
are the host bits.

④ IP₁ = 144.89.99.115

Subnet mask : 255.255.252.0

① Subnet Id = ?

② Sbnet no = ?

Soln: ∵ 144 ⇒ Class B

99: 01100011

252: 11111100

01100000 00000000

S H

96

∴ Subnet Id, 144.89.96.0

Subnet mask, 11111111 11111111 111111 00 00000000

N S H

Subnet no. = 24th subnet

No. of hosts in each subnet = $2^9 - 2$; 9 = No. of host bits

Q.⑤ IP₁ = 199.89.79.135 (class C)

Subnet Mask = 255.255.255.224

① Subnet Id

(ii) First host of that subnet

(iii) DBA of that subnet

(iv) Last host of that subnet

Soln: ① 135: 10000111

224: 11100000

128 : 100 00000

S H

Subnet Mask: 255.255.255.224

11111111 11111111 11111111 111 00000

N S H

② Subnet Id = 199.89.79.128

N

③ 100 00001 = 199.89.79.129

S H

(iii) DBA of that subnet: 100 11111 = 199.89.79.159

S H

(iv) 100 11110 = 199.89.79.158

S H

We are subtracting two addresses in the no. of hosts in each subnet because one is used for subnet id and the other one is used for DBA of that subnet.

Q. IP₁ = 199.89.99.115

Subnet Mast = 255.255.255.240

11111111 11111111 11111111 1111 0000

N S H

① 3rd Subnet Id = 0011 0000 = 199.89.99.48

S H

(ii) 5th subnet ID = 0101 0000 = 199.89.99.80

S H

Q. (7) No. of Subnets = $2^R - 2$; R → No. of subnet bits.

(7) IP_1 = 203.83.73.113

Subnet Mask = 255.255.255.224
11111111 11111111 11111111 ↳ 111 00000 (N; S H)

(i) Net Id = ?

Class C, 203.83.73.0 (N; H) ↳ 00000000

(ii) DBA of the network = 203.83.73.255 → 11111111 (N; H)

(iii) First Subnet ID : 001 00000 (S; H)

= 203.83.73.32

(iv) Last Subnet ID

111 00000 (S; H)

DBA: 111 11111 (S; H) X

110 00000 (S; H)

↓

110 11111

We are subtracting two addresses in no of subnets because one is used for Net ID and other one is used for DBA of networks.

(8) IP_1 = 201.44.89.99

IP_2 = 201.44.89.117

IP_3 = 201.44.89.126

Subnet Mask = 255.255.255.240

Identify the IP's belong to same subnet ?

M-I ✓

M-II ✓

Subnet Mask : 255. 255. 255. 240

1111 0000 (S; H)

M-I

99 → 0110 0011 (S) → 6th subnet

117 → 0111 0101 → 7th subnet

M

126 → 0111 1110 (S) → 7th subnet

(9) IP_1 = 199.49.69.113

IP_2 = 199.49.69.62

IP_3 = 199.49.69.73

Subnet Mask : 255.255.255.224

Identify the IP's belong to which host of which subnet ?

Soln:

11111111 11111111 11111111 (N) 111 00000 (S H)

for IP_3 : 73 : 010 01001 (S; H) → 9th host of 2nd subnet

for IP_2 : 62 : 001 11110 (S; H) → 30th host of 1st subnet

for IP_1 : 113 : 011 10001 (S; H) → 17th ——— 3rd subnet

(10) IP = 197.32.63.89
↳ class C

Subnet mask = 255.255.255.240
11111111 (N) 1111 0000 (S H)

(i) 1st host of 3rd subnet
= 00110001 = 197.32.63.49

(ii) 3rd host of 1st subnet
00010011 = ——— 19

(iii) 2nd host of 4th subnet
01000010 = ——— 66

Ans
(11) DBA of subnet is given as: 201.89.39.31 (class C, N) → 00011111
which of the following can be possible subnet mask?

(a) 255.255.255.192 → 11 000000 (S H) to become DBA 111111 (6 1's) ✗
(b) " " " 240 → 1111 0000 to become a DBA 4 1's are req. ✓
(c) " " " 128 → 10000000 (S H) to become a DBA, 7 1's are req. ✗
(d) None

Ans
(12) Given subnet mask: 255.255.255.240 → 1111 0000 (S H)
which of the following can be a DBA of subnet?

(a) 201.89.99.63 → 0011 1111 ✓
(b) 201.89.99.60 → 0011 1101 ✗
(c) 1 → 00000111 ✗
(d) 127 → 0 ✗

(13) IP = 199.89.99.115

(a) Subnet Mask: 255.255.255.224 (N) → 111 00000 (S H) // Continuous Mask

(i) Net Id: 199.89.99.0 (N) . 0 (H) → 00000000

(ii) First subnet Id = 001 00000 (S H) = 199.89.99.32

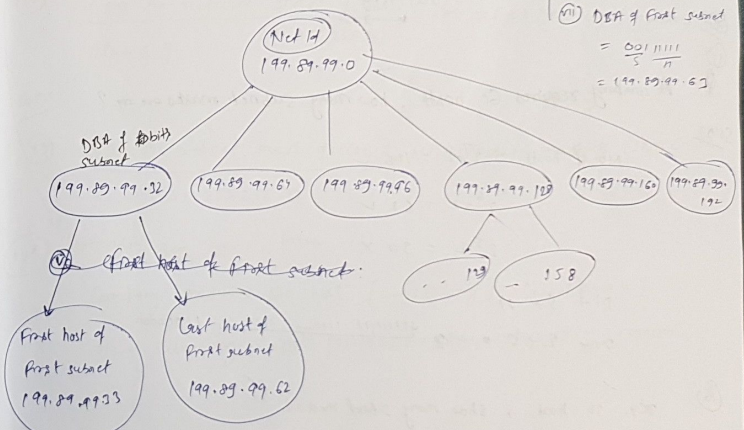
(iii) Second Subnet Id = 010 00000 = 199.89.99.64

(iv) Third Subnet Id = 011 00000 = 199.89.99.96

(v) First host of first subnet
= 001 00001
= 199.89.99.33

(vi) Last host of first subnet
= 001 11110
= 199.89.99.62

(vii) DBA of first subnet
= 001 11111
= 199.89.99.63



If continuous Mask is taken designing of a network will become simple and easy.

MSQ

(14) DP$_1$ = 201.44.89.99 → class C

Subnet Mask = 255.255.255.224

11111111 — 111 00000 (N — S — H)

Which of the following can be the last host of subnet ?

↳ address just before the DBA

↳ address ending with 0.

Soln:

(a) 201.44.89.63 → 00111111 ✗

(b) 201.44.89.126 → 01111110 ✓

(c) 201.44.89.6 → 00000110 ✗

(d) 201.44.82.62 → 00111110 ✓

(15)

Q. A company requires 60 hosts, how many subnet masks are req. ?

Soln:

No. of hosts = $2^7-2 = 126$ ✓

$2^6-2 = 62$ ✓

$2^5-2 = 30$ ✗

N + S + H

24 + 2 + 6 = 32 → 11111111 11111111 11111111 11000000

(16) req. 30 host, show many subnet mask ?

No. of hosts = $2^5-2 = 30$

N + S + H

24 + 3 + 5 = 255.255.255.224

11111111 11111111 11111111 111 00000 (24 — 3 — 5)

(17) Company req. 500 hosts,

subnet mask = ?

$2^9-2 = 512-2 = 510$

No. of hosts in each subnet = $2^9-2 = 510$

11111111 11111111 11111110 00000000 (H — S — H)

255.255.254.0

(18) Can the network mask of class C can act as the subnet mask of Class B ?

255.255.255.0

True

Soln:

(19) Can the subnet mask of class A, act as network mask of class C ?

255.255.255.0

True

(17') Extended Q17

Company requires 500 host [class C only]. Subnet mask = ?

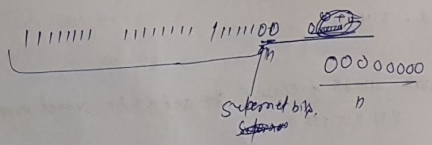
Here Subnetting is not possible for this Supernetting is required.

Supernetting :-

Joining two or more networks to form a larger network according to the requirement of the user; is known as Supernetting.

(i) In class C, if the supernet mask = 255.255.252.0

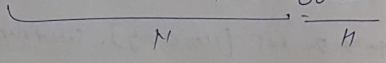
No. of networks that can be joined?



255.255.255.0

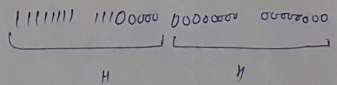
(ii) In class C, if Supernet mask = 255.255.128.0

No of networks that can be joined = $2^1 = 2$



(iii) In class B, if Supernet mask is 255.224.0.0

No. of networks that can be joined? $2^5 = 32$



mod 10

divisor 10

Math 10

Base 10

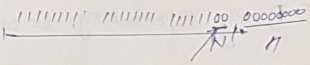
00	10	20
01	11	21
02	12	22
03	13	23
04	14	24
05	15	25
06	16	26
07	17	27
08	18	28
09	19	29

Q. One of the address of a supernet = 200.14.99.99.

Supernet Mask = 255.255.252.0.

Soln

Range of Supernet :-



min & max → DOA of Supernet

Supernet ID

200.14.99.99

255.255.252.0

200.14.96.0

~~Range of Supernet~~

Range of supernet = [Supernet ID → DOA of Supernet]

96.0 = 01100000 . 00000000 (Supernet . h) → 1st network → 256 → 96.0 – 96.255

⋮

01100000 . 11111111

01100001 . 00000000 → 2nd network → 256 → 97.0 – 97.255

01100001 . 11111111

0 11000 10 . 00000000 } 98.0 – 98.255 → 256
0 11000 10 . 11111111

0 1100011 . 00000000 } 99.0 – 99.255 → 256
0 1100011 . 11111111

mod(mn) = mod m × mod n

mod(4×256) = mod 4 × mod 256

4×256 = 1024

Note:
① During supernetting, we can join power of 2 networks
② During supernetting, continuous networks can be joined (even the available networks are discontinous, we will make it as continuous by taking as power of 2).

Ex. Can we form supernetting. (yes)

201.4.8.0
201.4.10.0
201.4.12.0
201.4.14.0

(4+4 = 8)

eg

201.4.8.0 – 201.4.15.255
8
10
11
12
.
.
15

Date: 19/07/22

Classless Addressing:

↓

Block = Group of IP Addresses

Representation of classless Addressing : x.y.z.w/n ← n 1's
(x.y.z.w = IP Address, /n = Mask)

↓

Classless Inter Domain Routing (CIDR Notation)

OR

Slash Notation

No. of IP Addresses in a block = 2^{32-n}

eg: 201.99.89.113/26

/26 = 11111111 11111111 11111111 11000000

255 . 255 . 255 . 192

/27 = 255.255.255.224

11100000

/22 = 255.255.252.0

00 00000000

/17 = 255.255.128.0

eg: One of the addresses of a block = 193.26.99.137/28

① No. of addresses of block = $2^{32-n} = 2^{32-28} = 2^4 = 64$

② Range of Block = ?

137 = 10.00|1001

128 ⇐ 10 000000 (All 0's)

191 ⇐ 10 111111 (All 1's)

} mod 64

⇒ Range = 193.26.99.128/26 to 193.26.99.191/26

1 – 128
11 – 192
111 – 224
1111 – 240
11111 – 248
111111 – 252
1111111 – 254
11111111 – 255

∴ Net Id = First IP Address

= 193.26.99.128/26

First Host = 193.26.99.129/26

Last Host = 193.26.99.190/26

DBA = Last IP Address

= 193.26.99.191/26

eg: One of the addresses of a Block

= 130.14.120.195/27

① No of addresses = $2^{32-n} = 2^{32-27} = 2^5 = 32$

Range of Block : ~~130.14.120.~~

195 : 11000011

11000000 ⇒ 128+64 = 192

11011111 ⇒ 223

∴ Range = 130.14.120.192/27

to

130.14.120.223/27

Note:

The first address of a block should be exactly divisible by number of address of the block.

eg:③ Block contains 16 IP addresses. which of the following can be first address of block :

(a) 203.64.8.8/28

(b) 203.64.8.159/28

✓(c) 203.64.8.192/28 divisible by 16

✓(d) 203.64.8.160/28

$2^{32-n} = 16 = 2^4$

$\Rightarrow n = 28$

M-2 ∵ $16 = 2^4$ ⇒ last 4 bits = 0's

(a) 8 = 00001000 ✗

(b) 159 = 10011111 ✗

(c) 192 = 11000000 ✓

(d) 160 = 10100000 ✓

Q.④ Block contains 1024 IPs addresses. which of the following can be the first address of a block:

No of IPs = 1024 = 2^{10}

⇒ 10 conf. bits must be '0'.

⇒ last two octets need to take

(a) 202.10.2.0/22

(b) 202.10.1.0/22

✓(c) 202.10.160.0/22

✓(d) 202.10.32.0/22

(a) 202.10.2.0

00000010.00000000 ✗

(b) 00000001.00000000 ✗

(c) 160 10100000.00000000 ✓

(d) 32: 00100000.00000000 ✓

eg(5) One of the addresses of a block is given as:

$36.89.99.115/21$

Range = ?

Soln: $n = 21 \rightarrow 2^{32-n} = 2^{32-21} = 2^{11} \Rightarrow 2048$

$\Rightarrow$ 2048 IP addresses

(last 11 bits)

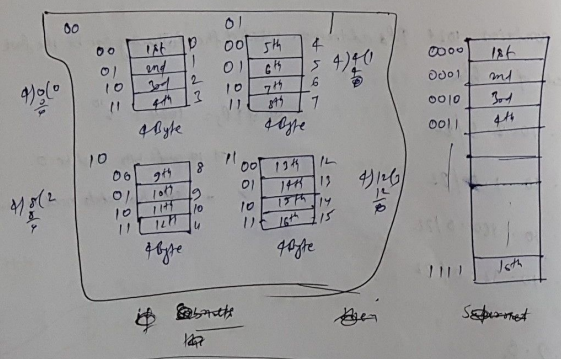
Range: 99.115 (8 bits from here) $= 01100011.01110011$

$\Rightarrow 01100000.00000000 \Rightarrow 96.0$

to

$01100111.11111111 \Rightarrow 103.255$

$\therefore 36.89.96.0/21$ to $36.89.103.255/21$



① If these are networks then → Supernet

② Subnets ← If these are s/w then

Q. One of the addresses of a block is —

$200.89.99.149/26$

This block is divided into 4 equal subblocks (subnets).

Soln: $2^{32-n} = 2^6 = 64$ possibility

0 to 63
64 to 127
128 to 191
192 to 255

$\therefore$ 149 lies b/w

149: 10.010.101

10 000000 = 128
10 111111 = 191

mod 64

$\therefore$ Range: $200.89.99.128/26$ to $200.89.99.191/26$

No. of addresses in each subblock $= \frac{64}{4} = 16 = 2^4$

$= 2^{32-28}$

128 ≤ 1000 0000
149 ≤ 1000 1111

Range of 1st subblock $= 200.89.99.128/28$ to $200.89.99.143/28$

144 ≤ 1001 0000
159 ≤ 1001 1111

Range of 2nd subblock $= 200.89.99.144/28$ to $200.89.99.159/28$

160 ≤ 1010 0000
175 ≤ 1010 1111

Range of 3rd subblock $= 200.89.99.160/28$ to $200.89.99.175/28$

176 ≤ 1011 0000
191 ≤ 1011 1111

Range of 4th $= 200.89.99.176/28$ to $200.89.99.191/28$

mod (mn) = mod m * mod n

mod (64) = mod (4×16)

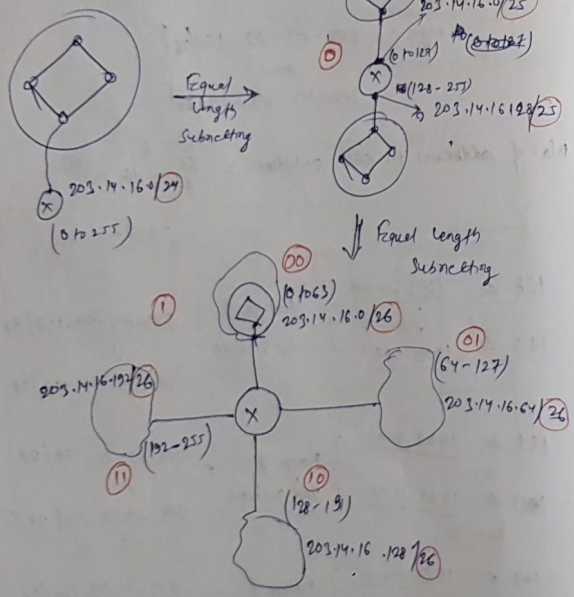
= mod |4| * mod |16|

Diagram View :-

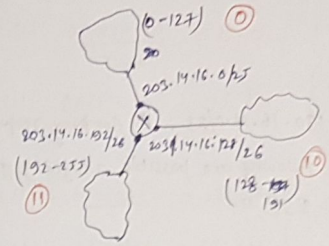
$2^{32-24} = 2^8 = 256 = (0-255)$

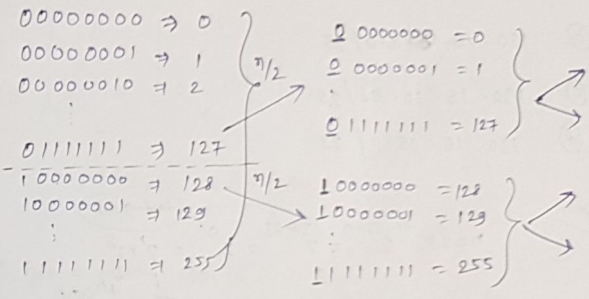
either or

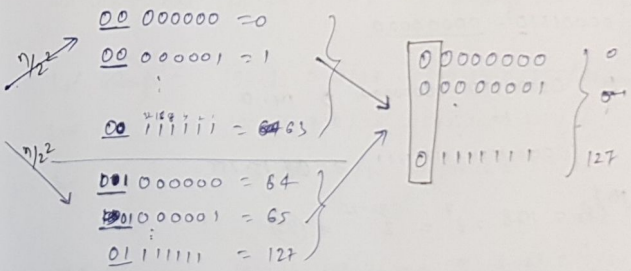
64 64 64 64 128 128

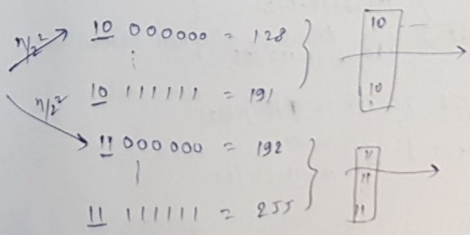


(VLSM) ⇒ Variable length Subnet Mask









GATE [2022]

Model Ques.

Q. An ISP has a block 130.16.14.0/23. A company requires 128 IP addresses. Which of the following are possible assigning of IP addresses to that company by ISP?

(a) 130.16.M.128/25

(b) 130.16.16.0/25

(c) 130.16.18.128/25

(d) 130.16.15.0/25

Soln:

n=23, $2^{32-n} = 2^{32-23} = 2^9 = 2^1 \times 2^8$ (last 9 bits: 3rd octet, 4th octet)

14.0 = 00001110.00000000

∴ Range: 0000 1110.00000000 ⇒ 14.0

to

0000 1111.11111111 ⇒ 15.255

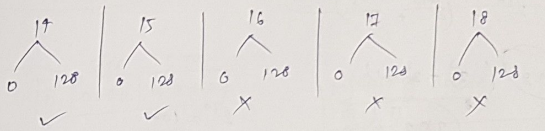
∵ Given No. of IPs = 128 = $2^7 = 2^{32-25}$ ⇒ (25)

0 0000000 = 0
⋮
0 1111111 = 127
} 130.16.14.0/25 to 130.16.14.127/25

1 0000000 = 128
1 1111111 = 255
} 130.16.14.128/25 to 130.16.14.255/25

0000 1111.00000000 = 15.0
0000 1111.01111111 = 15.127
} 130.16.15.0/25 to 130.16.15.127/25

0000 1111.10000000 = 15.128
0000 1111.11111111 = 15.255
} 130.16.15.128/25 to 130.16.15.255/25



⇒ option a & d Ans.

Q. An ISP has a block 190.16.0.0/16. ($2^{32-16} = 2^{16}$)

1st Group has 128 companies, each company requires 256 IP addresses ($2^8 = 2^{32-24}$)

1st company = 190.16.0.0/24 – 190.16.0.255/24

2nd " = 190.16.1.0/24 – 190.16.1.255/24

3rd " = 190.16.2.0/24 – 190.16.2.255/24

128th company = 190.16.127.0/24 – 190.16.127.255/24

2nd Group has 64 companies, each company req. 128 IP add. ($2^7 = 2^{32-25}$)

1st company = 190.16.0.0/25 – 190.16.0.127/25

2nd " = 190.16.0.128/25 – 190.16.0.255/25

63 Company = 190.16.63.0/25 – 190.16.63.127/25

190.16.128.0

Calculate the leftover IP addresses with the ISP.

Soln:

$$2^{16} - [\underbrace{128 * 256}_{\text{Group-1}} + \underbrace{64 * 128}_{\text{Group-2}}]$$

$$2^{16} - (2^{15} + 2^{13})$$

$$3 \times 2^{13} \left(2^3 - 2^2 - 1\right)$$

$$3 \times 2^{13}$$

$$= 24576$$

$2^{10} = 1024$

2048

4096

8192

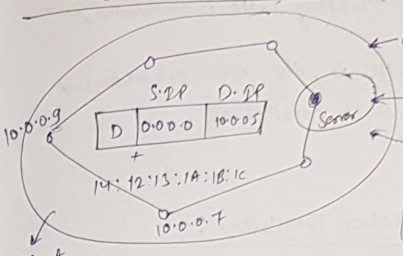
16384

24576

(IP Address)

- Private IP Address
  1. Communicating in LAN
  2. Loading Networking (NOS) Operating System (Server)
  3. Free of Cost
  4. eg. 10.0.0.0 – 10.255.255.255
     172.16.0.0 – 172.31.255.255
     192.168.0.0 – 192.168.255.255
  5. Will not get Internet Service
- Public IP Address
  1. Scope is globally unique.
  2. Control of ISP
  3. Not free of cost.
     eg: 14.5.6.7

Assigning Private IP Addresses in a LAN :-



	S.IP	D.IP	LBA
D	10.0.0.5	255.255.255.255	

DHCP client

	S.IP	D.IP
D	0.0.0.0	10.0.0.5

Mapping Table

IP	MAC
10.0.0.7	16:14:12:13:14:15
10.0.0.9	14:12:13:1A:1B:1C

Client → DOS, XP

NOS Server → Windows 2003 → DOS
NT

Commands
+
Networking Protocols

DHCP
HTTP
FTP

→ Once the server is loaded with Network Operating System (NOS), it will get group of Private IP Addresses out of which one IP is assigned to server.

→ The server's IP is informed to all the clients using Limited Broadcast Address (LBA).

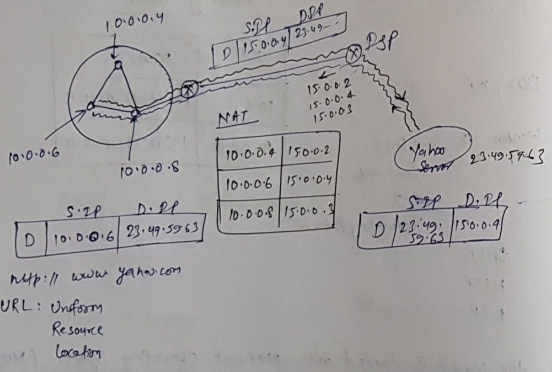
→ When the client doesn't have any IP address still it can send a request packet using 0.0.0.0 as the source IP address (along with that MAC address is also transmitted so that server can recognize which system is requesting).

→ In response to the request, an IP address is assigned to that computer and a Mapping Table is maintained.

→ The purpose of Mapping Table is, the admin can understand which IP is assigned to which computer.

S-NAT (Static - Network Address Translation) :-

(One to one Mapping)



http:// www.yahoo.com

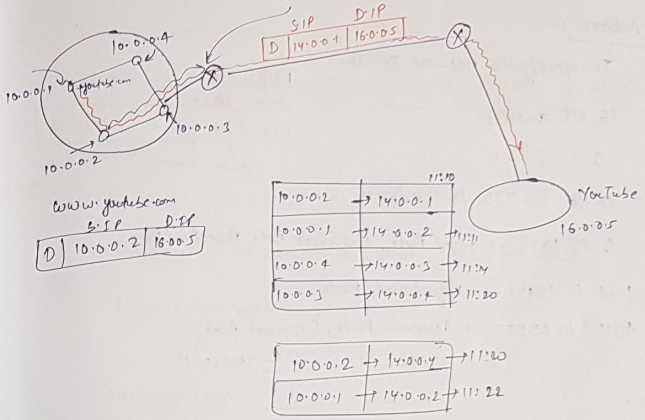
URL : Uniform Resource Locator

→ If 'n' systems are available in LAN then 'n' Public IPs are purchased in Static NAT (Cost becomes high).

→ Static NAT comes under One to One Mapping (ie; the mapping table at the router is fixed. (So the processing time at the router is less).

→ The drawback of S-NAT is that the internal systems of a LAN can be compromized by continuously observing the packets.

D-NAT (Dynamic NAT) :-



→ In case of the Dynamic NAT, when 'n' systems are in the LAN network then 'm' public IPs are required (=Cost becomes high).

→ The processing time at the local router is high bcoz everytime a session is started for a system, mapping is done.

→ In Dynamic NAT, security is high bcoz mapping is dynamic ie; Internal systems can not be compromized.

P- NAT (Port - NAT)

Port Address :-

→ To identify the network process.

→ 16 bit address

0 to $2^{16}-1$

→ 0 to 65535 port address.

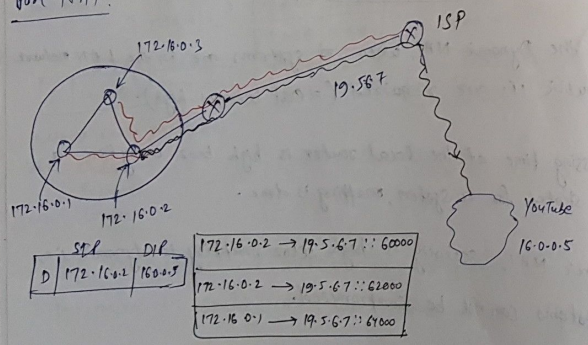
0 to 1023 → Fixed Ports, Universal Ports, Predefined Ports

1024 to 49151 → Registered Ports

49152 to 65535 → Dynamic Ports, Ephemeral Ports
↑ short lived

HTTP: 80
SMTP: 25
FTP: 21, 20
(Data Control)

Port NAT:



SIP	DIP
D | 172.16.0.2	160.0.5

172.16.0.2 → 19.5.6.7 :: 60000
172.16.0.2 → 19.5.6.7 :: 62000
172.16.0.1 → 19.5.6.7 :: 64000

Date: 20/7/22

Special Cases:

① IP_1 = 200.99.89.115 (Class C)

Calculate host on this network. → Make the n/w bits as all 0's.

Shortcut: 0.0.0.115 for class 'C'

Method

Mask for Class C : 255.255.255.0

Complement of IP address is called 'Wild Card Mask.'

∴ Wild Card Mask = 0.0.0.255

∵ IP_1 = 200.99.89.115

Host on this N/w: 0.0.0.115

(Bitwise AND op. b/w Wild Card Mask & IP address gives Host on the N/w)

eg ① —— ② (Not possible if Source & dest have different N/ws)

10.0.0.5 172.16.0.6

SIP	DIP
D | 10.0.0.5 (N)	172.16.0.6 (N)

S.IP	D.IP
D | 0.0.0.5	0.0.0.6

① —— ②

172.16.0.1 172.16.0.4

SIP	DIP
D | 172.16.0.1	~~0.0.0.0~~ 172.16.0.4

SIP	DIP
D | 0.0.0.1	0.0.0.4

eg. (Class B)

IP = 144.19.89.99 (N)

Host = 0.0.89.99 on this N/w

(2) DP = [No. of Subnets = $2^K - 2$]

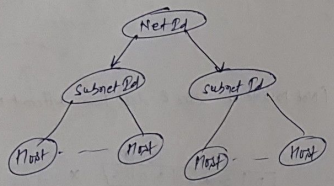
IP_1 = 201.44.55.89
↑ class C

Subnet Mask = 255.255.255.128

∵ N/w wishes to form subnets
OR
Explicitly configured zero subnet and DBA subnet
} No. of subnets = 2^K

$2^1 = 2$ subnets

11111111 11111111 11111111 1 0000000
N S H



(i) Zero Subnet Id = 0 0000000 = 201.44.55.0
H

(ii) First host of zero subnet = 0 0000001 = 201.44.55.1
H

(iii) Last ——— = 0 1111110 = 201.44.55.126

(iv) DBA of Zero Subnet = 0 1111111 = 201.44.55.127

(v) DBA of Subnet Id = 1 0000000 = 201.44.55.128
S H

(vi) First host of DBA subnet = 1 0000001 = 201.44.55.129
S H

(vii) Last ——— = 1 1111110 = 201.44.55.254
S H

(viii) DBA of DBA Subnet = 1 11111111 = 201.44.55.255
S H

(3) IP_1 = 201.55.66.87

N/w wishes to form subnets

Subnet Mask = 255.255.255.224

No. of subnets = 11111111 . 11111111 11111111 111 00000
N S H

$2^K = 2^3 = 8$

(4) IP_1 = 202.89.99.113
↑ class C

Subnet Mask = 255.255.255.41 // Discontinuous Mask, not preferred bcz. It is Non-Deterministic.

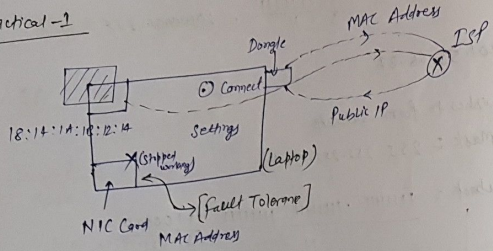
11111111 11111111 11111111 00101001
N Host Bits
Subnet bits

(i) First Subnet Id (001 00000) = 0 0 0 0 0 0 0 1 (--0-0--1)
= 202.89.99.1

(ii) Find Subnet Id (010 00000) = 0 0 0 0 1 0 0 0 (---0-1---)
= 202.89.99.8

(iii) Third Subnet Id (011 00000) = 0 0 0 0 1 0 0 1 (---0-1--1)
= 202.89.99.9

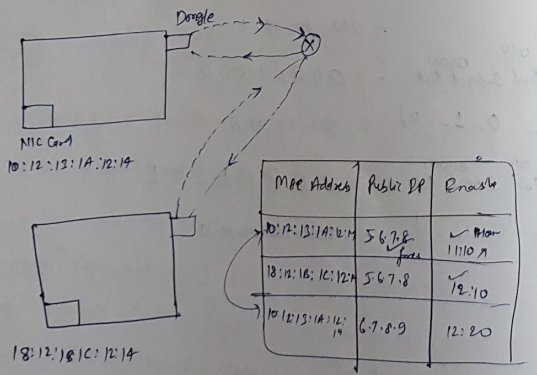
Practical - 1



MAC Address	Public IP	Enable
16:12:10:12:14:1A	4.5.8.7	✓
18:14:1A:16:12:14	4.5.8.7	✓

A computer can have multiple MAC Addresses to support fault Tolerance.

Practical - 2

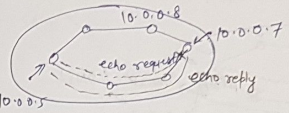


MAC Address	Public IP	Enable
10:12:13:1A:12:14	5.6.7.8	✓ Plan 1:10
18:12:18:1C:12:14	5.6.7.8	12:10
10:12:13:1A:12:14	6.7.8.9	12:20

A computer can have multiple IP addresses at different instances of time.

Ping ⇒ PING ⇒ Packet Internet Grapher
(ping)

Networking Command



cmd

C:/> ping -t 10.0.0.7 ↵

	S.IP	D.IP
D	10.0.0.5	10.0.0.7

Positive Ack ⇐ T_{TL} : 4msec R_{TT}: 6.8msec

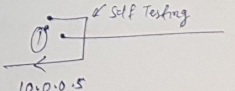
(ICMP Protocol) C:/> ping -t 10.0.0.7 ↵ (OR)

Negative Ack ⇐ Destination Unreachable

ping is used to troubleshoot whether the other systems are properly connected in the network.

0 – 127

Class A (1–126) → 127.x.y.z (Loop Back Address)



this packet will never enter into N/w

loop back Address

C:/> ping -t 127.0.0.1

	S.IP	D.IP
D	10.0.0.5	127.0.0.1

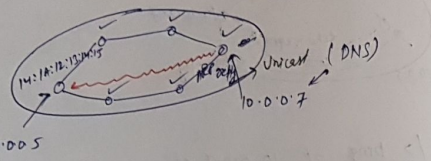
D	0.0.0.0	127.0.0.1

Positive Acks ⇐ T_{TL} = 0.014 ms
R_{TT} = 0.08 ms

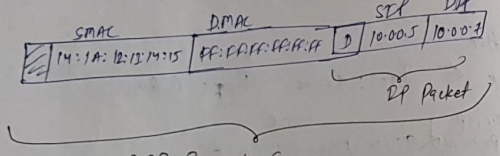
Loop back address will always be used as Destination IP.

ARP (Address Resolution Protocol) :-

↳ To find out the Dest MAC Address.



C:/> ping -t 10.0.0.7



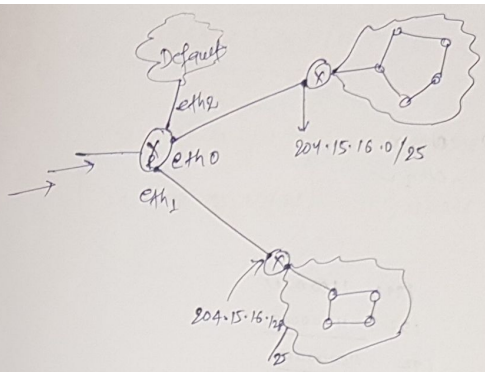
Broadcast MAC Address = FF:FF:FF:FF:FF:FF

Sorce will Broadcast
and Dest will reply in a Unicast way.

→ ARP request packet contains Source IP, Destination IP, source MAC but it doesnot contain Destination MAC (ARP req. packet is a broadcast packet).

→ ARP reply is a Unicast, replied with Destination MAC.

Q.



Packet reached to Router R with the destination IP of the packet is 204.15.16.190 then the packet will be forwarded to -

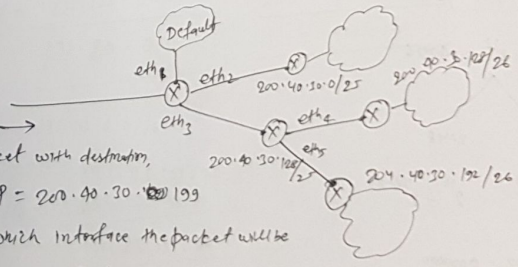
(a) eth0 (b) eth1 (c) eth2 (d) none.

Soln: 204.15.16.190

/25 = 255.255.255.128

(i) 204.15.16.128 → eth1

(ii)



Packet with destination,
IP = 200.40.30.199

On which interface the packet will be forwarded by router:

(a) eth2 (b) eth3, (c) eth4 (d) eth5 (e) eth1

200 . 40 . 30 . 199
/25 = 255 . 255 . 255 . 128
200 . 40 . 30 . 128 ⇒ eth2 ✗
eth3 ✓

again

200 . 40 . 30 . 199
/26 = 255 . 255 . 255 . 192
200 . 40 . 30 . 192

199 : 11000111
192 : 11000000
192 11000000

⇒ eth5 ✓ Any

When ever a packet comes to the router and router identifies that more than 1 path is available then the path which is having more no of 1's in the mask, is preferred (that is the place where exactly hosts are available).

Pg-87

T-6 245 . 248 . 128 . 0/20

$2^{32-20} = 2^{12} = 4096$

2048 2048

$2^3 \times 2^8 \leq 2^{11} = 2^{32-21}$ $2^{11} = 2^{32-21}$

128.0 = 10000 000 . 0000000
135.255 = 10000 111 . 11111111
136 0 = 10001 000 . 00000000
143.255 = 10001 111 . 11111111

245 . 248 . 128 . 0/20

245 . 248 . 128 . 0/21
⇒
245 . 248 . 135 . 255/21

245 . 248 . 136 . 0/21
⇒
245 . 248 . 143 . 255/21

T-7

① 131 . 16 . 0 . 0 /12

131 . 23 . 151 . 76
/12 = 255 . 240 . 0 . 0
131 . 16 . 0 . 0

23 = 0001 0111
240 = 1111 0000
16 = 0001 0000

② 131 . 88 . 0 . 0/14

131 . 23 . 151 . 76
/14 = 252 . 252 . 0 . 0
131 . 20 . 0 . 0

23 = 0001 0111
252 = 1111 1100
20 = 0001 0100

③ 131 . 19 . 0 . 0/16

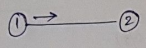
131 . 23 . 151 . 76
/16 = 255 . 255 . 0 . 0
131 . 23 . 151 . 76

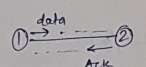
④ 131 . 22 . 00/15 ✓

131 . 23 . 151 . 76
/15 = 255 . 254 . 0 . 0
131 . 22 . 0 . 0

→ Longest Path one will be the ans.
⇒ Any - 1 . not 2

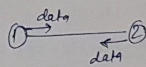
Basic Concepts :-


: Simplex Transmission



: Half - Duplex Transmission

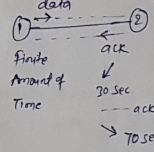
eg Walkie Talkie



: Full Duplex Transmission

eg: Lane Road.

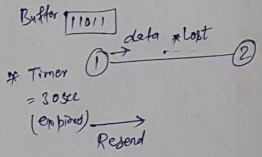
Timer is reg.



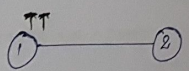
= 60sec finite Amount of Time

Worst Case Time (within this time ack should be received).

When error the data is transmitted, a timer is started because waiting time is finite.



→ Whenever the data is lost ~~or timer~~ automatically the timer is expired, we can resend the data by taking the data from the buffer.



Transmission Time = Data size / Bandwidth

eg: Data size = 2 K bits

BW = 10 Mbps

$TT = \frac{2 \times 10^3 \text{ bits}}{10^7 \text{ bits/sec}} = 2 \times 10^{-4}$ sec

$T.T = 200 \times 10^{-6}$ sec

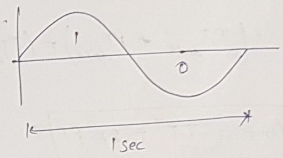
$= 200$ μsec.

Kilo $= 10^3$, milli $= 10^{-3}$

Mega $= 10^6$, micro $= 10^{-6}$

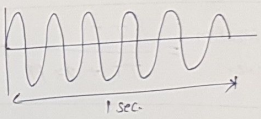
Giga $= 10^9$, nano $= 10^{-9}$

Lower Frequency :



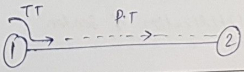
eg. 2 bits/sec

Higher Frequency :



eg 10^7 bits/sec.

High frequencies will travel longer distances in small amount of time



Propagation Time = Length of Cable / Velocity of Medium

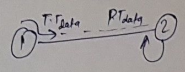
eg $l = 2$km

$v = 2 \times 10^8$ m/s

$PT = \frac{2 \times 10^3 \text{ m} \times s}{2 \times 10^8 \text{ m}} = 10^{-5}$ s

$= 10^{-5}$ s $= \frac{10 \times 10^{-5}}{10}$ s $= 10^{-6}$ s $= 10$ μsec Ans

* Timer



TT_{ack}.

for all practical purposes, Ack size << Data size

$$TT_{ack} = \frac{\text{Ack size}}{BW}$$

TT_{ack} is Negligible.

$$PT_{ack} = PT_{data}$$

$$\text{Total Time} = (TT_{data} + PT_{data}) + (\cancel{TT_{ack}}^{\approx 0} + PT_{ack})$$

$$\therefore \boxed{\text{Total Time} = TT + 2*PT}$$

$$\boxed{\%\ \text{Link Utilization of Sender} = \frac{TT}{TT + 2*PT} * 100\%}$$

The time taken to place the data on the channel out of the total time given is known as Link Utilization of Sender.

(3) $\%\ LU = 50\%$

$$50 = \frac{TT}{TT + 2PT} \times 100$$

$$\Rightarrow TT + 2PT = 2TT$$

$$\Rightarrow \boxed{TT = 2PT}$$

(4) $\%\ LU = 50\%$

$l = 200\ m$

$V = 2 \times 10^8\ m/s$

$BW = 10\ mbps$

Data size = ?

Data size = $T.T \times BW$

$\because \%\ LU = \frac{TT}{TT + 2 \cdot PT}$

$PT = \frac{l}{V} = \frac{200\ m}{2 \times 10^8\ m/s} = 10^{-6}\ s$ - (1)

$TT = 2 \times PT$

$\frac{\text{Data size}}{BW} = 2 \times \frac{l}{V} \Rightarrow \frac{x}{10^7} = 2 \times \frac{200}{2 \times 10^8} = 10^{-7} = 20\ bits$

ex (5) $BW = 100\ mbps$

Calc. 1-bit delay.

Soln: $BW = 100\ mbps$

$\Rightarrow 1\ sec = 10^8\ bits$

$\Rightarrow 1\ bit = 10^{-8}\ sec$

$= 10^{-6} \times 10^{-2}\ sec$

$= \frac{1}{100}\ \mu sec$

$= 0.01\ \mu sec.$ Ans

(6) BW = 100 mbps

$V = 2 \times 10^8$ m/sec

Cal. 1 bit delay in meter of cable.

Soln:

∵ BW = 100 mbps

⇒ 1 Sec = 10^8 bits

1-bit delay = 10^{-8} sec

∵ $V = 2 \times 10^8$ m/sec

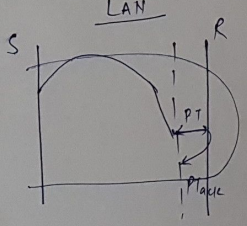
⇒ 1 sec → 2×10^8 m

∴ 10^{-8} sec → $2 \times 10^8 \times 10^{-8}$ m of cable

= 2 m of cable.

Prototype Analysis :-

LAN

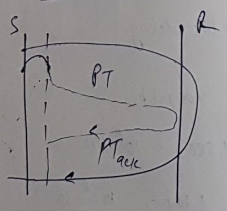


TT + 2PT

L is small

PT↓, TT↑

WAN / Internet



TT + 2PT.

L is Large

$PT = \frac{L}{V}$

PT↑, TT↓

(7) BW = 100 mbps

RTT = 50 MS

Round Trip time

Cal. no: of bits that are transmitted in RTT in LAN ?

Soln:

1 sec = 10^8 bits

RTT = 50 MS = 50×10^{-6} sec

No of bits in RTT = $50 \times 10^{-6} \times 10^8$

= 5000 bits

(8) BW = 50 Mbps

RTT = 50 M sec

Data Size = 25 bits

Cal. No of data units that can be transmitted in LAN ?

Soln:

Throughput,

(6) **Throughput :-**

The rate at which, user transmits the data is known as the Throughput.

$$\text{Throughput} = \frac{\text{Data Size}}{TT + 2 * PT}$$

Soln

(8) eg. BW = 100 mbps

l = 200 m, $v = 2 \times 10^8$ m/sec

Data size = 100 bits

Throughput = ?

$$T\text{put} = \frac{\text{Data size}}{TT + 2 \times PT} = \frac{100 \text{ bits}}{\frac{\text{Data size}}{BW} + 2 \times \frac{l}{v}}$$

$$= \frac{100 \text{ bits}}{\frac{100 \text{ bits}}{100 \text{ mbps}} + 2 \times \frac{200 \text{ m}}{2 \times 10^8 \text{ m/s}}}$$

$$= \frac{100 \text{ bit}}{(1 \times 10^{-6} + 2 \times 10^{-6}) \text{ s}}$$

$\frac{100 \times 10^6}{3}$

Bandwidth 33.33×10^6 bits/

33.33 Mb/sec

$\because$ BW = 100 mbps

& T-put = 33.33 mbps

$\Rightarrow$ We can say $\boxed{\text{Throughput} \leq BW}$

$f(n) \leq C \cdot g(n)$

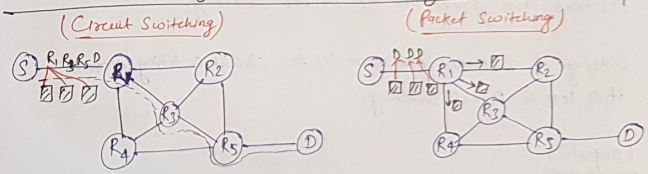
$$\because \%\ LU = \frac{T \cdot T}{T \cdot T + 2 * PT} \times 100\ \%$$

$$= \frac{\text{Data Size} / B.W}{TT + 2\,PT} \times 100\ \% \quad \left(\text{Data Size} / B.W = \text{Throughput}\right)$$

$$\Rightarrow \boxed{\%\ LU = \frac{\text{Throughput}}{BW} \times 100\ \%}$$

In the prev. ex. $\%\ LU = \frac{33.33}{100} \times 100\ \% = 33.33\ \%$

Circuit Switching & Packet Switching :-



(i) Connection Establishment
(ii) Data Transfer
(iii) Connection Release

(i) Data Transfer

(1) In Circuit Switching, there are three phases : Connection Establishment, Data Transfer & Connection release where as in Packet switching, directly data can be transmitted.

(2) Incase of Circuit switching, each packet will have entire path address which is given by the source where as in packet switching, each packet will have the destination address, the intermediate path will be decided by routers.

③ Circuit Switching is not a Store & Forward Technique whereas, Packet Switching is Store & forward Technique bcoz packet are Stored, Routing algorithms are applied and forwarded on the best path.

④ In circuit switching, transmission of the data is done by source where as In Packet Switching, transmission of data is done not only by the source but also by mediating routers.

⑤ In Circuit switching, the delay between the data packets is uniform where as In Packet Switching, the delay between the data packets is variable.

⑥ Resource Reservation is a feature of Circuit Switching where as Resources are shared in the Packet Switching.

⑦ Wastage of resources are more in the circuit switching where as it is less in Packet Switching.

⑧ Congestion:

If more no. of packets are coming in less amount of time then the router buffer will be full in no time that is the router is congested i.e) some packets will be dropped,

In Circuit switching, congestion can happen during connection establishment phase where as in Packet switching, congestion can happen during data transfer phase.

⑨ Circuit Switching is not a fault Tolerent technique where as Packet Switching is a fault tolerant technique bcoz whenever the link gets broken they can be diverted via other alternate paths.

⑩ Circuit Switching is reliable where as Packet Switching in not reliable.

⑪ Circuit Switching is used for sending long messages where as Packet Switching is used for sending short messages

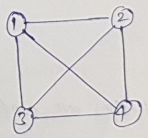
⑫ Circuit Switching is slow where as Packet Switching is fast.

LAN Topologies :-

1.) Mesh Topology
2.) Star Topology
3.) Bus Topology
} Physical Topology

1.) IEEE 802.3
2.) IEEE 802.11
} Logical Topology

1.) Mesh Topology :- Every system is connected to every other system with a cable.



4 devices, 6 links are required

∴ for 'n' devices, $^nC_2$ links are required.

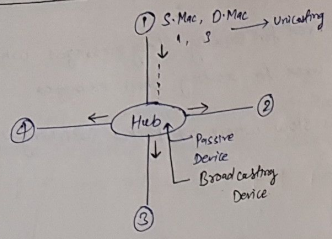
eg for 100 devices, $^{100}C_2 = \frac{100 \times 99}{2} = 4950$ cables

Adv.: If 'n' is small, $O(n^2)$ is small.
If 'n' is large, $O(n^2)$ is very large

Disadv: Cost is very high, maintainance Difficulties

For small group or project, Mesh Topology is preferable (Reliable & Secure)

② Star Topology →



for 4 devices, 4 links are required

100 " 100 " " "

⇒ Cost is less

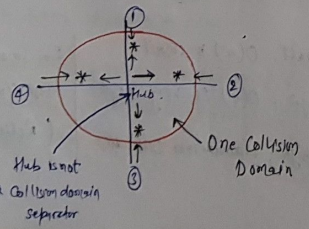
→ Hub is broadcasting device beoz whenever a packet comes to hub. It will be diverted in all the directions.

Collision :

Two or more station's data interfere each other, it is faceted as Collision.

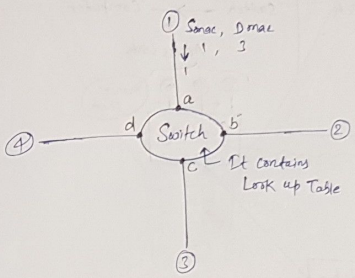
Collision Domain :-

The place or the area where the collisions are confined is known as Collision Domain.

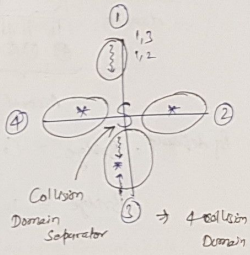


If hub is used as a centre device then entire network has same collision domain (Single Collision Domain) i.e: Hub is not a collision domain separator.

Switch :



Interface	Station
a	1
b	2
c	3
d	4

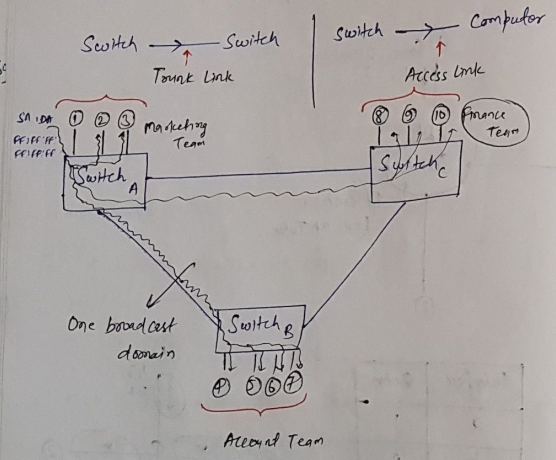


By default, Switch is a collision domain separator i.e: if switch is used as Centric device then each port has a separate collision domain.

for n ports → n collision domains

Broadcast MAC Address

FF:FF:FF:FF:FF:FF



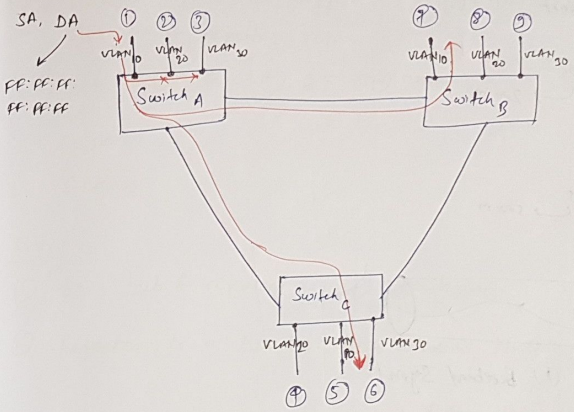
By default, Bridge = Collision domain separator

Bridge = is not a broadcast separator.

If LAN ⇒ VLAN (Virtual LAN)

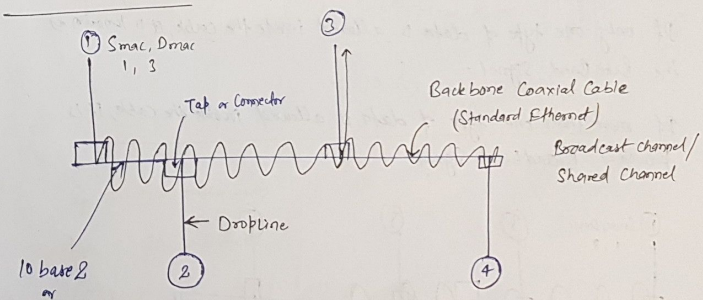
↳ by configuring the ports of switch.

eg: VLAN 10 ⇒ Marketing
VLAN 20 ⇒ Account
VLAN 30 ⇒ Finance



If a LAN is converted into a VLAN then switch will act as the broadcast domain separator.

③ Bus Topology :



for 4 devices, 4 dropline + 1 coaxial cable

∴ for n device = n dropline + 1 coaxial cable

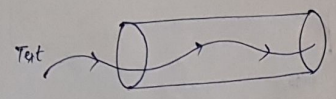
Standard Ethernet

↳ (10) base (2) → 200 m

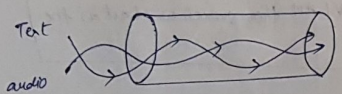
BW: 10 mbps

or

10 base 5 → 500 m



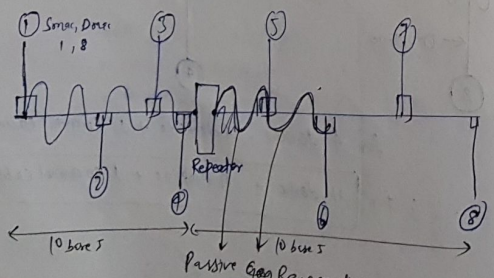
(i) Baseband Signal



(ii) Broadband Signal

If only one type of data is allowed inside the cable, it is known as the Base Band Signal.

If more than one type of data is allowed inside the cable, it is known as Broadband Signal.



eg 3000 m of bus topology LAN is required. 10 base 5 cables are used then no. of repeaters req.

(a) 6 (b) 7 (c) 5 (d) none

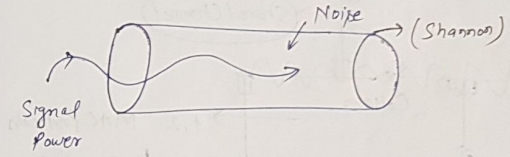
$l = 500$ m

6 cables

Note:

(1) Both hub & repeater are passive devices.

(2) Repeater is a two port device where as Hub is a multiport device



Signal to Noise Ratio = $\log_{10} \frac{\text{Signal Power}}{\text{Noise Power}}$ bels

$= 10 \log_{10} \frac{S_p}{N_p}$ decibels (dB)

eg: $S_p = 100$ milliwatts

$N_p = 10$ milliwatts

$\left(\frac{S}{N}\right)_{Ratio} = ?$ $\quad 10 \times \log_{10} \frac{S_p}{N_p} = 10 \times \log_{10}\left(\frac{10^{-1}}{10^{-2}}\right)$

$= +10$ dB

$\Rightarrow$ Signal Power is dominating Noise Power

(6) eg: (2) $S_p = 10$ mW

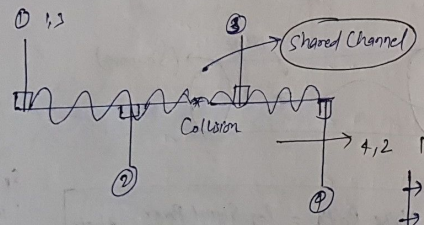
$N_p = 1000$ mW

Soln

$$\left(\frac{S}{N}\right)_{Ratio} = 10 \log_{10} \frac{10}{1000} = -20\,dB\ (-ve)$$

⇒ Noise Power is dominating signal Power.

Maximum Data Rate = $B \log_2 \left(1 + \frac{S}{N}\right)$



MAC Protocol

Medium Access Control Protocol

MAC Protocols

- Pure Aloha
- Slotted Aloha
- CSMA
- CSMA/CD
- CSMA/CA

Note:

(1) When more than one station transmit the data in the shared channel then there is a possibility of collisions.

(2) When there are more no of collisions then throughput will decrease so protocols have to be applied such that collisions are reduced and throughput is increased.

Lab

IPv4 Addressing

Q.3 $2048 = 2^{11} = 2^{32-21}$

by /21

Q.4 $IP_1 = 172.60.50.2$

OSI Model → 7 Layers

(Open Systems Interconnection)

Data — Sender

Message ← Application Layer
Presentation Layer
Session Layer

TCP Segment, UDP Datagram ← Transport Layer → Gateway: All Layer Switch, Active Device
↳ Port Address (16 bit)

Packets ← Network Layer → Router: Three Layer Switch
↳ IP Address (32 bit) WAN (Internet)

Frame ← Data Link Layer → Bridge: Two Layer Switch
↳ MAC Address (48 bit address)

Bits ← Physical Layer → Repeater, Hubs,
(PDNT SPA) Passive Devices

Data Link Layer is responsible for node to node delivery and the systems will be identified by MAC address.
↳ Scope of MAC address is Local.

Network Layer is responsible for source to destination delivery ~~between~~ across the networks

Piggybacking ↓ Data+Ack

Transport Layer is responsible for process to process delivery and end to end delivery and the process will be identified by Port Address.

Application Layer (AH: App. Header)	AH | Data	Application Layer
Presentation Layer (PH: Presn. Header)	PH | AH | Data	Presentation Layer
Session Layer	SH | PH | AH | Data	Session Layer
Transport Layer	TH | SH | PH | AH | Data	Transport Layer
Network Layer	NH | TH | SH | PH | AH | Data	Network Layer
Data Link Layer	DLH | NH | TH | SH | PH | AH | Data	Data Link Layer
Physical Layer	PLH | DLH | NH | TH | SH | PH | AH | Data	Physical Layer

Bits

Network Architecture is known as Protocol Stack Architecture because the last header that is attached at the sender side is the first header that is removed at the receiver side.

Deals with

Application Layer: Application Services like http, ftp, SMTP, DNS, TELNET

Presentation Layer: Syntax and Semantics of data, Encryption & Decryption (rules) (meaning)

Session Layer: Session and Dialog Control, Session Time

Transport Layer: Flow Control, Error Control, Segmentation, TCP, UDP, (Global) Congestion Policies

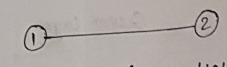
Network Layer: Traffic Sharing, Routing Algorithms, IP, ICMP, Fragmentation

Data Link Layer: Flow Control, Error Control, Access Control, Framing (Local)

Physical Layer: Physical & Electrical properties of cable.

7 Layers of OSI model has been reduced to 5 layers of TCP/IP in which presentation & session layer functionalities are included in Application Layer.

Soln



Error Control Policies

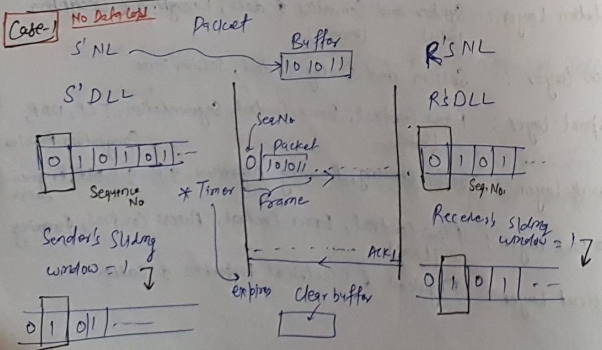
Error Detection Policy	Error Correction Policy
i) Parity	i) Hamming Code
ii) Checksum	
iii) CRC	

Data Link Layer:

Flow Control Policies.

Stop & Wait ARQ → (Automatic Repeat Request)

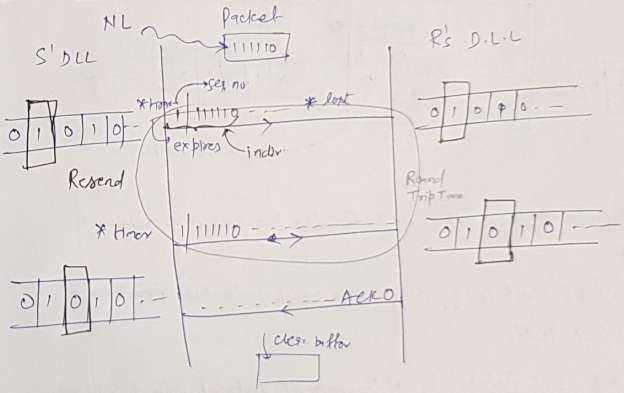
Case-1 No Data Lost



→ Once the data is reached to the receiver, the sequence no of the data is compared with receiver's sliding window no. If there is a match, data will be accepted and receiver window will slide by 1 bit (If there is a mismatch, data will not be accepted).

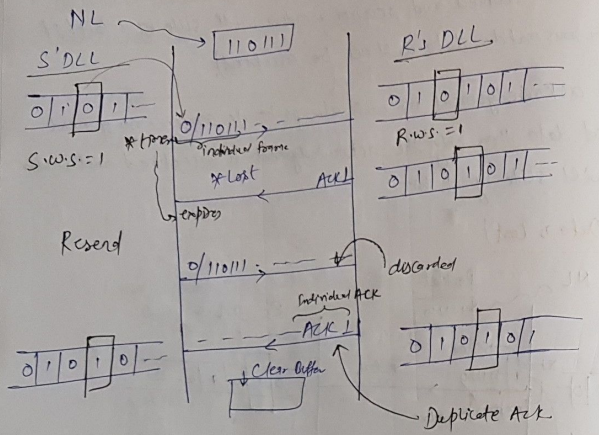
→ The acknowledgement no. will always be the sequence no of next expected data then only the acknowledgement is accepted and sender window will slide by 1 bit.

Case-2 (Data is Lost)



→ Whenever the data is lost, automatically the timer will expire then the protocol itself resends the data then this data is accepted and once the ack is reached to the sender, ack is accepted and sender window will slide by 1 bit.

Case-II (when ACK is lost) :-



→ Duplicate Ack is the ACK for the previous ACK which is lost

→ In Stop & Wait ARQ, it supports only individual frames and individual ACKs.

→ Stop & Wait Protocol is a theoretical protocol without sliding window where as Stop & Wait ARQ is a practical protocol with sliding window.

→ In all sliding window protocols, the maximum sender window & maximum receiver window will always be equal to distinct sequence no count

→ There is no pipelining in Stop & wait ARQ, so utilization is less.

→ In all sliding window protocols, the maximum sender window size indicates no of frames that are transmitted in Round trip time.

eg:

BW = 100 Mbps

RTT = 50 msec

Frame size = 25 bits

1 sec = 10^8 bits

50 msec = $50 \times 10^{-6} \times 10^8$ bits

No. of bits in RTT = 5000 bits

No. of frames in RTT = $\frac{5000}{25} = 200$ = $\frac{\text{No. of bits}}{\text{Frame size}}$

Bw utilization % in Stop & wait ARQ = $\frac{1}{200} \times 100 = 0.5\%$

⇒ Utilization is very less

```
Seq=0;
for (i=0 ; i<n; i++)
{
   for (j=0; j<2; j++)
      { seq. = (seq+j) mod 2;
        pf ("%d", seq);
      }
}
```

i=0 & j=0,1 → 2

i=1, j=0,1 → 2

i=2, j=0,1 → 2

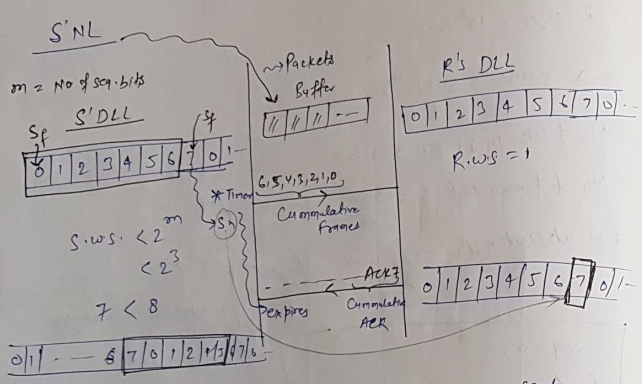
[2+2+2+ ... n] ⇒ (2n)

In Go Back N ARQ,

Seq. bit	Seq No
1 bit	0, 1
2 bits	00, 01, 10, 11 — 0, 1, 2, 3
3 bits	000, 001, ... 111 — 0, 1, 2, 3, 4, 5, 6, 7

Go Back N ARQ :- (Stop & wait ARQ is a special case of Go Back N ARQ)

Case-1 Packet & ACK reached safely:



eg: 5 bit sequence no. is used. What is the maximum sender window size and receiver's window size in Go Back N ARQ.

	SWS	RWS
Go Back N ARQ	31	1

$\because SWS < 2^m$

$< 2^5$

< 32

$\Rightarrow 31$

eg: In Go Back N ARQ, in the sender window condn i.e; $SWS < 2^m$ when $m=1$, it behaves as Stop & wait ARQ.

$\Rightarrow SWS = 1$ & $RWS = 1$

Go Back N ARQ supports both Individual ACK as well as Cummulative ACK (Cummulative ACK is the best option bcoz we are able to convey the information with less no. of ACKs.

eg: '7' is maximum sender window size in Go Back N ARQ,

No of sequence bits are ___ $\log_2(1+7)$

$\because SWS < 2^m$ $= \log_2(1+8)$

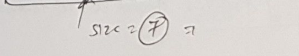
$\Rightarrow SWS_{max} = 2^m - 1$

$\Rightarrow 2^m = 1 + SWS_{max}$

$\Rightarrow m = \log_2(1 + SWS_{max})$

eg: Maximum seq. no. in Go Back N ARQ is 'P', maximum sized sender's window ___

(a) P-1 (b) P+1 (c) P (d) none

eg:  P=7

size = (7) $\Rightarrow$

eg: BW. = 50 mbps $\Rightarrow$ 50×10^6 bit/sec

RTT = 10 M sec $\rightarrow$ 1 sec = 5×10^7

10×10^{-6} sec

frame size = 5 bits $\therefore$ in 10 MSec = $10 \times 10^{-6} \times 5 \times 10^7$

SWS = ?

Soln: No of seq. bits in Go Back N ARQ = $\uparrow$ 500 bits in 10 MS (RTT)

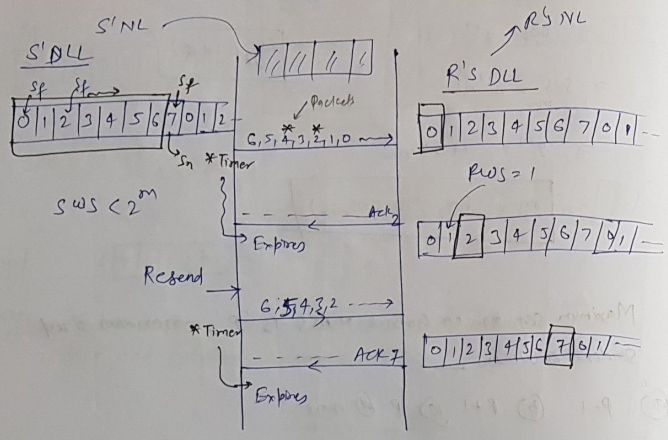
$\therefore$ No of frames = $\frac{\text{No. of bits}}{\text{frame size}} = \frac{500}{5}$

= 100 frames

	SWS	RWS
6 bits	63 ✗	1
By Greedy Approach → 7 bits	128 ✓	1
8 bits	255 ✓	1

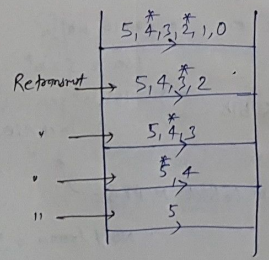
Soln

Case-I (Some Frames are lost)



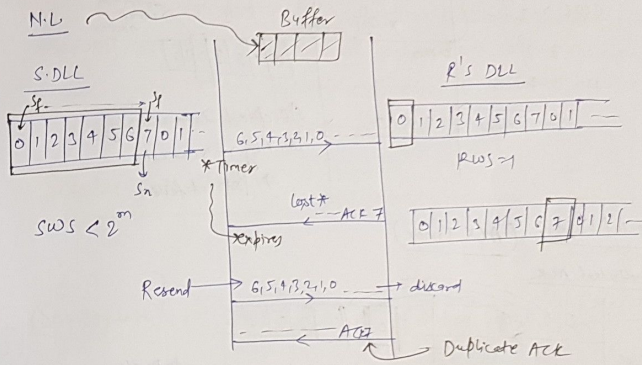
→ In Go Back N ARQ, if a frame is lost then that frame as well as all the following frames should be re-transmitted.

Noisy Channels:



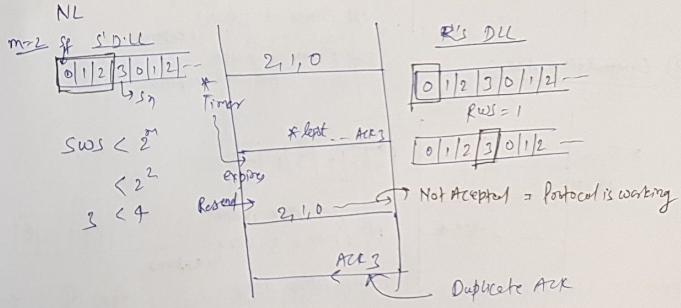
→ Whenever the receiver's window size (RWS) = 1, it accepts only In-order frames.

Case-II (ACK is lost):



Analysis

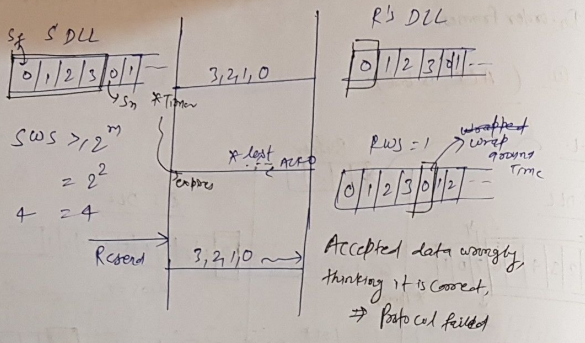
① NL



(4)

Soln

(2)



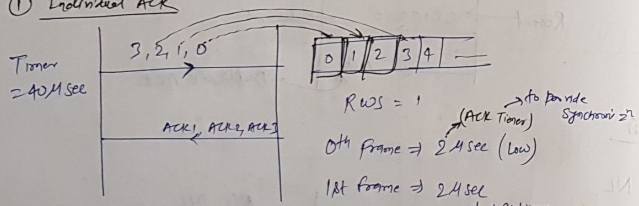
$SWS > 2^m$

$= 2^2$

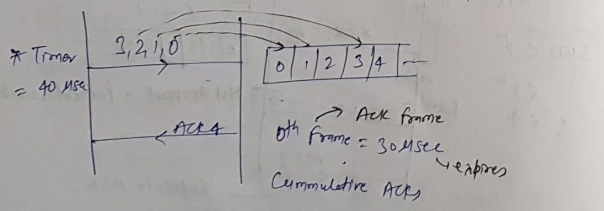
$4 = 4$

Special Case : (ACK Timer)

① **Individual ACK**



② **Cummulative ACK :**

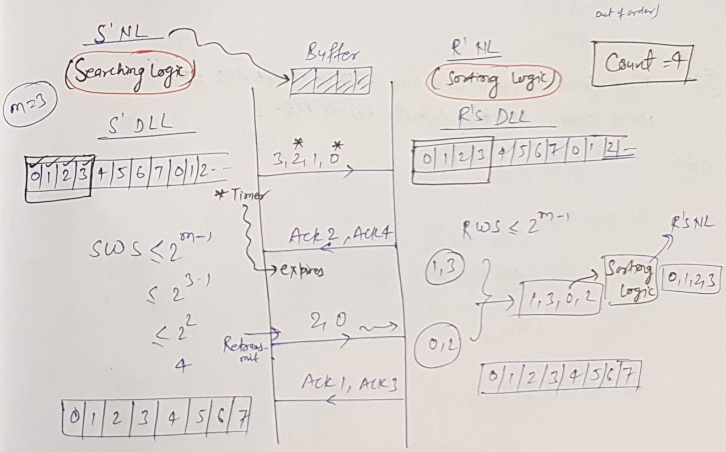


→ In case of Individual ACKs, the timer is started for every frame that is received. This timer value should be small enough so that we can send the ACK immediately.

→ In case of Cummulative ACKs, the timer is started for the first frame that is received. It should not be so small so that the remaining frames might not have arrived and also it should not be so large that the waited time is expired. It should be moderate.

Selective Repeat ARQ :- Aim: (No. of Retransmissions should be as less as possible)

(Sender is best case if out of order)



→ In case of Selective Repeat ARQ, it supports individual acknowledgement.

→ In the Selective Repeat ARQ, sender requires Searching Logic and receiver requires Sorting Logic.

Q.

(1) 5 bit sequence number is used in the SR ARQ, what is the SWS & RWS.

	SWS	RWS
SR ARQ,	(16)	(16)
Go Back N ARQ,	(31)	(1)

Soln

SR ARQ,

$SWS \leq 2^{m-1}$

$\leq 2^4$

≤ 16

Go Back N ARQ,

$SWS \leq 2^m$

$< 2^5$

< 32

(2) Max Sender Window size in Selective Repeat ARQ, = ?

No. of sequence bits in Selective Repeat ARQ = ?

$= \log_2(2S)$

Soln:

$\because SWS \leq 2^{m-1}$

for max SWS,

$SWS = 2^{m-1}$

$\Rightarrow (m = 5)$

$SWS_{max} = 2^{m-1}$

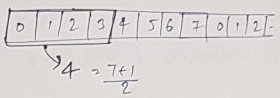
$SWS_{max} = \frac{2^m}{2}$

$\Rightarrow 2^m = 2 \times SWS_{max}$

$\Rightarrow \boxed{m = \log_2(2 * SWS_{max})}$

(3) Max. Sequence No. in the Selective Repeat ARQ is '7'. What is the max. sender window size = ? $\frac{N+1}{2}$ (N → 7)

Soln:



(4) BW = 100 mbps → 100×10^6 b/s

RTT = 50 μsec → 1 sec → 10^6 bits → $50 \times 10^{-6} \times 10^6 = 50$ bits

frame size = 25 bits

Sender window size in SR ARQ = ?

No. of frames = $\frac{2 \times 5000}{25} = 200$ frames

$SWS \leq 2^{m-1}$

$200 = 2^{m-1}$

$2^{7} = 2^{m-1}$

$m = 8$

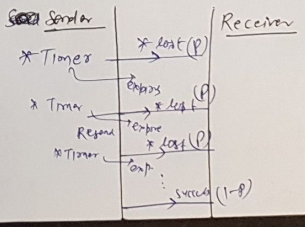
$m = \log_2(2 \times 200) = \log_2 400$

No. of Seq. bits in Selective Repeat ARQ = 8 bits

No of Seq. bits → Go Back N = (8) bits

→ Compared to Go Back N ARQ, Selective Repeat ARQ requires 1 extra sequence bit for maintaining the same window size.

(1) Probability of frame being lost is 'P'. Mean no of transmissions of a frame is $(1/1-p)$



$P, P, P, \ldots$ — $(1-P)$

$(K-1)$ time — K^{th} time

K transmissions of same frame

$$E(K) = \sum_{K=1}^{\infty} K * P(K) \quad \text{or} \quad \int_{K=1}^{\infty} K P(K)$$

// Discrete // continuous

$$E(K) = \sum_{K=1}^{\infty} K * P * P * \cdots * (K-1) * (1-P)$$

$$= \sum_{K=1}^{\infty} K * P^{K-1} * (1-P)$$

$$= (1-P) \sum_{K=1}^{\infty} K * P^{K-1}$$

$$= (1-P)\left(1 + 2P + 3P^2 + 4P^3 + \cdots\right)$$

$$= (1-P)(1-P)^{-2}$$

$$= \frac{1}{(1-P)}$$

$\because (1-x)^{-1} = 1 + x + x^2 + \cdots$

$(1-x)^{-2} = 1 + 2x + 3x^2 + 4x^3 + \cdots$

② Probability of frame being reached safely is 'q',

then mean no. of transmissions of a frame is $\boxed{1/q}$

$q = 0.1$

$= 10$

$\because P = 1 - q$

$$\frac{1}{1-(1-q)} = \left(\frac{1}{q}\right)$$

Error Control Policies of DLL :-

Error Correction Code (Hamming Code) :-

Data + Parity Bits = Code word

eg Data to be sent from Sender's DLL to Receiver DLL

Data : 10011010

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

where, m = message bits

r = Parity bits.

eg: Here $m = 8$

take $r = 3$

$\therefore 2^3 \geq 8 + 3 + 1$

$8 \not\geq 12$

$\therefore r = 3$ ✗

take $r = 4$

$2^4 \geq 8 + 4 + 1$

$16 \geq 13$

$r = 4$ ✓

Parity bits should be placed in power of 2 positions

2^0	2^1	3	2^2	5	6	7	2^3	9	10	11	12
P_1	P_2	1	P_4	0	0	1	P_8	1	0	1	0

P_1 : take 1 bit, leave 1 bit

$\therefore P_1$: 1, 3, 5, 7, 9, 11

Sol

P_1 : 1 3 5 7 9 11

0 1 0 1 1 1 → No of 1's = even

[even Parity] $P_1 = 0$

P_2 : take 2bits, leave 2bits

2 3 6 7 10 11

1 1 0 1 0 1 [even Parity] $P_2 = 1$

P_4 : take

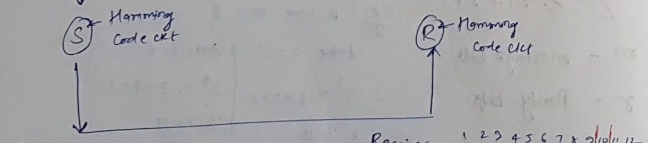
4 5 6 7 12

1 0 0 1 0 ($P_4 = 1$)

P_8 : 8, 9 10 11 12

0 1 0 1 0 ($P_8 = 0$)

Data: 10011010



Sender Codeword: 01110010 10

Receiver Codeword: 1 2 3 4 5 6 7 8 9 10 11 12
0 1 1 1 0 0 1 0 1 1 1 0

= P_1 P_2 1 P_4 0 0 1 P_8 1 1 1 0

Received Parities in ~~zeer~~ received codeword [$P_1 = 0, P_2 = 1, P_4 = 1, P_8 = 0$]

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

P_1 P_2 1 P_4 0 0 1 P_8 1 1 1 0

P_1 : 1, 3, 5, 7, 9, 11

0 1 0 1 1 1

Calculated received Parity ~~cal~~

$P_1 = 0$ ✓

P_2 : 2, 3, 6, 7, 10, 11

0 1 0 1 1 1

$P_2 = 0$ X

P_4 : 4 5 6 7 12

1 0 0 1 0

$P_4 = 1$ ✓

→ 2+8 = 10

P_8 : 8 9 10 11 12

1 1 1 1 0

$P_8 = 1$ X

→ 10th bit is an error (changed by Noise)

So Change it (1 to 0)

It is → Error Correction Code

→ The drawback of Hamming code is, it will correct only single bit errors.

→ In case of correcting codes, receiver will not send any negative ACK to the sender asking for the data to resend.

→ If noise modifies the parity bits copy, receiver will be knowing immediately by comparing with reliable copy.

Parity Scheme :-

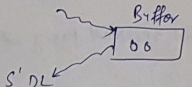
Data + Parity Bit = Codeword

00 + 0

01 + 1

10 + 1

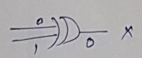
S'NL

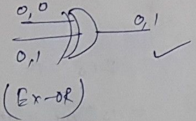


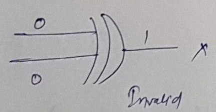
S'DL

x	y	Output even
0	0	0
0	1	1
1	0	1
1	1	0

} → Valid Code words

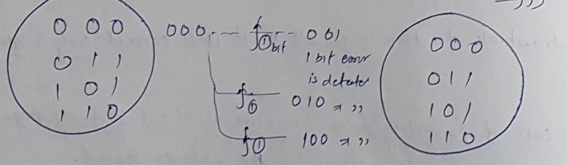






Sender

Receiver



000 —f②— 011 ⇒ errors are not detected ×

000 —f② bits— 000 ✓

→ When a valid codeword is converted into invalid codeword by noise then errors are detected.

→ When a valid codeword is converted into another valid codeword, then errors are not detected.

→ When a valid codeword is received as it is then the data content is accepted.

Hamming Distance :-

The no. of different bits in two nos. } apply Ex-OR

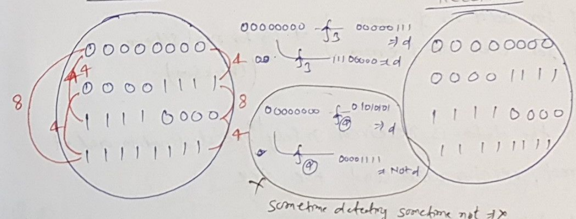
To detect 'd' errors, the minimum hamming distance is (d+1).

eg " " 1 error " " " " 1+1 = 2

eg: How many errors = ?

Sender

Receiver

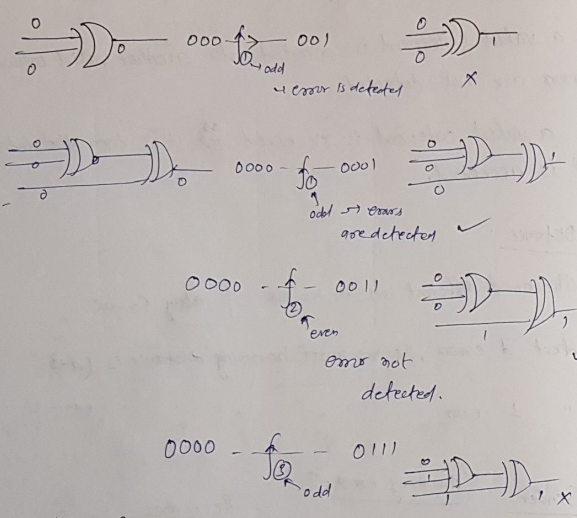


To detect 3 errors, min. ham dist = 3+1 = 4

Vice versa, H.D = 4 ⇒ 3 errors

Sender

Receiver



Working for odd no of errors
not working for even no. of errors
} ⇒ Go for next scheme (Check Sum)

① When the data is received safely to the destination and it is correct, receiver will send +ve Ack

② Duplicate Ack :

When the original Ack is lost and once again the receiver is sending the Ack that Ack is known as Duplicate Ack

③ -ve Ack :-

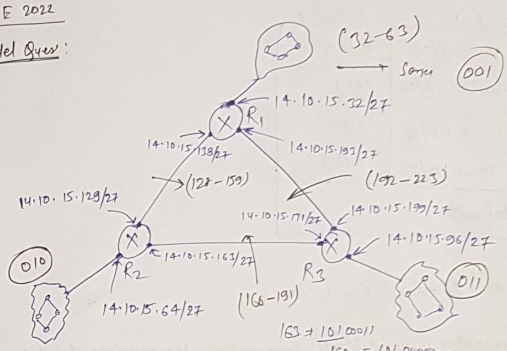
Whenever the data is received to the receiver and receiver finds that there is an error then receiver will send -ve Ack.

④ The -ve Ack is generally transmitted for Errors Detection Policies.

⑤ The Round Trip Time will be less for Error Correction Policies.

GATE 2022

Model Ques :



(1) No of Subnets = ?

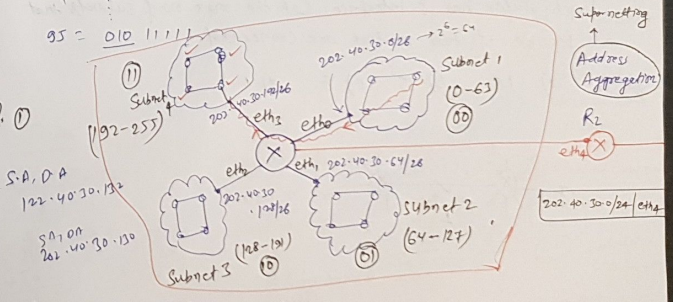
The cable b/w two Routers is also a Subnet

$2^{32-27} = 2^5$

64 = 010 00000

95 = 010 11111

(2) Qn (1)



A comp. in subnet-1 wants to broadcast to subnet 4 then what is the destn address that should be used? → 202.40.30.255/26

Q. (11) A computer in subnet 1 wants to broadcast in subnet-2 then which destination address is used?

→ 255.255.255.255/26

Routing Table:

Subnet-1	Interface
202.40.30.0/26	eth 0
202.40.30.64/26	eth 1
202.40.30.128/26	eth 2
202.40.30.192/26	eth 3
Default	

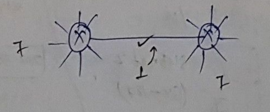
In Router, min 1 interface is req.

→ During Supernetting or Address Aggregation, the number of entries will be less so that the searching time will be less so that package will be forwarded fastly.

→ The another name for Supernetting is Hierarchical Routing.

Q. Each router has 8 interface. Cal. the max. no of subnets that are possible if two routers are connected.

Soln: a) 16 b) 15 c) 8 d) 1



Checksum :

Data + Extra bits = Codeword

↓

(Checksum bits)

Here, we can apply our own rules on both the sides.

eg **Sender** Codeword

eg 239376 - - - → Case(i) Noise modifies data bits

23
93
76
---
192 → 92 + 1 = 93 → 9's complement: 99 − 93 = 06

∴ Data is 239376, 06 (Data bits, Checksum)

Receiver

249676 (06) → Received Checksum in received code word = 06

24
96
76
---
196 → 96 + 1 = 97 → 99 − 97 = 02 (Calculated Checksum at receiver)

Error is detected

Sender

23937606 — Case-(ii) Noise modifies Checksum bits —

Receiver

239376 (89) → 89 = Received Checksum

23
93
76
---
192 → 92 + 1 = 93 → 99 − 93 = 06 (Calculated Checksum at receiver)

→ error is detected

Sender

239376, 06

23
93
+76
---
192 → 92 + 1 = 93 → 99 − 93 = 06

Noise modifies

↑

Vertical Bit Error (as there are placed vertically)

⇓

Such errors cannot be detected.

Receiver

259176 (06) → (06) Received Checksum

25
91
76
---
192 → 92 + 1 = 93 → 99 − 93 = (06) Calculated Checksum

Parity Scheme does not work for even no. of errors

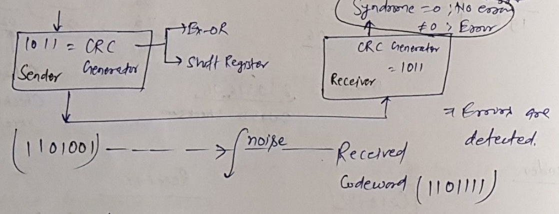
→ If noise modifies the data in such a way that the vertically placed bits will cancel out each other then the calculated checksum is equal to received checksum. Such Errors cannot be detected by the receiver. These errors are known as Vertical Bit Errors.

→ It is an Error Detection Policy.

* Cyclic Redundancy Check (CRC) :-

(→ multiple XOR op & shift)

Data : 1101



1101 1011 → n = 4

(n-1) 3 '0' padding

```
1011) 1101000 (1111
      1011          ⊕ Ex-OR
      ----
       1100
       1011
       ----
        1110
        1011
        ----
         1010
         1011
         ----
          001  → CRC bits
```

attach with the data i.e.) replace 1101000 by 1101001

∴ data = (1101001)

(No padding at receiver's side)

```
1011) 1101111 (1111
      1011
      ----
       1101
       1011
       ----
        1101
        1011
        ----
         1101
         1011
         ----
          110  → Syndrome
```

If Syndrome = 0; No error
≠ 0; Error

If (Calculated Checksum at receiver == Received Checksum) ⇒ accept the data

or (Calculated Checksum at receiver − Received Checksum) == 0

(Calculated Checksum at receiver − Received Checksum) = Syndrome

CRC Rules

① CRC generator should not contain 'x'.

Proof: Data = 1011

CRC generator = x = $1 \times x^1 + 0 \times x^0$ = (10) (Coeff of x^1 & x^0)

```
10) 10110 (1011
    10
    --
     01
     00
     --
      11
      10
      --
       10
       10
       --
        0
```

Syndrome = 0; No error
≠ 0; Error.

Sender Codeword	Received Codeword
10110	10010

```
10) 10010 (1001
    10
    --
     00
     00
     --
      01
      00
      --
       10
       10
       --
        0
```

(Syndrom = 0) ⇒ accept but actually it is wrong data.

3 case possible: Syn = 0; ≠ 0; = 0 & data is wrong

② Data = 1011

CRC generator = $x+1$ = $1\times x^1 + 1\times x^0$ = 11

```
11) 10110 (1101
    11
    ---
     11
     11
     ---
      01
      00
      ---
       10
       11
       ---
        1
```

∴ 10110 → 10111

Sender Codeword —— Case(i) (1 bit) Noise ① —— Received Codeword

10111 → 10110 ⇒ 1 bit error is detect

```
11) 10110 (1101
    11
    ---
     11
     11
     ---
      01
      00
      ---
       10
       11
       ---
        ① → Syndrome ≠ 0
```

⇒ 1

10111 —— Case(ii) (Noise) 2 bit —— 10100

2 bit error is not detected

```
11) 10100 (1100
    11
    ---
     11
     11
     ---
      00
      00
      ---
       000
        00
       ---
        ⓪ → Synd = 0
```

10111 —— Case-III 3 bit ③ —— 10000

→ 3 bit errors are detected.

```
11) 10000 (1111
    11
    ---
     10
     11
     ---
      10
      11
      ---
       10
       11
       ---
        ① → Synd. = 1
```

① ∴ If $(x+1)$ is generator then it can detect odd no. of errors.

→ CRC-32 generator can detect any no. of errors.

→ CRC-32 is standard LAN standard for detecting errors in the LAN network.

Framing :-

Framing :-

Sender → Receiver

eg 1000 → (1 bit) → 1001

$4C_1 = 4$

0001
1101
1011
1000

eg 1000 → (2) → 1011

$4C_2 = 6$

eg 99999 → (2 bits) →

$99999\ C_2$ = high

AL: [AH | Data]

TL: [TLH | AH | Data]

NL: [NLH | TLH | AH | Data] → DLL

→ Dividing the large amount of data into small parts so that the errors can be detected easily by the CRC is known as framing.

→ The efficiency of any error detection scheme decreases as the length of data increases.

(i) Character Count :-

S'NL ⇒ 7312 05634 63

S'DLL → [4|7|3|1|2] [5|0|5|6|3|4] [2|6|3]

Count Data Count Data Count Data

R'NL ↑ R's DLL

→ In the character count technique, count value indicates size of the frame.

→ In this particular scheme, if noise modifies the data, CRC can easily find out at receiver's Data link layer.

→ But if noise modifies the count value, both sender and receiver are out of synchronization. ⇒ we use char stuffing

(ii) Character Stuffing or Byte Stuffing →

eg S'NL : A B → S'DLL : FLAG A B FLAG ——→ R's DLL : FLAG A B FLAG → R'S NL A B

eg S'NL : A FLAG K → S'DLL : FLAG A FLAG K FLAG ——→ R'DLL : FLAG A FLAG K FLAG → R'S NL : A

S'DLL : FLAG A ESC FLAG K FLAG →

R's DLL : FLAG A ESC FLAG K FLAG ← Pre appended with ESC ⇒ Char stuffing

R'NL : A FLAG K

eg. $expr 4*3 ← all

$expr 4*3 ← multiplication (stuffing) ⇒12

eg $expr 4/2

$expr 4\/2 = 2 ← stuffing

eg: S'NL : A ESC FLAG K

S'DLL FLAG A ESC ESC ESC FLAG K FLAG — 8 bit stuffing

R'DLL : FLAG A ESC ESC ESC FLAG K FLAG

R'NL : A ESC FLAG K

→ In case of character stuffing, for every FLAG occurs in the data, an ESC char is stuffed so overhead size will increase.

Bit Stuffing :-

FLAG = 01111110

A → 65 → 01000001

B → 66 → 01000010

S'NL : A FLAG B

S'DLL : FLAG A ESC FLAG B FLAG

01111110 01000001 011111010 01000010 01111110

After 5 1's, stuff a '0'

eg: Data at sender's NLL : 01111110 111110 . What would be the data at sender's DLL after stuffing ?

Soln : After 5 1's

01111110 011111010 1111100 01111110
(Flag) (Flag)

eg. Data at S'NL : 011110 11110

Flag : 011110

011110 0111010 111100 011110

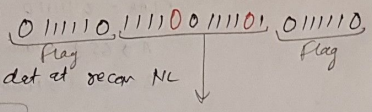
eg. Data at S'NL : 100000 1000000 10000 1

Flag : 100001

Data at S'DLL = ?

Soln : 100001 (Flag) 1000010 10000100 1000011 100001 (Flag)

Eg Data at receiver's DLL is



the data at recvr NL

Destuffing → data: 1111011111

Networking Devices :

Hub, Repeater. // Passive Devices

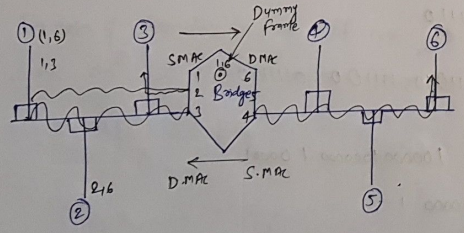
Bridge, Router, Gateway // Active Devices.
(Intelligent Devices)
Take decision)
→ They have table to take decisions

↓
LAN Dev
MAC Add
Similar LAN

Bridge :-

① Bridge is a LAN device and it's operation is based on MAC Address

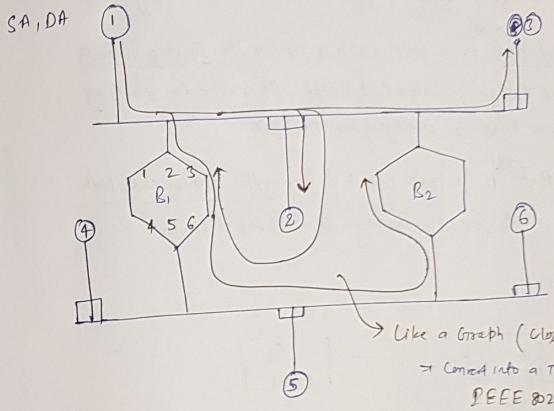
② Bridge is used for connecting similar LAN networks



(i) Initially the bridge table of a bridge is empty.

① The properties of the bridge are: Learning, Blocking and Forwarding

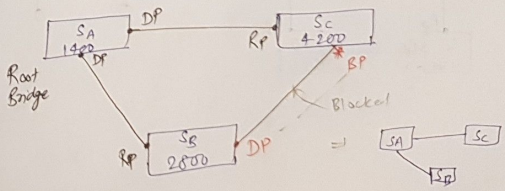
② Once Bridge knows the complete information of the N/w, it is treated as Converge and Stable.



Between the similar LAN N/ws, we connect more than 1 bridge to support Fault Tolerence.

→ When more than 1 bridges are connected b/w similar LANs, there is a possibility of loop or cycle in the network, so the graph should be converted into a tree using Spanning Tree Protocol.

IEEE 802.1C :-



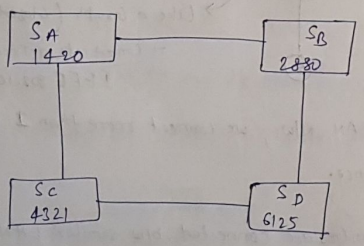
→ The bridge which is having the least MAC address will become the Root Bridge and remaining are Non Root Bridges.

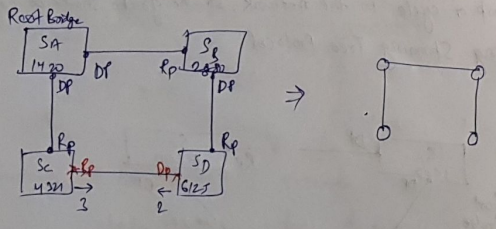
→ Root Port (RP) is a port which is having the least cost path from Non Root Bridge to Root Bridge. It is used for sending data.

→ Designated Port (DP) is a port which is having the least cost path from Root Bridge to Non Root Bridge. It is used for sending Configuration files or managing the network

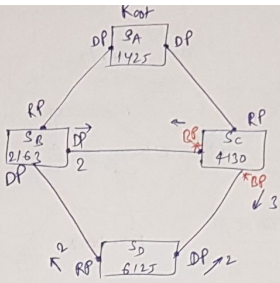
→ Blocked Port (BP) is a port which is having the highest cost path and it is used for temporarily disabled the network.

(2.)

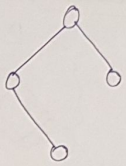




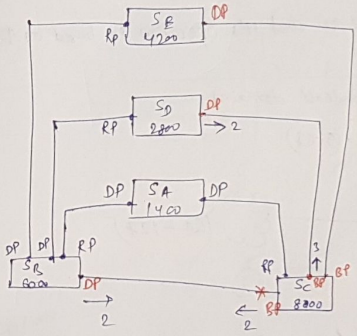
(3)

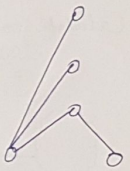


Remove the arrows of DP

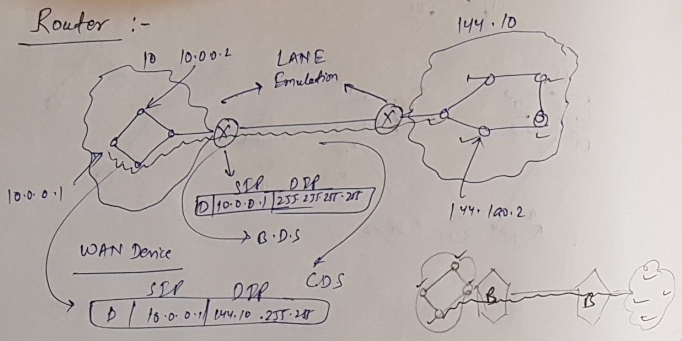


(4)





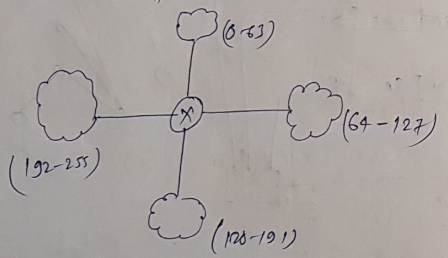
Router :-



Router is a WAN device and it's operation is based on IP Addresses.

eg. Calculate no. of Broadcast domains -

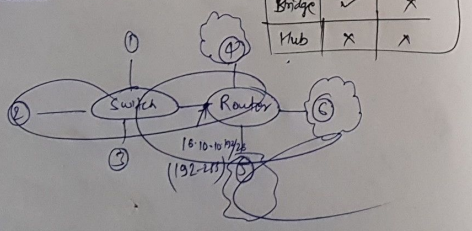
(1)

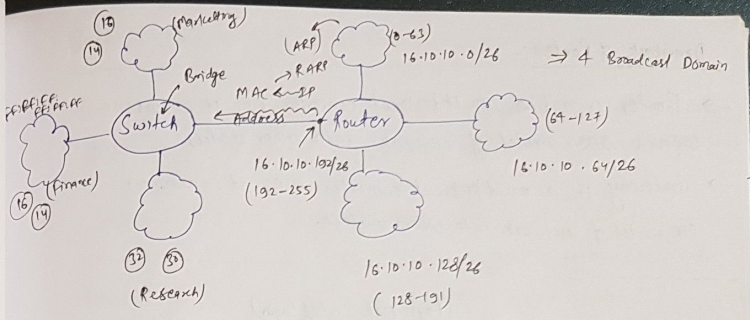


4 B.D

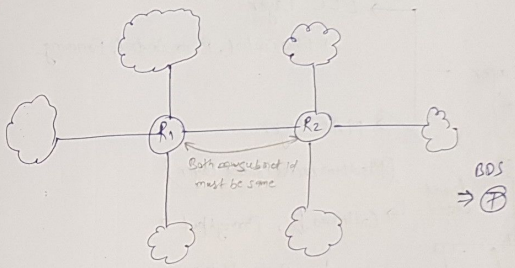
(2)

	CDS	BDS
Router	✓	✓
Bridge	✓	×
Hub	×	×

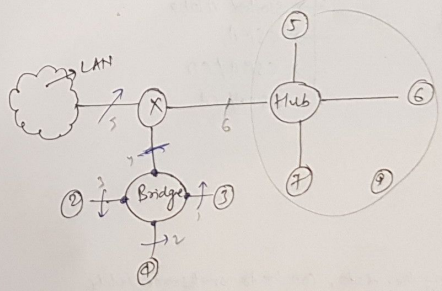




(3)



(4)



Q. Cal. the no. of B.D. for router → 3

Q. No of Collision Domain = 6

Drawback of Router :-

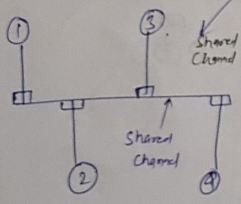
→ Router is not a multiprotocol converter i.e; it cannot convert one model of network into other models.

→ Gateway is a multiprotocol converter i.e; it can convert one model of network into other models.

(Logic Link Control Layer)
→ LLC Layer
→ Flow Control, Error Control, Framing

Data Link Layer (LAN)

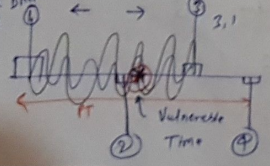
→ MAC Layer (Medium Access Control Layer)
↳ Collisions ↓, Throughput ↑



- Pure Aloha
- Slotted Aloha
- CSMA,
- CSMA/CD
- CSMA/CA

Pure Aloha Protocol :-

Any stations is having the data, can be transmitted immediately

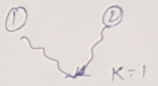


Backoff Time or Exponential Backoff Algorithm :-

Waiting some random amount of time whenever there is a collision is given by an algorithm, is called, Exponential Backoff Algorithm

Q. Stations 1 & 2 have transmitted their data for the first time and collided and waited for some random amount of time. What is the probability that station 1 will retransmit before station 2 ?

Soln:



$WT_1 = (0 \text{ to } 2^K - 1) * PT$ $\quad WT_2 = (0 \text{ to } 2^K - 1) * PT$

$= (0,1) * PT$ $\quad = (0,1) * PT$

WT_1	WT_2	
0	0	
0	PT	= (1/2)
PT	0	
PT	PT	

Q. In the above problem what is the prob that both the systems will retransmit at the same time ?

Soln: For K=1 = Chance = $\frac{1}{2}$ = 50%

Q. S1 & 2 have transmitted their data for the 2nd times and collided. What is the prob that S-1 will retransmit befor S-2 ?

Soln:

WT_1	WT_2
0	0
PT	PT
2PT	2PT
3PT	3PT

$\frac{3+2+1}{16} = \frac{6}{16} = \frac{3}{8}$

Q. In the above problem what is the prob that both the stations will retransmit at the same time?

Soln:

WT_1	WT_2
0	0
PT	PT
2PT	2PT
3PT	3PT

$S = 16$, Fav. events = (0,0), (PT, PT), (2PT, 2PT), (3PT, 3PT)

$= \frac{4}{16} = 0.25 = 25\%$

$\therefore$

For K=1, Chance of Collisions $= \frac{1}{2} = 50\%$

For K=2, " " $= \frac{1}{4} = 25\%$

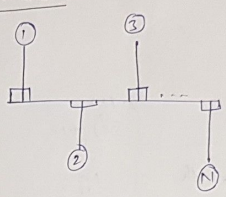
For K=3, " " $= \frac{1}{8} = 12.5\%$

.

K=10.

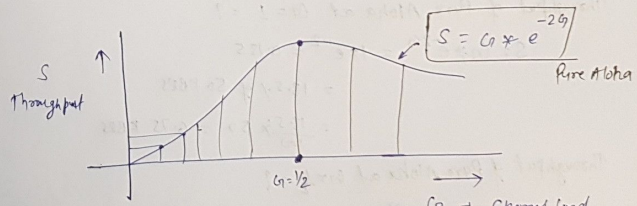
⇒ As 'K' increases, chance of collision is decreases so that chance of data reaching safely increases.

Pure Aloha :-



No. of Stations	No. of stns ready to transmit	Collisions	Data reached safely
100	50 (50/100)	30	20
100	100 (100/100)	50	50
100	40 (40/100)	10	30
100	200 (every stn is transmitting 2 frames)		

(Non Deterministic → Poission Distribution)



$G = 1$ → Critically Loaded

$G < 1$ → Under Loaded

$G > 1$ → Over loaded

From max/min

$\frac{dS}{dG} = 0 \Rightarrow G(-2)e^{-2G} + e^{-2G} \cdot 1 = 0$

$\Rightarrow G = 1/2$

$S_{max}\big|_{at\ G=\frac{1}{2}} = \frac{1}{2} * e^{-2\times\frac{1}{2}}$

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

$= 0.184$

$S_{max} = 18.4\%$ of Bandwidth

2.7×2
$10)\ 54$
50
40
40
14

→ Out of 100 frames data transmitted, max 18.4 frames will safely reach the destination, remaining 81.6 frames will suffer from collisions.

→ The rate at which user transmits the data and the data should reach safely is known as Throughput.

① Bandwidth = 50 KBPS

Max t-put of Pure Aloha = ?

18.4% of 50 KBPS

$= 18.4 \times \frac{1}{100} \times 50 = 9.2$ KBPS

② Throughput of Pure Aloha at $G = 1$ = ?

$S = G * e^{-2G} = 1 * e^{-2} = 0.135$

= 13.5% of 50 KBPS

$= \frac{13.5}{100} \times 50 = 6.75$ KBPS

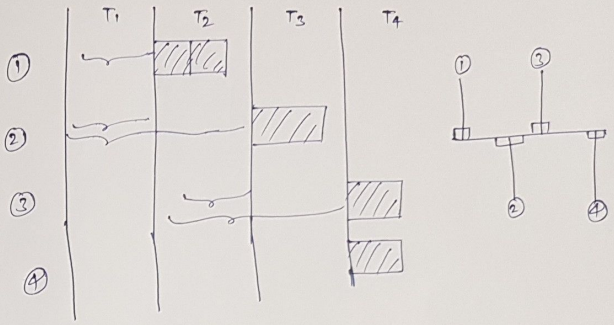
③ Throughput of Pure Aloha at $G = \frac{1}{2}$ = ?

$S = G * e^{-2G}$

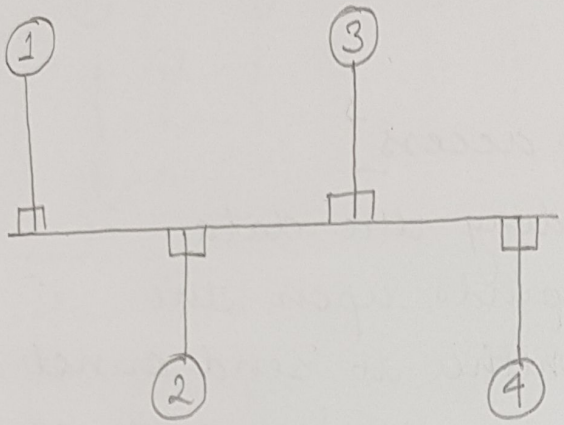
$= \frac{1}{2} \times e^{-2\times\frac{1}{2}}$

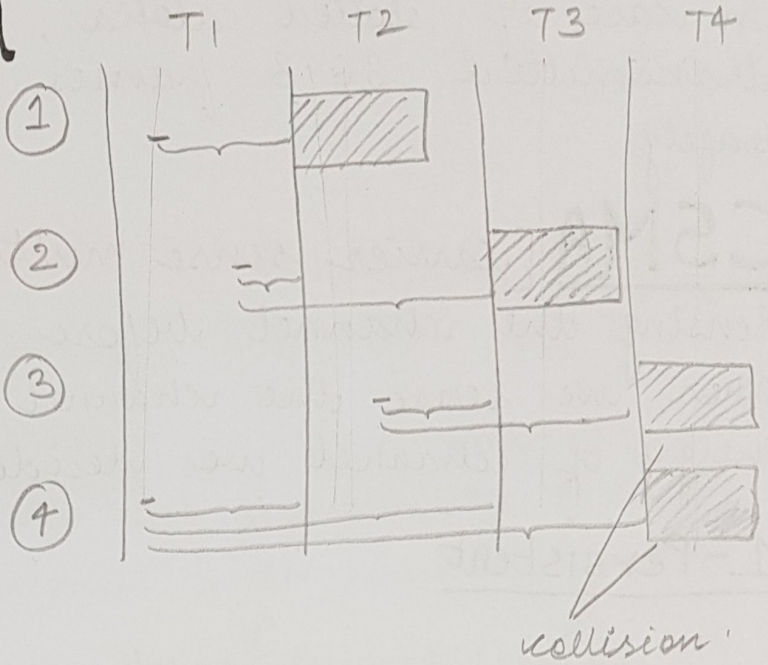
$= \frac{1}{2e} = 0.184 \rightarrow 18.4\%$ of BW $= \frac{9.2}{\frac{18.4}{100}} \times 50 = 92$ KBPS

Slotted Aloha :-



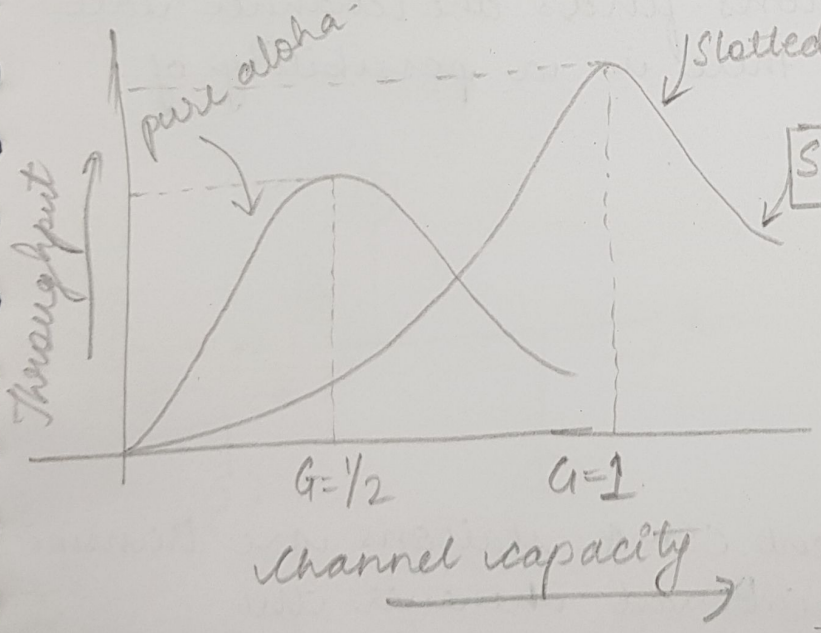
SLOTTED ALOHA





Only at the starting of the time slot we can send data
Not necessary to transmit immediately

#stations	#station ready	T1	T2	T3	T4 .....
100	50	10	20	5	15
		[2-C, 8-SR]	[10-C, 10-SR]	[1-C, 4-SR]	[10-C, 5-SR]



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

$$\frac{dS}{dG} = -G \times e^{-G} + e^{-G} = 0$$

$$e^{-G}[1-G] = 0$$

$$G = 1$$

$$S_{max} = 1 \times e^{-1} = 1/e$$

$$= 0.368$$

$$= 36.8\%$$

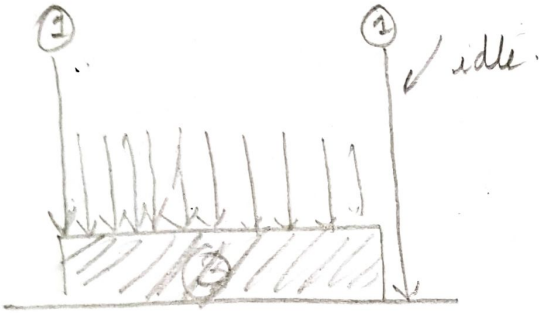
In case of slotted aloha, out of 100 frames transmitted 36.8 frames will reach the destn safely.

CSMA [carrier sense multiple access]

Sensing the channel before sending the data.
When we sense the channel depends upon the energy of channel we decide whether to send or not.

1 Persistent
Programmed I/O

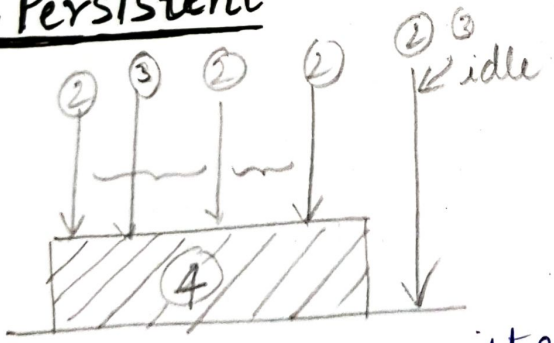
1-Persistent



In case of 1-persistent CSMA stations will continously sense the channel. Once the channel is idle, it will transmit with the probability $P = 1$

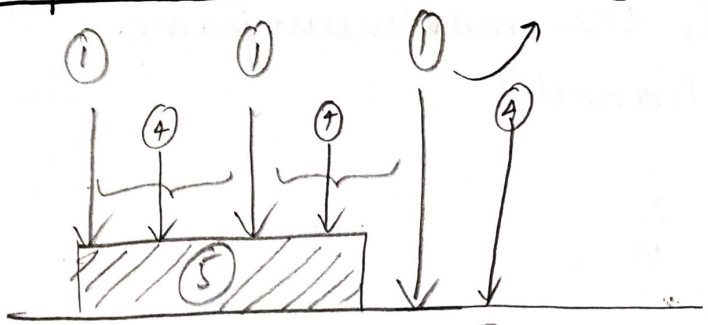
2. If two or more stations finds the channel idle at the same time then there is a possibility of collision.

Non-Persistent



In case of non-persistent CSMA, stations are transmitting at different time interval whenever the channel is idle. In this the possibility will be less as compare to Non-persistent.

P-persistent [1-P Non P].



[Interrupt driven DMA]

1. In case of P-persistent CSMA, once the channel is idle, it will transmit with the probability P or it may not transmit with probability (1-P)

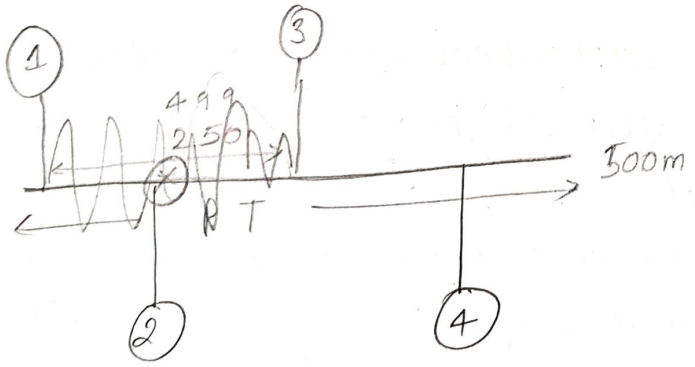
1. There are 4 station in a slot. Probability of transmitting the data is 0.4. What is the probability that only 1 station transmit in the given time.

$$[{}^{n}C_{1} * P^{1} * (1-p)^{n-1}]$$ Condⁿ for critical section

$0.6 * 0.6 * 0.6$
≈ 0.4
$= 0.3456$

CSMA-CD [Carrier sense multiple access w/ collision detection]

Cannot sense at in full region only at this point



collision occurence	collision detection
0.1 * PT	0.2 * PT
0.2 * PT	0.4 * PT
0.5 PT	1 PT
0.6 PT	1.2 PT

(1) If Data Size ↑ then efficiency increases [large packet]
∴ For large packet CSMA/CD is good

(2) If Distance ↑ then efficiency decreases CSMA/CD is suitable for LAN (small distance) Not for long distance.

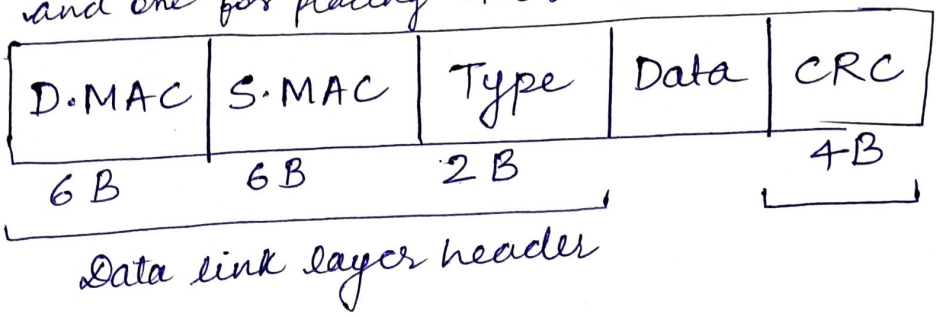
$$\eta = \frac{1}{1 + 6.44\left(\frac{\text{Distance}}{\text{velocity}} * \frac{\text{Bandwidth}}{\text{Data Size}}\right)}$$

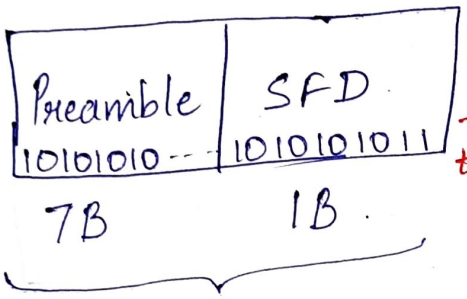
IEEE 802.3

D.L.L

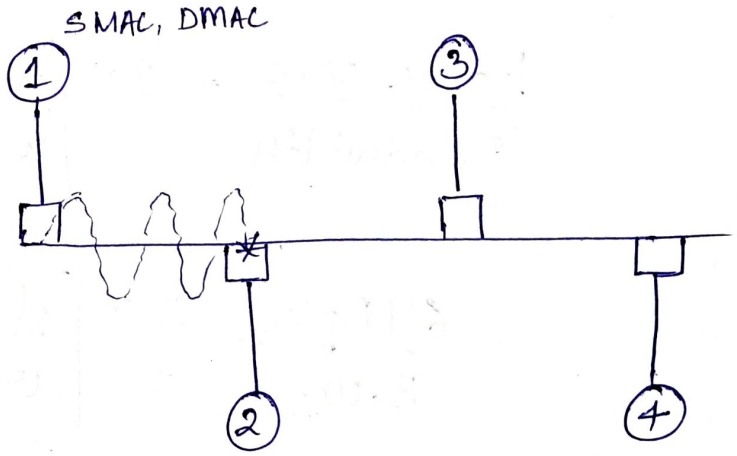
frame format

Why CRC at end?
If we will append CRC in header only then it will take 3 unit of time [1 for calculating CRC in comp, 2 for placing data on the channel and one for placing CRC on the channel].





Gives an alert to Destn sys. that be ready to take the data



1. Preamble and SFD is to alert the station whenever the data is reaching.
2. The only layer which is attached trailer along with the header is the data link layer.
3. The minimum frame size in IEEE 802.3 is 64B or the Minimum data in IEEE 802.3 is 46B.
4. The maximum frame size in IEEE 802.3 1518B
   The maximum data in IEEE is 1500B, this restriction is to give fair and equal chance to all station in the n/w. or not to assign any priority to any particular station.

1: In CSMA/CD, Ethernet, IEEE 802.3, B.W = 100Kbps. $v = 2 \times 10^8$ m/sec. calculate the maximum frame size to acquire the channel?

$$\frac{\text{frame size}}{BW} = 2 \times \frac{L}{v}$$

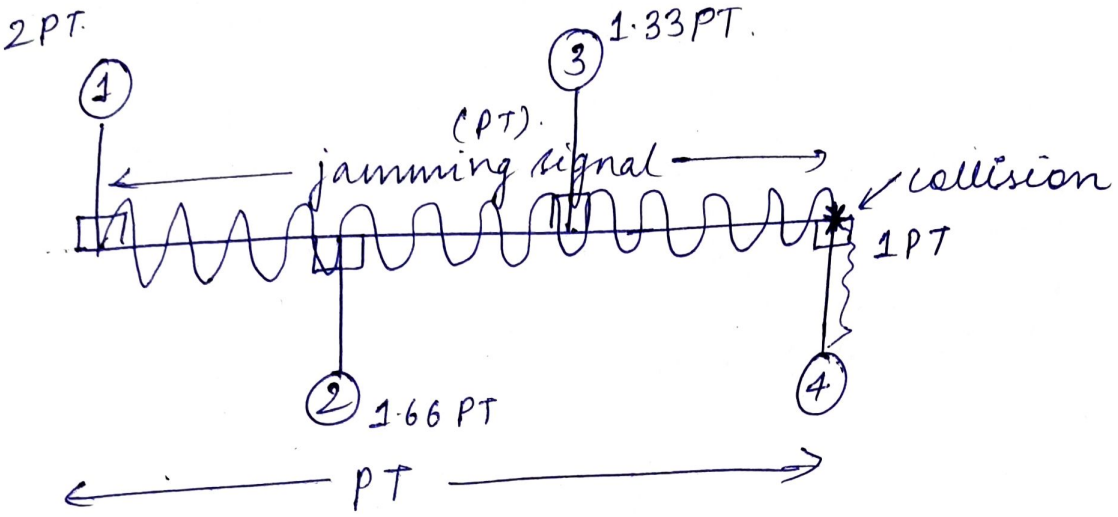
$$x = 2 \times 100 \times 10^3 \times \frac{200}{2 \times 10^8} \quad 100 \quad 10^5$$

$$\boxed{x = 200 \text{ bits}}$$

2. In CSMA/CD (&) Ethernet

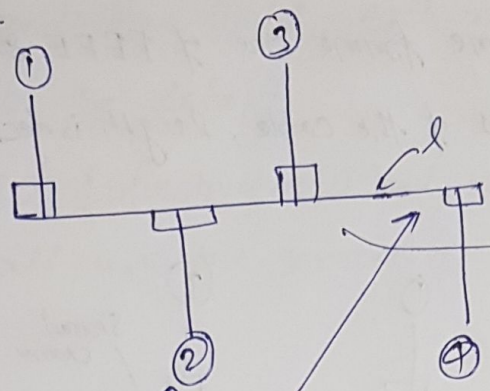
1. If the collision is not detected at the worst case of 2PT, then at 2PT the station confirms it has acquired the channel.
2. If the stations have detected the collision at the worst case of 2xPT, then station will stop sending the data and apply exponential backoff algorithm.

Special case [jamming signal].



1. The purpose of jam signal is to inform to unknown station about the collision.
2. In CSMA/CD, jam signal is acting as an acknowledgment.
3. Not getting a jam signal is a confirmation that the station has acquired the channel.
4. Getting a jam signal is a confirmation that there is a collision in the n/w.

28/07/22



10 base 5 → 500 m

IEEE 802.3 (Protocal)

Standard Ethernet
↓
10 base 5
↓
BW = 10 mbps

maximum frame size
64 * Bytes

maximum frame size
↓
1518 Bytes

$TT = 2 * PT$

$\frac{\text{Frame size}}{BW} = 2 * \frac{l}{v}$

Switched Ethernet
↓
100 mbps

100 base T (Twisted)
1000 base F (Fibre optic)

if $\frac{64 * \text{Bytes}}{10 * BW} = 2 * \frac{l/10}{v}$

100 mbps

if $\frac{64 \text{ Bytes}}{100 * BW} = 2 * \frac{l/100}{v}$

Giga Ethernet
↓
1000 mbps

→ Thick Ethernet cable cannot bend at the corners.
Thin Ethernet cable can bend at the corners.

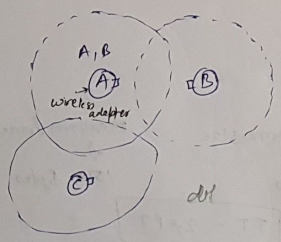
→ When the cables are changing from Standard Ethernet to Switched Ethernet, Bandwidth is increased and length is decreased.

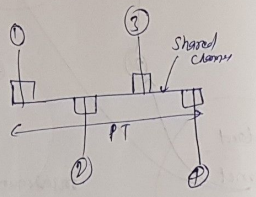
→ Switched Ethernet Cable is known as 100 Base T

→ Gigabit Ethernet is also known as 1000 Base F

* In order to maintain the same frame size of IEEE 802.3, in all the different Bandwidths of the cable, length is decreased

Wireless :- (Wireless LAN)





(Same shared channel for every node)

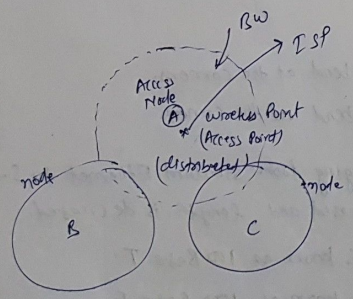
(Wired Connection)

Peer - Peer Model

Adhoc Mode of Transmission.

→ In case of Wireless, every node has it's own shared channel and the data will be transmitted to Omni directions.

→ In Adhoc mode of transmission, each node will use it's own resources to transmit the data.

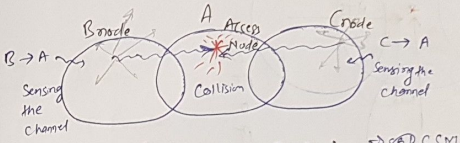


→ Infrastructure Mode
client - server Mode

→ Wireless LAN
OR
BSS (Basic service set)

→ In Peer to Peer Model, each node will use it's own resources to transmit the data.

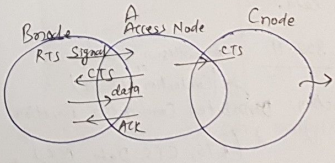
→ In case of Infrastructure Model, or a client-Server Model, all the each nodes will use the services of Access Node.



(Hidden Node Problem) ⇒ CSMA/CD cannot be applied : use CSMA/CA

→ Nodes B, A, C are in the planar region and when nodes B & C transmit the data to the access node A at the same time, then there is a collision at Access Node A. This collision cannot be detected by either B or C becoz collision energy is lost immediately. This problem is known as Hidden Node Problem.

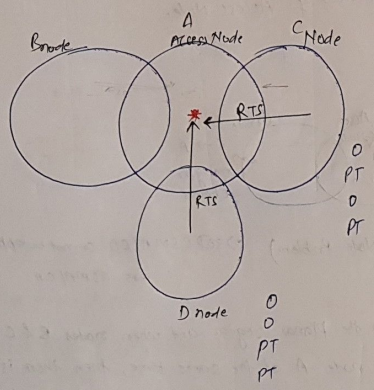
CSMA/CA : Carrier Sense Multiple Access / Collision Avoidance :-



RTS → Request to Send
CTS → Clear to Send
} Control Signal

2 Sept 22

→ When CSMA/CA protocol is used, it uses 4-way Handshaking (RTS, CTS, data, ACK).



→ When more than one node sends RTS at the same time then there is a collision at Access Node.

→ Not getting the CTS is a confirmation that there is a collision at access node, then both the nodes will apply Exponential Backoff Algo. So the station who waits for less amount of time will get a chance to transmit the data.

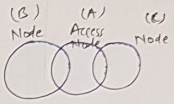
IEEE 802.11 → Collision Channel or (Contention Channel)

- DCF Function: (Low Priority) → Distributed Coordination Function
  When Node sending data to Access Node
  & (RTS, CTS, Data, ACK)
- PCF Function: (High Priority) → (Contention less Channel) Point Coordination Function
  Obbsire
  & (Data, ACK)

→ When a node wants to send the data to access node, it uses DCF.

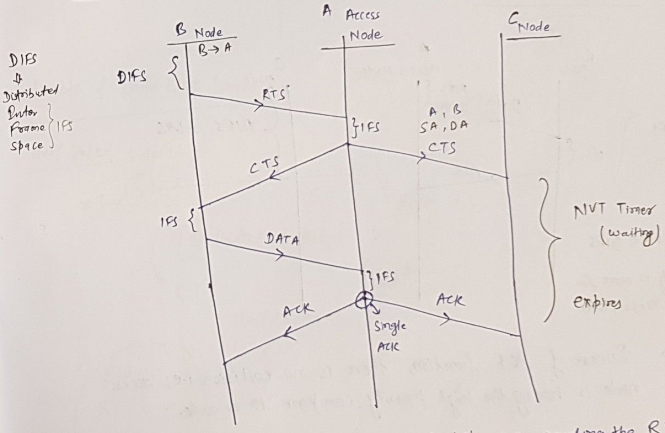
→ When the access node wants to send the data to a node, it uses PCF.

→ PCF is having high priority over DCF function.



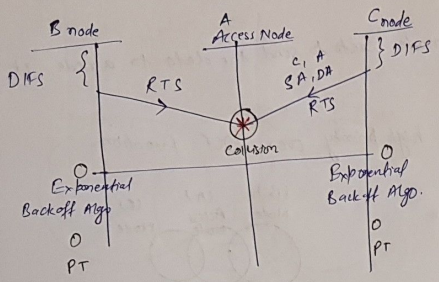
Timing Diagram :-

1.) For DCF function :-

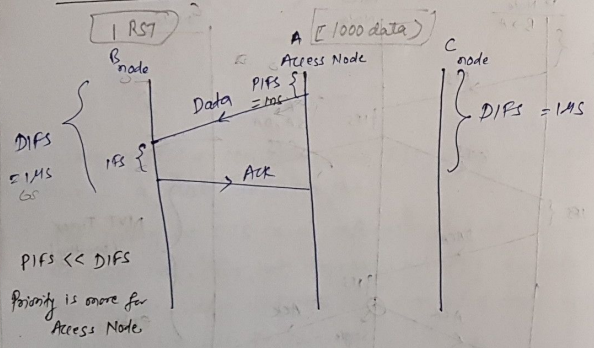


→ In the above diagram, other node 'C' starts sending the RTS after getting the ACK.

Continued diagram (Two nodes are sending RTS at the same time)



(ii) For PCF function :-

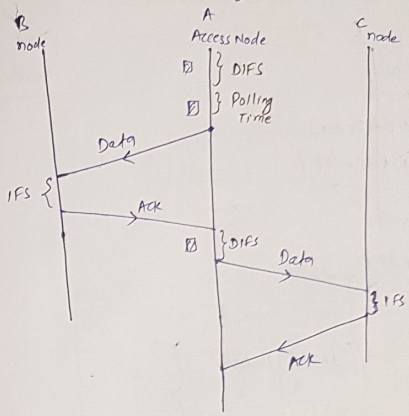


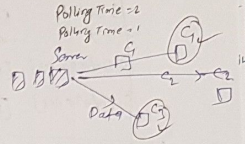
→ Incase of PCF function, there is no collision i.e; access node is having the high priority compare to a node.

D →
Ack → single user
D

Ack → 1001

[PIFS] + Polling Time <<< DIFS

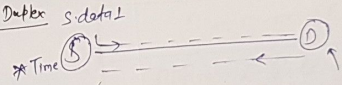




Doubts of Data Link Layer :-

LAN → ℓ ↓ PT ↓ TT ↑

Half Duplex S:data ⊥



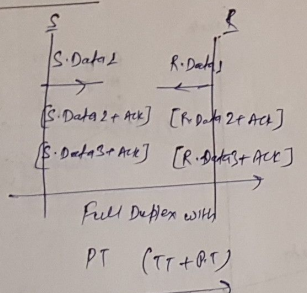
[D: Data ⊥ + ACK]
↳ Piggy backing
R.T.T

Half Duplex

BW :-
RTT :-
frame size :-
TT

→ No: of bits in RTT = ~
No: of frames in RTT = ~

Full Duplex :-



$\therefore LU = \frac{TT}{TT+2PT}$ // Half Duplex

$\therefore LU = \frac{TT}{TT+PT}$ // Full Duplex

0	1	0	01	0

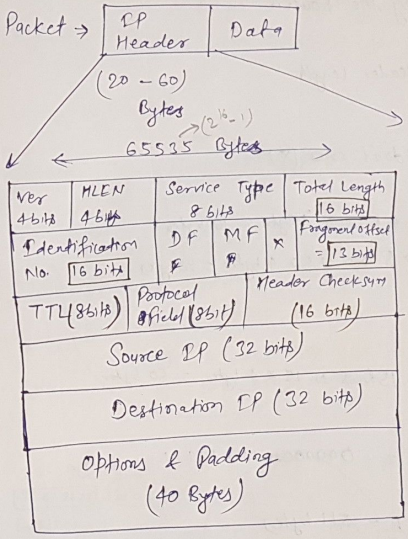
Stop & Wait ARQ, $\therefore$ LU of sender $= 1 * \left(\frac{TT}{TT+2PT}\right)$

Go Back N ARQ $= N * \left(\frac{TT}{TT+2PT}\right)$

Selective Repeat ARQ $= \left(\frac{Q+1}{2}\right)\left[\frac{TT}{TT+2PT}\right]$

Network Layer

IP Protocol :-



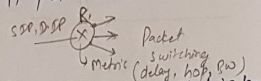
Ver → IP version
IPv4 / IPv6

0100 = IPv4
0110 = IPv6

0100 → 0111
0110 → IPv4
0110 → 1000

IPv4 0100 → IPv6 0110 [Checksum bothers to handle it]

→ The starting 4 bits of the IP packet decides whether the packet is a IPv4 or IPv6.



→ Service Type indicates the type of service that is provided to the packet by the Router.

HLEN : Header Length

0000
0001
0010
0011
0100 → 4 Rows * 4 Bytes = 16 bytes
0101 → 5 Rows ⇒ 5 * 4 bytes = 20 bytes
0110
⋮
1111 → 15 Rows ⇒ 15 * 4 bytes = 60 byte

don't cares (X)

Total length bits = 0000000011111111

Size of packet = 511 bytes

HLEN = 1010

Size of Header = 10 * 4 = 40 B

Header + Data = Packet

40 + x = 511

x = 471

Payload or Data

→ Fragments belonging to the same packet will be given the identification number so that at the destination, we can easily combine the fragments belonging to the same packet.

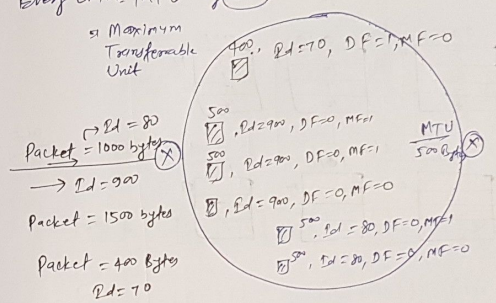
→ For all the intermediate fragments starting from the first, MF (More Fragment) value is 1 and specially for the last fragment, MF = 0.

Every LAN = MTU eg (1500 B)

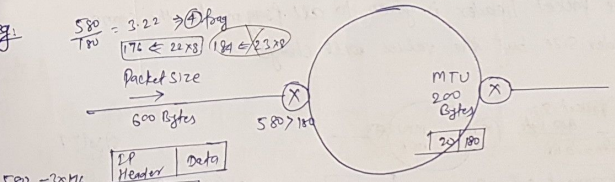
⇒ Maximum Transferable Unit

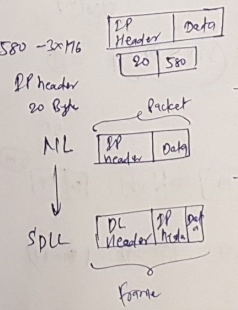
DF : Do not Fragment bit

MF : More Fragment Bits

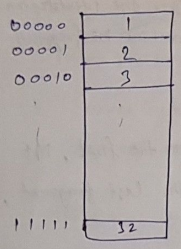


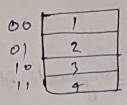
eg:





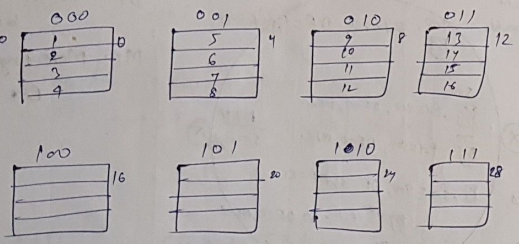
	1st Frag	2nd Frag	3rd Frag	Last Frag
Id ⇒	90	90	90	90
DF ⇒	0	0	0	0
MF ⇒	1	1	1	0
Frag bytes	20 | 176	20 | 176	20 | 176	20 | 92 | +4 48 Padding
Fragment offset	(0-21)	(22-43)	(44-65)	(66-72)





No. of chips = $\frac{32}{4} = 8$ memory chips

$\frac{2^5}{2^2} = 2^3 = 8$



The packet header is given to all fragments, the same header size but the values will change.

Q. Packet Size = 400 Bytes, IP header = 20 B, MTU = 100 B. Fragment offset?

20 | 80

380 > 80

$\frac{380}{32} = 11.7$, $60 \times 1 = 60$

Soln:

20 | 380

Frag B: 20 | 80 | 20 | 80 | 20 | 80 | 20 | 80 | 20 | 64

$\frac{380}{32} = 11.7$, $60 \times 1 = 60$, $320 + 60 = 380$

FO: (0-9) (10-19) (20-29) (30-39) (40-47)

0, 10, 20, 30, 40

Df: 0 0 0 0 0

MF: 01 1 1 1 0

40 : 101000

(40-49) (50-59) (60-69) (70-79) (80-87)

Q. Packet size 2000 B, MTU 600 B, IP header 20 B. Frag Bytes & FO = ?

Soln:

20 | 1980

20 | 580

Frag B: 20 | 576 | 20 | 576 | 20 | 576 | 20 | 256

FO: (0-71) (72-143) (144-215) (216-247)

$1976 = 23 \times 8$

$1980 \div 8$

$576 = 72 \times 8$

$1980 = 247.5 \times 8$

$174 \times 8 = 1392$

$580 \div 8 = 72.5$

Type-2

Q. The fragment offsets are given as 0, 60, 120, 180. IP header is given as 20 B. All fragments are of equal size. Cal. the packet size.

Soln:

FO: (0-59) (60-119) (120-179) (180-239)

FB: 20 | 480 | 20 | 480 | 20 | 480 | 20 | 480

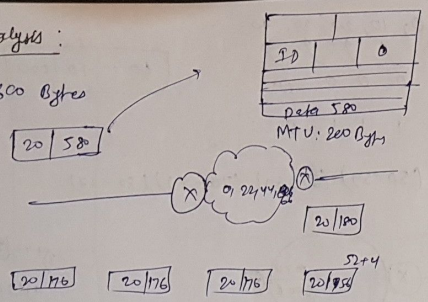
Df: 0 0 0 0

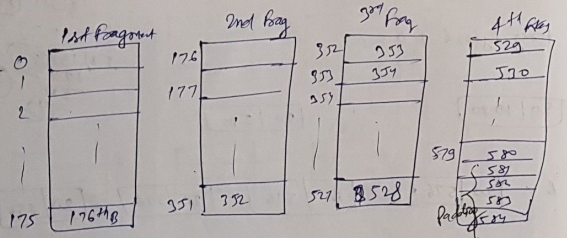
MF: 1 1 1 0

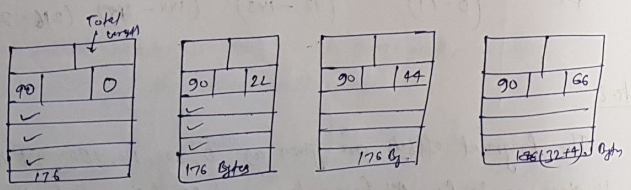
20 + 4 × 480

20 + 1920 = 1940 Bytes

Analysis :





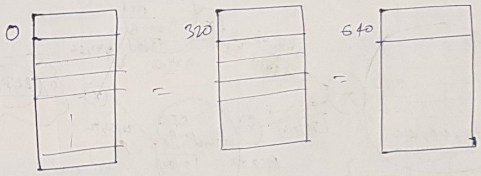


* → Total length of a packet will give us the packet size.
* → Total length of a fragment will give us the fragment size.
* → The fragment offset multiplied by 8 will give the ~~start~~ starting address of the fragment.

→ If MF = 0, it will tell that it is the last fragment but whether padding bits are attached or not can be known by comparing with the starting address of the next packet.

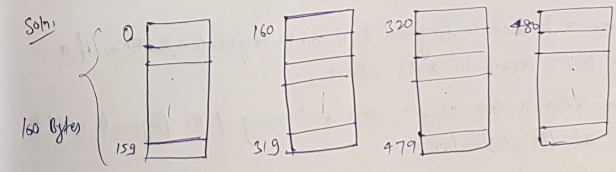
Q. Ⓐ Is continuous fragment offsets are given as: 0, 40, 80.
→ Not possible
Calculate no. of bytes in fragment?

Soln:



Q. Cond. frag. offsets are given as 0, 20, 40, 60
No. of bytes in frag. = ?
If header = 60

Soln:



If header = 60 Bytes
Size of fragment: 60 | 160 → 220 B

Q. Fragment offset of a packet = 40

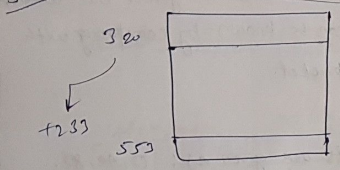
IP header = 20 Bytes

Total length fields in IP header ⟦ 0000000011111110

Packet size = Data + IP header

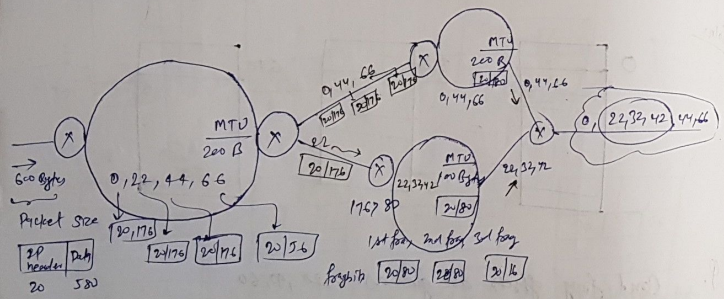
254 Bytes

Soln:



254 = x + 20

x = 234 Bytes



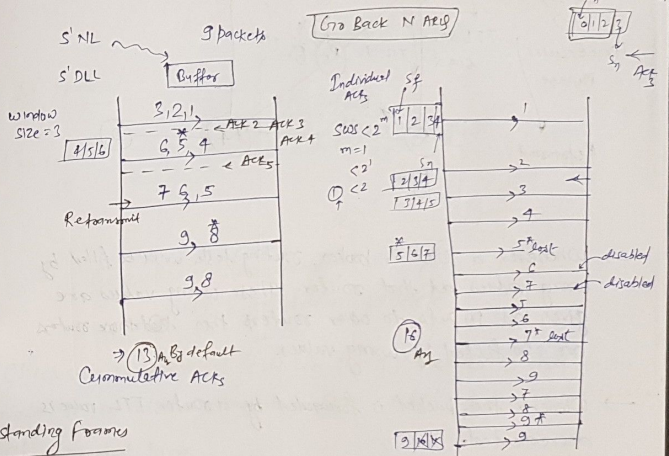
→ Whenever a packet is fragmented, it can be fragmented further, if a smaller MTU occurs in the network.

→ Fragmentation is done at the source and joining of the fragments will be done at the destination.

→ For the fragments, Id, DF, MF, Frag Offset will not change in between or from end to end.

→ DF value, MF value, Id value & Frag. value of a packet will remain same end to end in the internet.

Q.

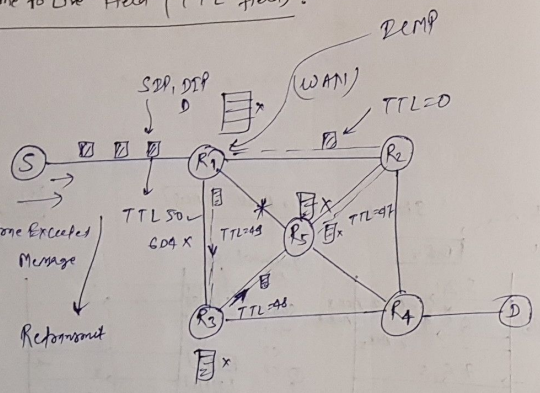


Outstanding Frames

The number of frames that are transmitted and waiting for their ACK are known as Outstanding frames.

→ Protocol is same for Packets as well as Fragments.

Time To Live Field (TTL field) :-



→ Whenever a link is booken, routing table will be filled by wrong values at that router. These wrong values are given as inputs to other routers then those routers are also filled by wrong values.

→ Whenever the packet is forwarded by a router, TTL value is decremented.

→ Whenever the packet forms a loop then at one point of time, TTL value becomes Zero (0) then the next upcoming router will drop the packet.

→ The ICMP protocol (Internet Control Message Protocol) will take the source IP from the dropped packet and informs to the source by sending 'Time Exceeded' message then source will resend that packet.

→ Without forming a loop, during the journey of a packet, TTL value will never become zero.

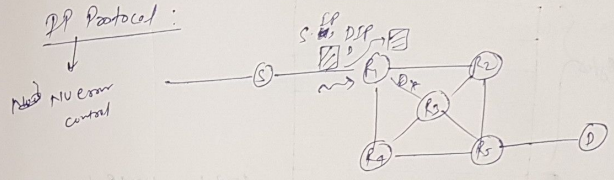
→ Protocol field will be helpful to find out which protocol at transport layer and network layer is belonging to that packet.

S'AL ⟶ http, ftp, SMTP, DNS, TELNET

S'TL ⟶ Port Address ⇒ TCP, UDP

S'NL ⟶ Protocol field ⇐ IP, ARP, RARP, ICMP

IP Protocol :



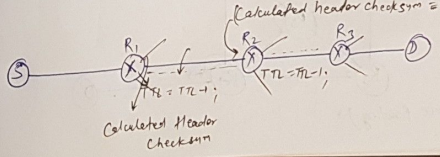
No error control

Connectionless, Unreliable, Best Effort delivery protocol.

→ Checksum is provided only for the IP Header so that for the data it is already provided error control by the TCP Protocol at Transport layer.

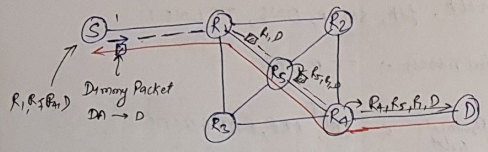
→ Checksum is provided only for the IP Header so for so that processing time is less so packet will be provided fastly.

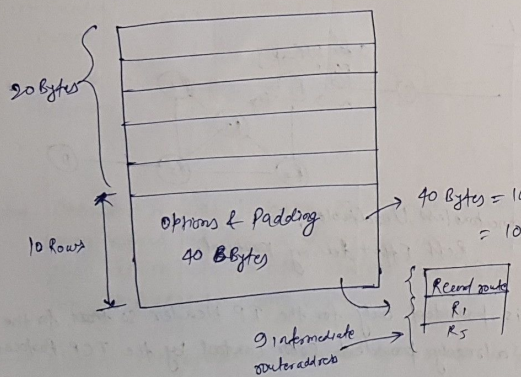
→ Checksum is provided only for the IP header so that packet will go to the correct destination (if it reaches).



Options & Padding :

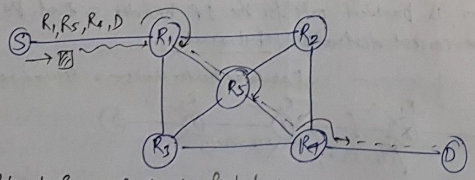
(i) Record Route Option :-



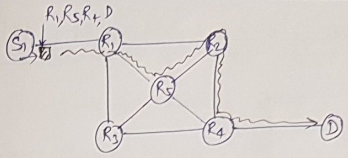


→ Maximum 9 intermediate router addresses can be placed in the Record Route Option.

(ii) Source Routing Option :-



(Strict Source Routing) → Packet strictly follows the path



(Loose Source Routing)

→ In strict source Routing, Packets will strictly follow the path which is specified by the source.

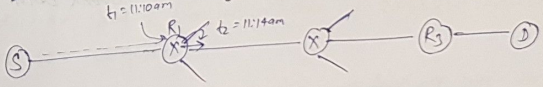
→ In case of Loose Source Routing, along with the path which is mentioned by the source, if some other paths are also visited then it is known as Loose Source Routing.

(iii) Time Stamp Option :-

→ Time stamp option in the IP Protocol will be helpful to know the processing time of a router on a packet.

→ It is a 3-Byte Option.

→ It is used in identifying wrap around.



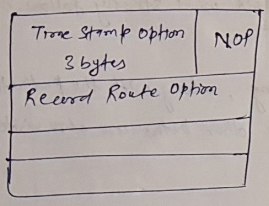
→ Packet coming to the destination having the same identification no. coming from the same source can be distinguished by Time Stamp.

→ Packets reaching to the destination can have same id. no. and same time stamp but they can be distinguished by source IP.

(iv) No Operation option (NOP option) → To create a delay b/w operations.

→ 1 Byte option

eg. while (Buffer Size == Full) { ; } ← NOP



→ NOP option is used to fill the gaps between the options.

(v) End of Operation option (EOP option) →

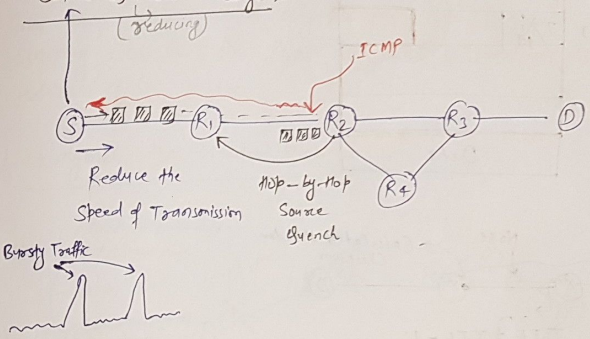
→ 1 Byte option

→ EOP option is used as a separator between Header & Data.

ICMP (Internet Control Message Protocol) :-

→ It is used for Reporting Errors & Management Queries.

(i) Source Quench Message :-

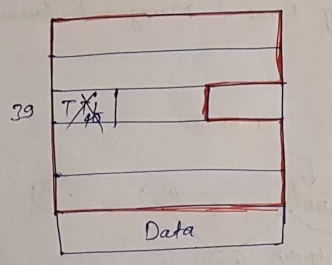


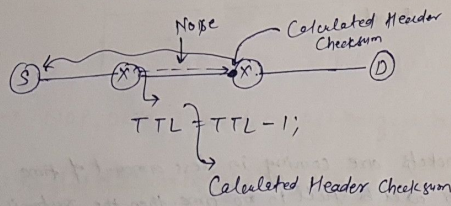
→ When more no. of packets are coming in less amount of time then the router buffer will be full in no-time. then the router is congested, then some packets will be dropped in the network.

→ ICMP will take source IP from the dropped packet and informs the source by sending Source Quench message. Then source will reduce the speed of transmission, then the congested router will be free from congestion.

→ If the congested router is far away from the source then ICMP will send Hop By Hop Source quench messages then every router via that path will reduce the speed of transmission.

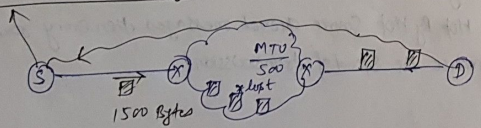
(ii) Parameter Problem :-





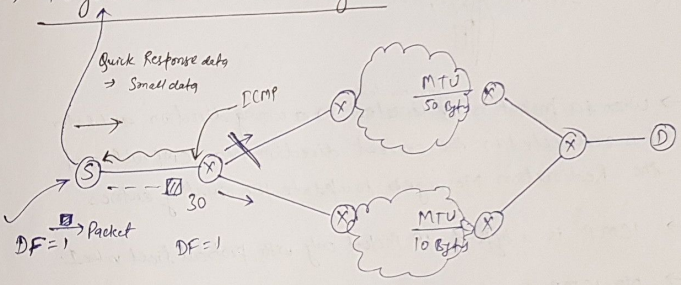
→ When noise has modified some header bits then the calculated header checksum will not be equal to received header checksum then the packet will be dropped. Then ICMP will take source IP from the dropped packet and informs to source by sending Parameter Problem message.

(iii) Time Exceeded Message :



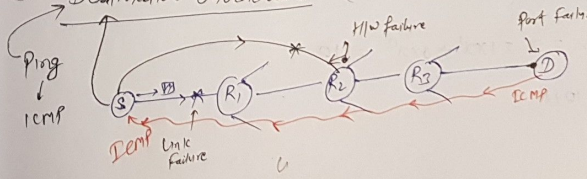
→ When some fragments are lost in the network then at the destination joining of the fragments is not possible. In this case fragments will be dropped and ICMP will take the source IP from the dropped fragment and informs to source by sending Time Exceeded message. This will be transmitted only for the first fragment bcz the starting address of the first fragment is same as the starting address of the packet.

(iv) Fragmentation Needed Message :



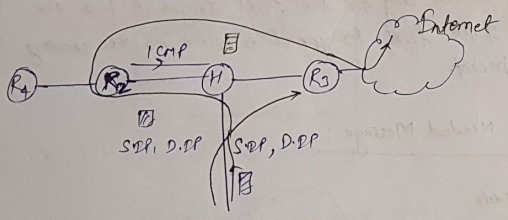
→ Whenever a packet is reached to the router and the router has to violate the rule of source specified the packet will be dropped then ICMP will take the source IP from the dropped packet and informs to the source by sending fragmentation Needed Message.

(v) Destination Unreachable :- (Link failure or H/w failure or Port failure)



→ ICMP error message will be transmitted not only by the redirecting router but also by the destination host.

(vi) Redirection Message :-



→ When a packet is ~~redirected~~ forwarded in a wrong direction and later it is redirected in the correct direction then ICMP will send the Redirection Message to update the routing entries

→ ICMP is a type of IP Packet only with protocol field value 1.

→ No ICMP error message will be transmitted to the broadcast ~~packet~~ package.

→ No ICMP message will be transmitted to the loop back address ~~package~~ packet.

CRC

(1) Data = 1011

CRC generator = $x = 1x^2 + 0x^1 + 1x^0 = 101$

101) 1011 (10
101

010

Sender Codeword — x is a bad gen — Receiver Codeword

1011 0

$x+1 =$ 1, 0, 1

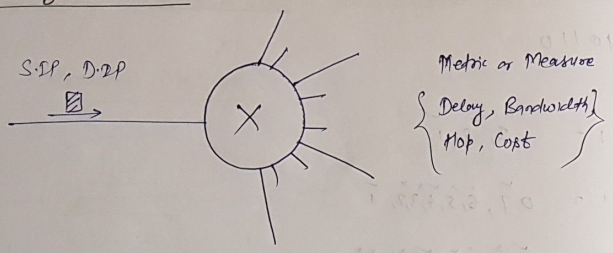
$x^2+1 =$ 0 1, 0, 1, 0, 1, 0, 1

$x^3+1 =$ 1, 0, 1, 0, 1, 0, 1, 0, 1

$x^n+1 =$ n+1, n, 1

Routing Algorithms :-

Hop : Router to Router



i) Static Algorithms →

It does not consider load on network.

(Non Adaptive Algorithms)

ex: Flooding Algorithm

(ii) Dynamic Algorithms →

It considers the load on network

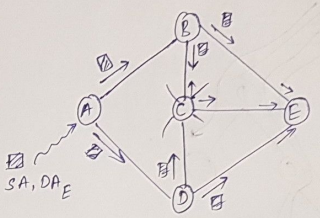
(Adaptive Algorithms)

eg: (i) Distance Vector Routing Algorithm (DVR)
(ii) Link State Routing Algorithm (LSR)
(iii) Path Vector Routing Algorithm (PVR)

① Flooding Algorithm :-

① Flooding Algorithm →

→ WAN Area



→ Whenever a packet comes to a router, it will divert it in all the directions except to the point of origin.

→ Flooding is used to find out unknown destinations. Generally it is used in the Military Operations. ↳ don't know dest^n MAC Address

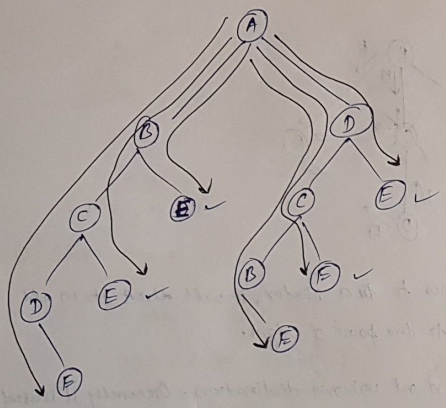
→ Flooding creates redundant packets which may lead to the congestion in the network.

Q: Cal. all possible paths from A to E using flooding algorithm and using hop as metric.

Soln:

ABE = 2 hops
ABCE = 3 "
ABCDE = 4 "
ADE = 2 "
ADCE = 3 "
ADCBE = 4 "

Q. Draw the flooding tree.



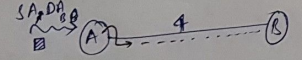
Dynamic Algorithms

① Distance Vector Routing Algorithm :- (Iterative Algorithm or Distributive Algo)

→ Initially the routing table of a router is empty.

→ Every router will be knowing the information of the directly connected routers without applying any Routing algorithm.

Case-I



→ Packet Switching supports Store & forward

→ ∵ 'A' has buffer so packet will be stored in the buffer

Routing Table of 'A'

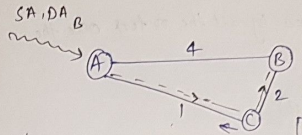
Destination	Estimated Delay	Next Hop
B	4	-

(↑ Now 'A' knows 'B')

→ directly connected.

All routers are in WAN area

Case-II



↙ Routing Table of 'C'

B	2	-

C → B = 2

R.T for 'A'

Destn	Estd Delay	Next Hop
B	3	C
C	1	-

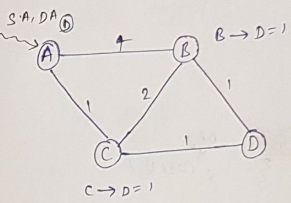
In case I, Path is A → B

In case II, Path is A → C → B

⇒ It is dynamic, not static, algo.

⇒ Router is calculating the path.

Case-III



B	3	C
C	1	-
D	2	C

→ When 'n' nodes are connected and a new node is connected, how much time will it take for all the routers to know about it is O(n).

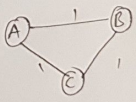
n = No of routers.

→ In a Distance Vector Routing, every router will get the complete information of network with the help of neighbouring routers.

→ This Algo is also known as the Iterative Algo bcoz o/p of R.T is given as i/p for the next router in the next iteration.

→ When the estimated cost converged towards final cost then estimated costs are ensured.

Q.



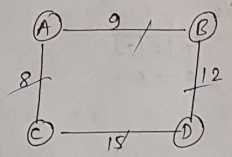
Cal. the no of unused links, once all the routers are converged by all the routers.

Soln:

Zero

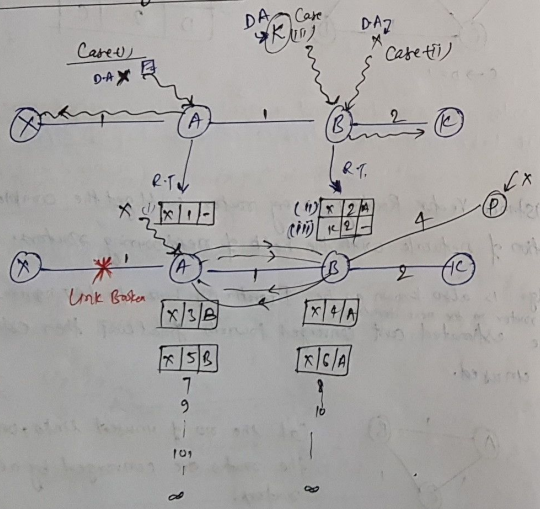
→ It is also known as the Distributive Routing Algo bcoz the o/p of the Routing Table is given as i/p for other routers and the tables are updated at every router.

Q Calculate the no. of unused links by all the routers once the routes are converged.



Soln: 0

Count to Infinity Problem :-



→ Whenever the links are broken, the routers are filled with the wrong values. These wrong values are given as input for other routers then those routers are also filled with wrong values. Finally the entire network will get collapsed. This problem is known as Count to Infinity Problem.

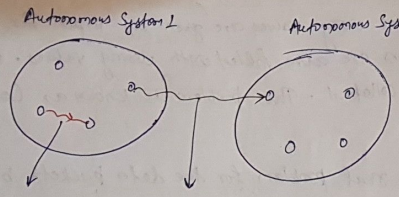
→ There is no real problem for the data packets bcoz they rotate only for a finite time. Once the TTL value becomes zero, packet will be dropped.

Properties of Distance Vector (DV.R) Routing Algorithm :-

(1) This algorithm is also known as Iterative Algorithm because output of routing table is given as input for the next router in the next iteration.

(2) It is also known as Distributive Routing Algorithm because the output of the Routing Table is given as input for other routers and the tables are updated at every router.

(3) It is also known as Asynchronous Algorithm because the ~~output~~ router will get information about the indirectly connected routers from the directly connected routers at different times.



Intra Domain Routing Protocol

Inter Domain Routing Protocol

eg BGP Protocol

ex: RIP, OSPF

RIP: Routing Information Protocol

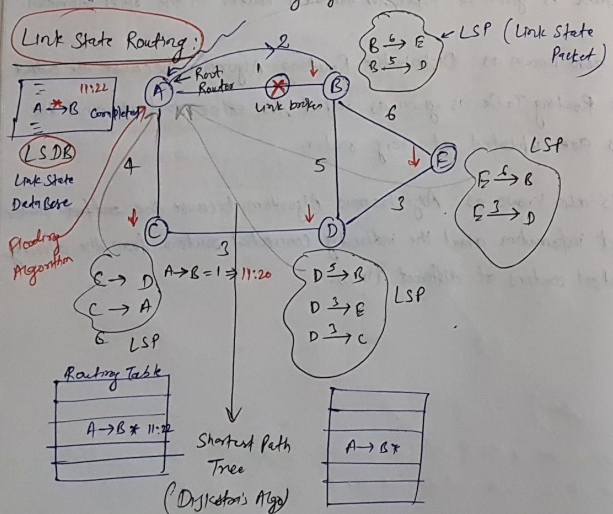
Root (Follows Distance Vector Routing Algo)

BGP: Border Gateway Protocol

follows Path Vector Routing

OSPF: Open Shortest Path Forwarding

follows Link State Routing Algo



→ Initially every router will generate LSP Packet.

→ These LSP Packets which are generated by the routers will be given to the ~~Router~~ Root Router. Then Root Router will generate LSDB Packet.

→ The LSDB Packet contains complete info of the network i.e; the no. of routers, no. of links, up & down links.
(working & not working links)

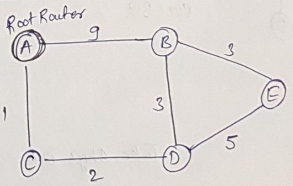
→ The LSDB Packet will be given to all the routers using Flooding of Algorithm.

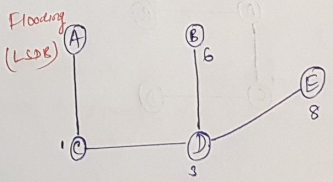
→ Before applying the Flooding Algo, graph will be converted into a Tree using Shortest Path Tree Algorithm (Dijkstra's Algorithm).

→ LSDB Packets should be generated periodically with the latest info of the network.

Dijkstra's Algorithm :-

eg ①





Count = ~~4~~ 3 2 4 0

From the root router,

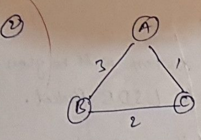
① Choose the router which is having least delay (C)

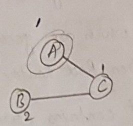
② C → D | delay is 2 ⇒ total delay = 3 from A & B

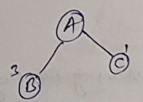
We can also reach to D via A B D but delay is 12 : C → D

③ from D, B is chosen bcoz delay is less for it. for E, it is 5.

(2)







Use (i) delay as metric

(ii) Hop '' ''

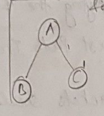
Steps:

(1) Shortest & delay

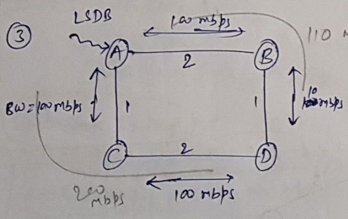
(2) For the next router, go at the root router fetched

Metrics used (i) delay } (ii) Hop }

If delay is same then go for Hop. ✓

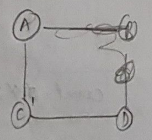


(3)



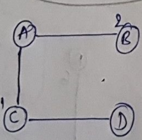
Metrics } (i) delay (ii) Hop (iii) BW

Soln



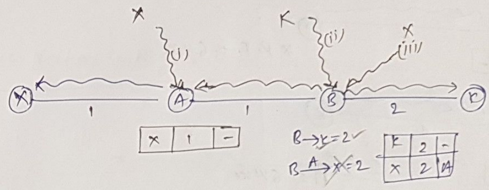
3

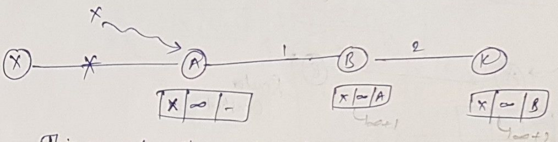
Take high BW



→ In Link State Routing Algorithm, there is no Count to Infinity Problem bcoz whenever the link is broken it is known to all the routers immediately with LSDB Packet.

Distance Vector Routing with Split Horizon :-





This is only applicable theoretically

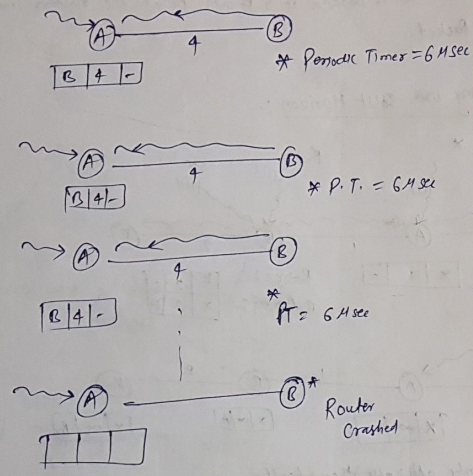
Definition :

→ Don't send the route information back to the node which we have learnt from it.

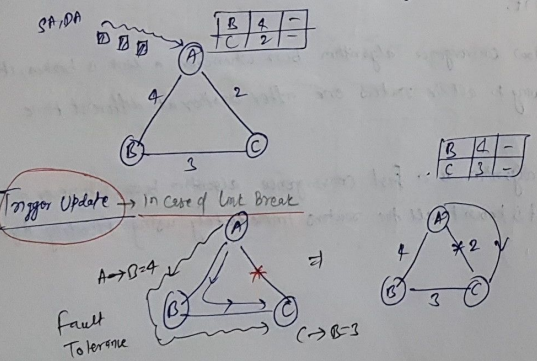
→ DVR is a slow convergence algorithm bcoz whenever a link is broken, it will be knowing to all the routers one after another at different time intervals

→ In LSR algorithm is a fast convergence algorithm bcoz whenever a link is broken, it is known to all the routers immediately using Flooding Algo.

Periodic Timer : (In case of Router fails)



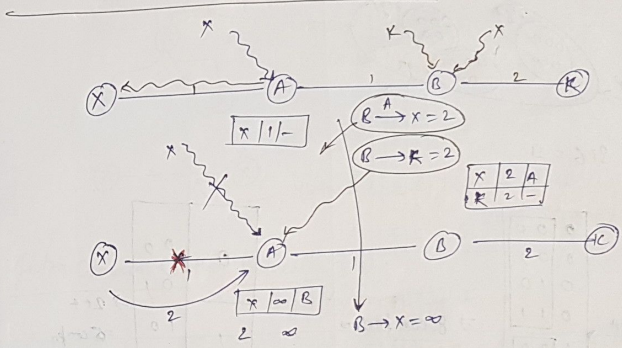
① Periodic Timer will be helpful to know the status of router.
② Whenever the router is crashed, the entry is removed.
③ Whenever the link is broken, the entry is made it as ∞.



Trigger Update → In case of Link Break

① The purpose of Trigger Update is, to know the status of the link.
② It is immediate and instantaneous.
③ Whenever there is a change is topology, Trigger Update is transmitted.
④ Change in topology does not mean the router is down. It means that the link is broken or new links are added.

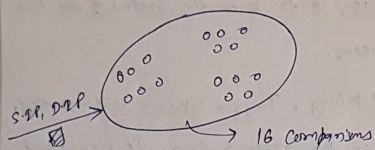
Distance Vector Routing with Poisson Reverse :-



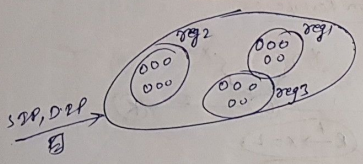
Definition :-

Send the route information back to the node which has learnt from it

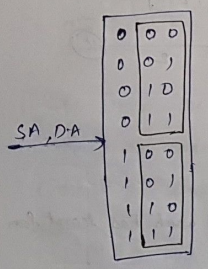
a) ∞



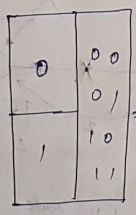
Hierarchical Routing



8+6 = 9

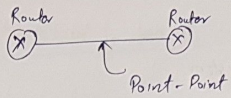


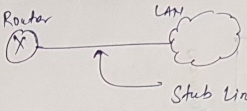
⇒ 8 comparisons

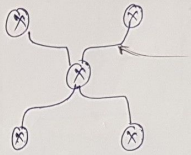


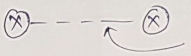
⇒ 2+4 = 6 comp.

Using Hierarchical Routing, logically the table size is reduced so that the searching time will be less and packet will be transmitted fastly.



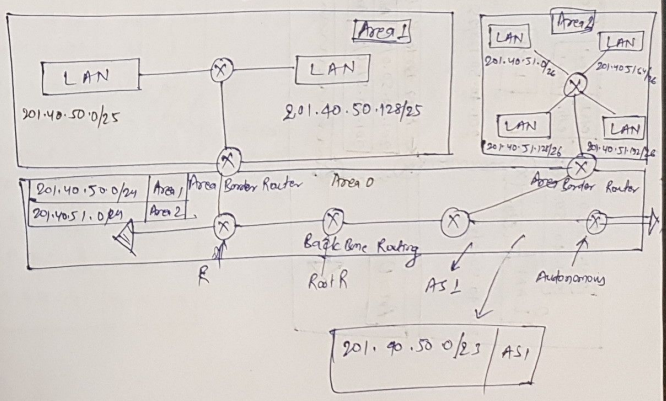






Intra Domain Routing Protocol :-

↳ Single Autonomous System

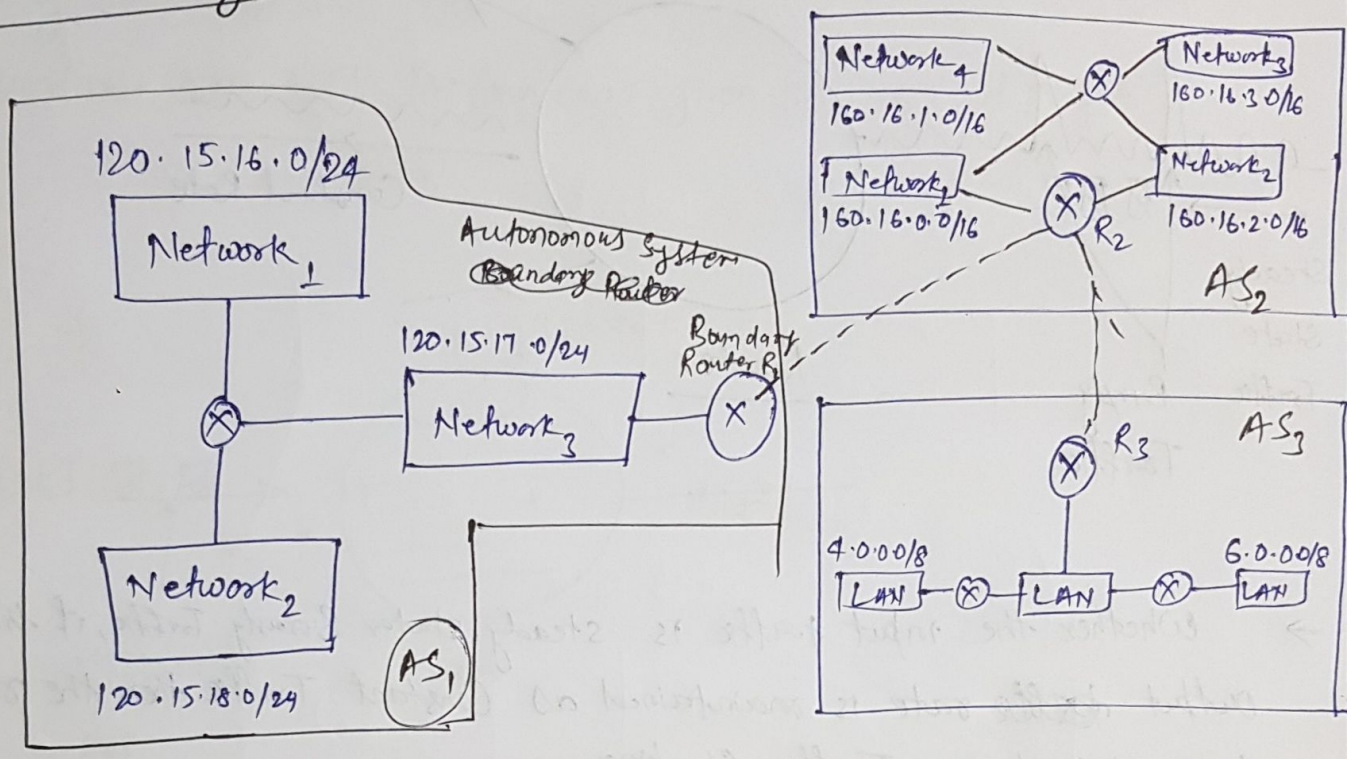


Intra Domain Routing Protocol :

↳ Single Autonomous System

Inter Domain Routing Protocol :-

Path Vector Routing :-



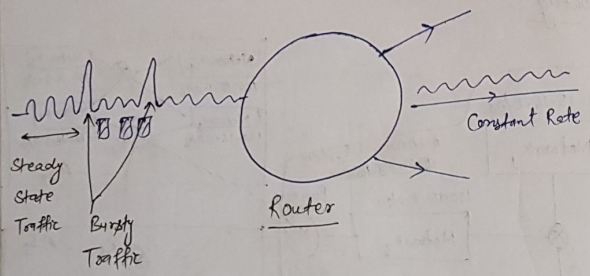
Network Path R_1

Network	Path
120.15.16.0/24	AS_1
120.15.17.0/24	AS_1
120.15.18.0/24	AS_1
160.16.0.0/16	$AS_1 \rightarrow AS_2$
160.16.1.0/16	$AS_1 \rightarrow AS_2$
160.16.2.0/16	$AS_1 \rightarrow AS_2$
160.16.3.0/16	$AS_1 \rightarrow AS_2$
4.0.0.0/8	$AS_1 \rightarrow AS_2 \rightarrow AS_3$
5.0.0.0/8	$AS_1 \rightarrow AS_2 \rightarrow AS_3$
6.0.0.0/8	$AS_1 \rightarrow AS_2 \rightarrow AS_3$

→ Address Aggregation (Supernetting)

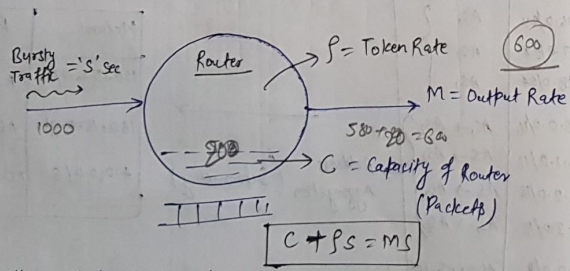
Network	Path
120.15.16.0/22	AS_1
160.16.0.0/14	$AS_1 \rightarrow AS_2$
4.0.0.0/6	$AS_1 \rightarrow AS_2 \rightarrow AS_3$

Traffic Shaping :-



→ Whether the input traffic is steady state or Bursty Traffic, if the output rate is maintained as Constant Traffic then the router has acheived the Traffic Shaping.

→ If initial capacity is less then more tokens are generated then more amount of data is forwarded but total data is constant.



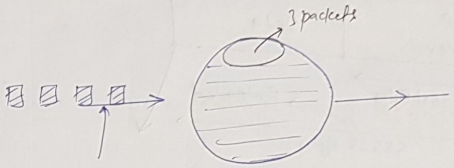
If the initial capacity is high then less tokens are generated then less amount of data is forwarded but total data is constant.

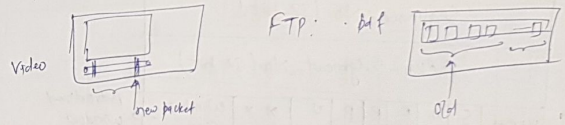
Load Shedding :-

→ It is a way of loosing packets when the packets cannot be handled by router.

→ Applications like FTP preference is given to the old packets.

→ " " multimedia, " " " new "





Q. C + ρs = Ms

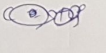
Initial capacity, C = 1 Mbits

Token rate, ρ = 6 Mbps

O/p Rate M = 8 Mbps

Cal. time of Bursty Traffic that can be handled.

Soln:



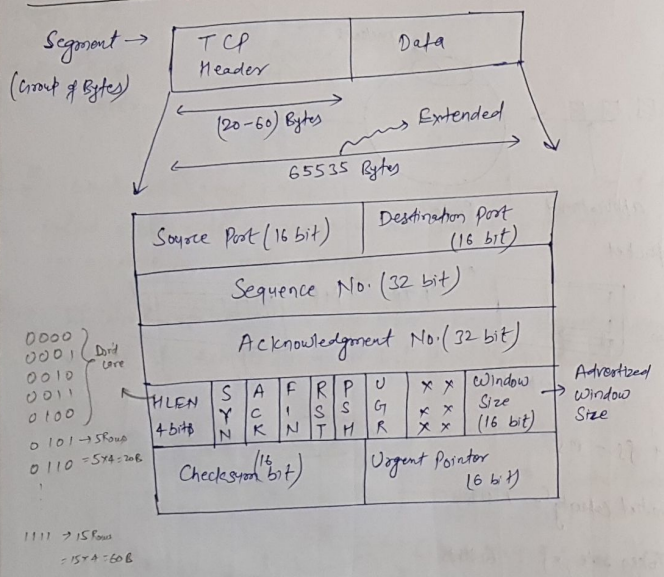
$C = (M - \rho) S$

$S = \frac{C}{M - \rho} = \frac{10^6}{8 \times 10^6 - 6 \times 10^6} = \frac{1}{2} = 0.5 \text{ sec}$

Transport Layer

Transport layer is responsible for process to process delivery or End to End delivery and the process will be identified by Port Address.

TCP Protocal :- (It supports Full Duplex).



{ Go Back N ARQ
Selective Repeat N ARQ }

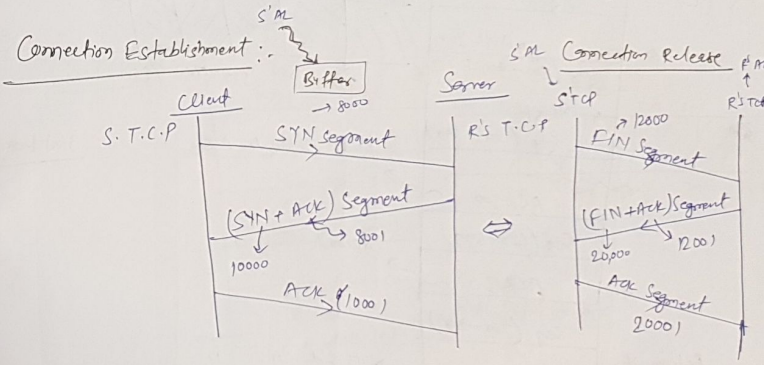
TCP → (i) Connection Establishment
(ii) Data Transfer
(iii) Connection Release

→ In the data link layer, sequence no. is provided for every frame where as in Transport layer, TCP protocal sequence no. are provided for every byte in the segment.

→ The initial sequence no. will always be a random number within the range $(0 \text{ to } 2^{32}-1)$.

FIN → Finished

Connection Establishment :-



→ For a complete connection establishment 3-way handshaking is required

→ SYN segment does not carry any data but it consumes 1 seq. no.

~~FIN & RST~~

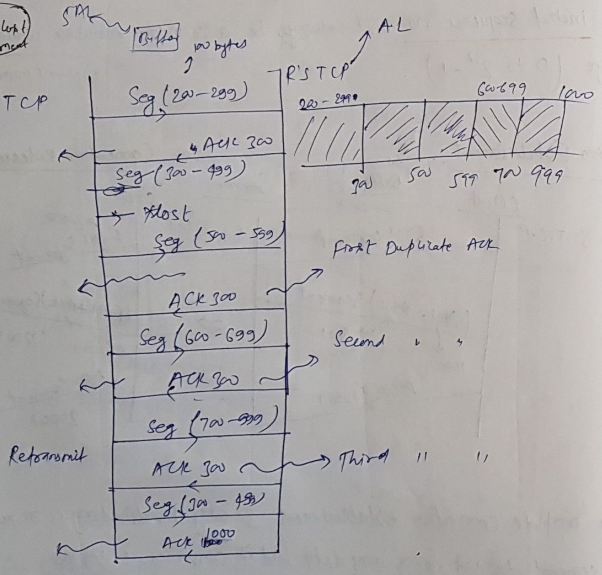
~~Connection~~ Release :-

→ For a complete connection release, 3-way Handshaking is required. In this connection release also, control ~~signal~~ segments are transmitted.

→ TCP can accept out of order segments but always sends in order ACKs.
(out of order: Selective Repeat ARQ; in order: Go Back N ARQ)

Data unit or Segment

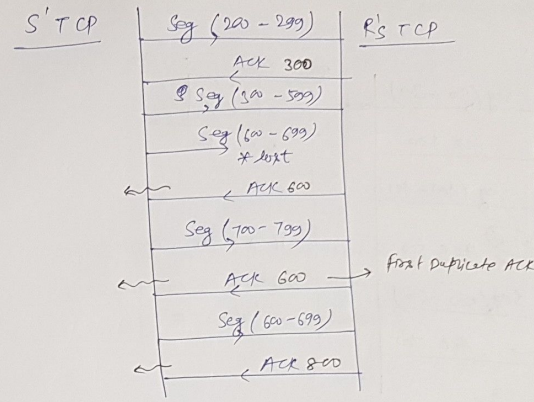
eg:



Seg (200 - 299)
↓
Seq no of 1st Byte in the segment

eg

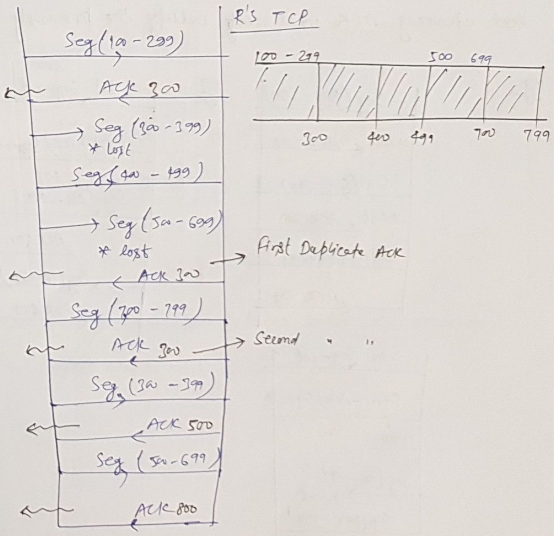
Segment lost



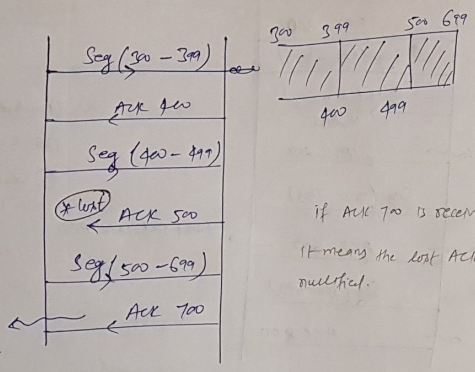
① what is expecting
② " got
③ what it's understood
↳ reached safely or not

eg:

Segment lost



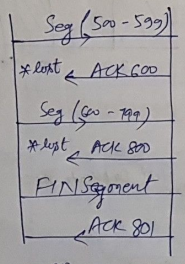
Ack is lost :-



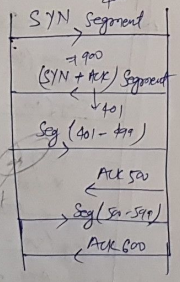
if Ack 700 is received then it means the lost Ack 500 is nullified.

Whenever the Acks are lost, TCP will not bother about it bcoz the next upcoming ACK will ~~nully~~ nullify the previously lost ACK.

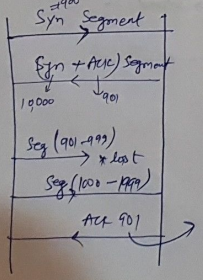
eg.



eg



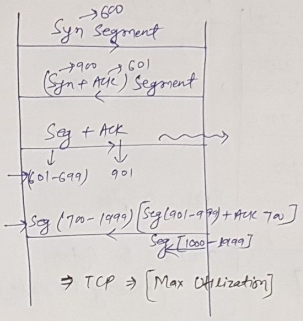
if Lost

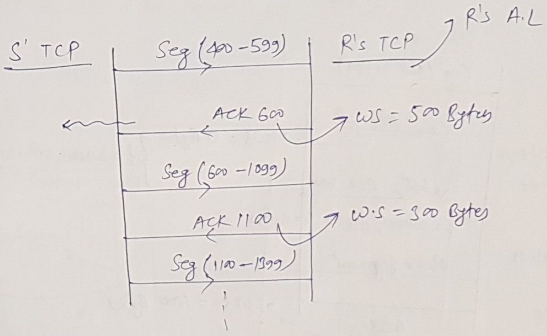


Duplicate Ack

Full Duplex :-

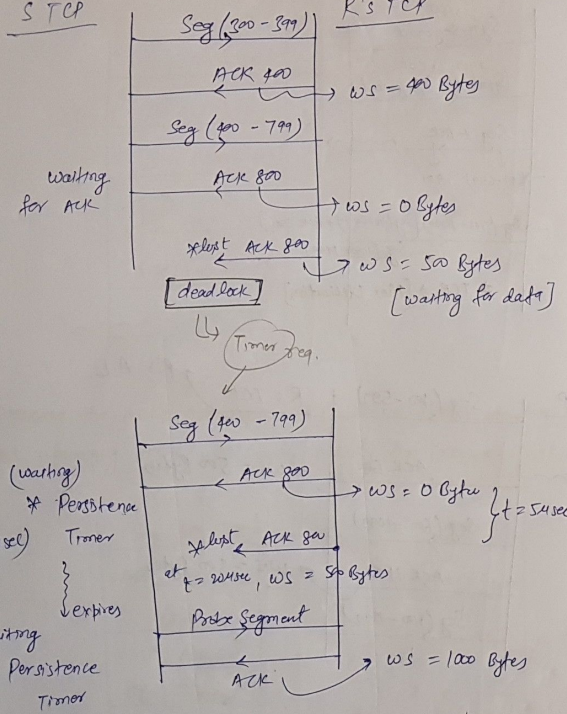
TCP does not bother about Acks.



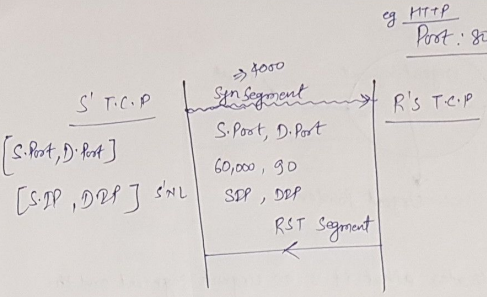


→ Window Size is used for synchronization between sender and receiver.

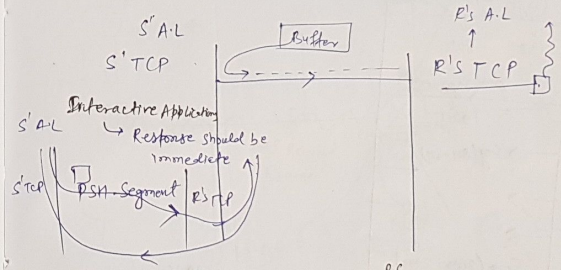
→ TCP provide flow control end to end in the Internet.

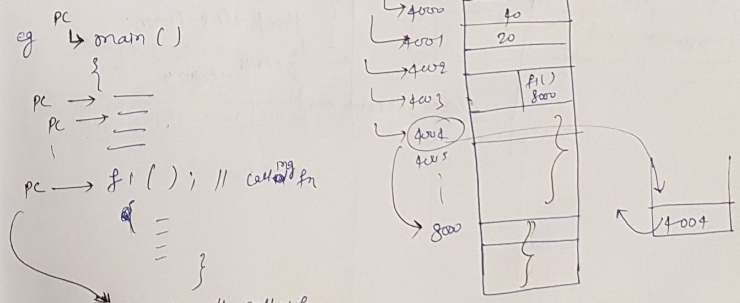


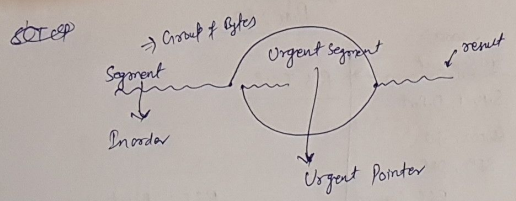
there exists HTTP, FTP... SMTP Server, There are the services that are provided by Server



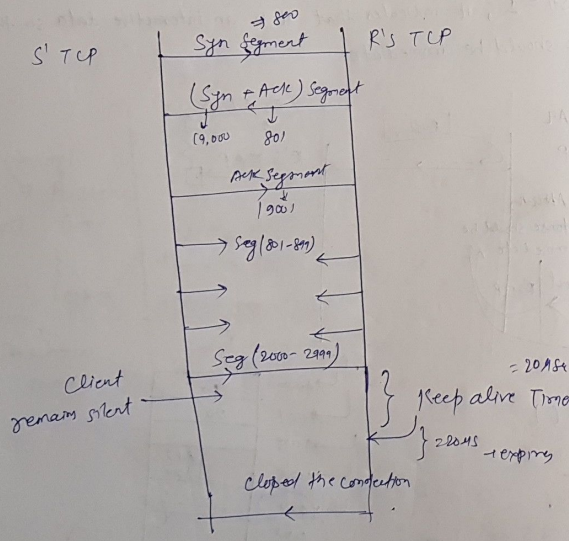
→ If PSH = 1, it indicates that it is an interactive data so the response should be immediate.

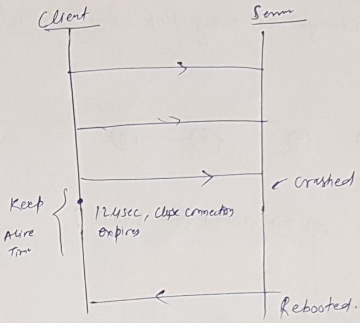




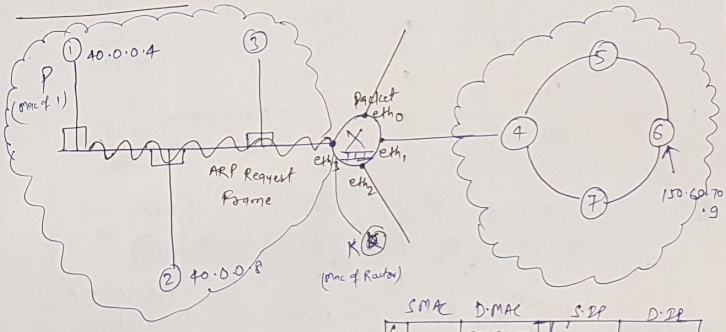


→ If URG = 1, it indicates that it is an urgent segment and the address of Urgent Data 100 is available in Urgent Pointer.





TCP Checksum :-



C:\> ping - t 150.60.70.9

P	FF:FF:FF:FF:FF:FF	D	40.0.0.4	150.60.70.9

S.IP D.IP

ARP Request Frame

K	FF:FF:FF:FF:FF:FF	40.0.0.4	150.60.70.9	

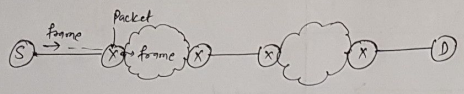
S.MAC D.MAC S.IP D.IP

IP Packet

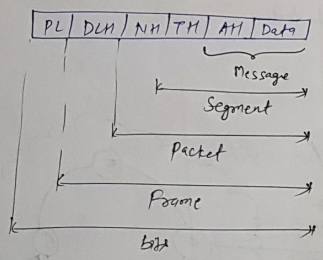
Frame

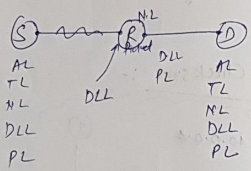
→

→ MAC address will change at every Hop when data is transmitted from end to end.

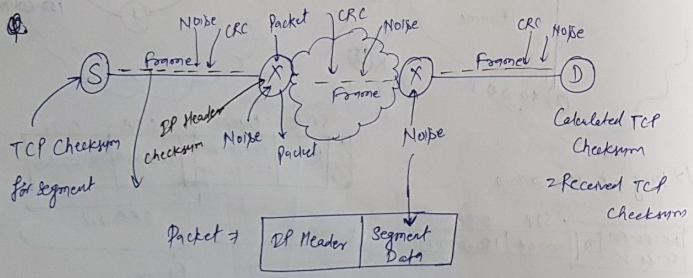
Q. 

* (i) Cal. no. of times DLL, NL are visited from S to D ?



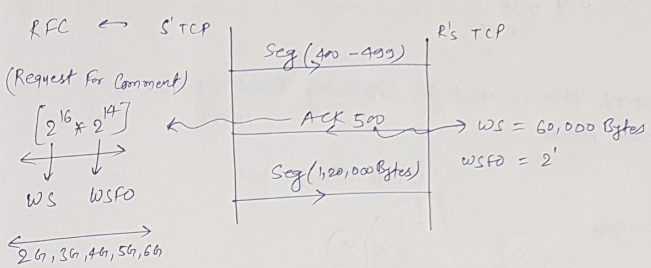


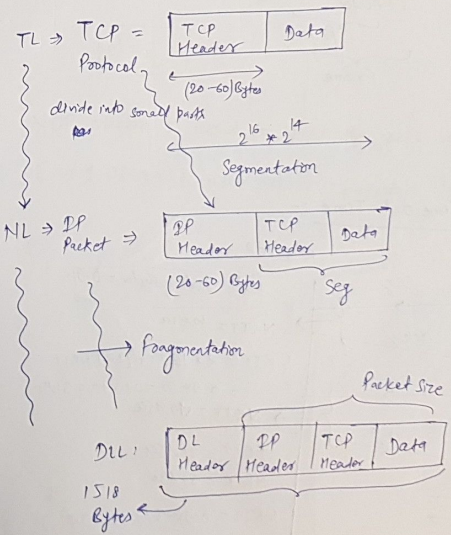
⇒ DLL = 4 Times
NL = 3 times

Q. 

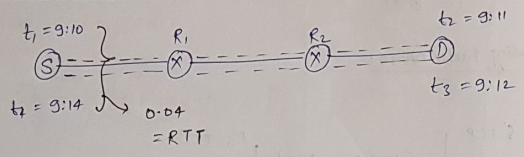
Options & Padding :-
↳ (40 Bytes)

(i) Window Scaling Factor Option :-

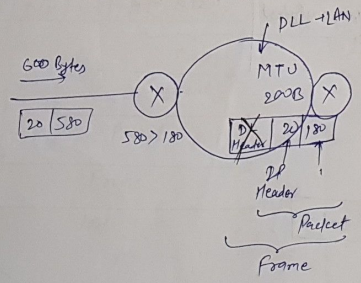




(ii) Time stamp option :-

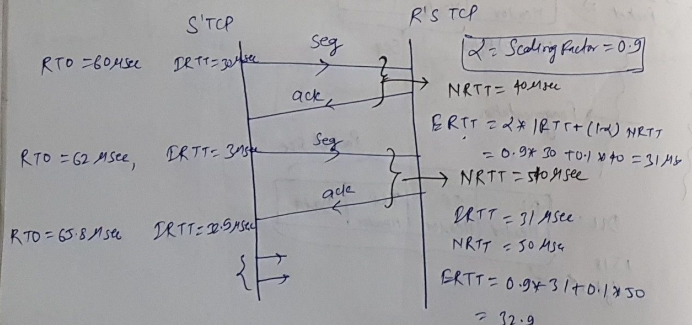


Time stamp option is used for calculating Round Trip Time b/w two end process (RTT)



RTO Timer :-

→ Retransmission after Time out Time :-



$$ERTT = \alpha * ERTT + (1-\alpha)\, NRTT$$

Estimated RTT — Initial RTT — New RTT

$\alpha \Rightarrow$ Scaling Factor

Q. For what value of α ERTT will be the avg of ERTT & NRTT

$$ERTT = \frac{ERTT + NRTT}{2}$$

$$\Rightarrow 2 \cdot ERTT + NRTT - 2 \cdot NRTT = \frac{I+N}{2}$$

$$\Rightarrow \alpha (I-N) + N = \frac{I+N}{2}$$

$$\Rightarrow \alpha (I-N) = \frac{I+N}{2} - \frac{2N}{2} = \frac{I-N}{2} \qquad \alpha = \frac{1}{2}$$

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

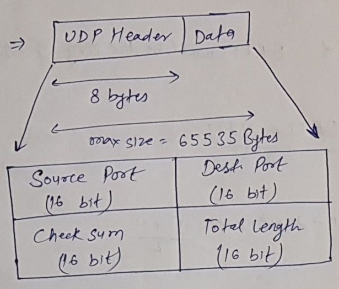
→ NOP option is used to fill the gaps between options.

→ End of option is used as a separator b/w header & data.

UDP Protocol :- (User Datagram Protocol)

Data is called Datagram.

Datagram ⇒ | UDP Header | Data |



eg.

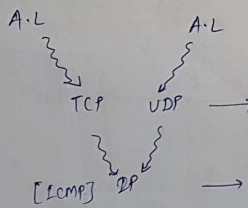
(i) Total length bits of UDP Protocol : 00000000 11111111
= 255 B

∴ Size of Datagram = 255 Bytes

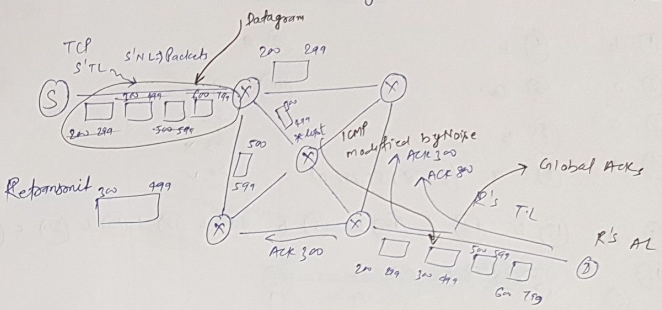
∴ Datagram : Header + Data = Packet Size

⇒ 8 B + Data = 255 B

∴ Data = 247 B Ans



→ TCP can accept out of order segments but sends In order ACK.



Difference b/w TCP & UDP :-

	TCP	UDP
①	Connection oriented virtually	Connection less.
②	Global ACK	NO ACK
③	Flow Control (window size)	No Flow Control
④	Error Control (TCP Checksum)	No Error Control
⑤	Reliable	Unreliable
⑥	Slow	Fast
⑦	Segments will wait at receiver's TCP.	Datagram will travel independently.
⑧	TCP does not support Multicasting & Broadcasting	UDP supports multicasting & Broadcasting.

Workbook Chap-5 Network Layer

① b ⑤ b ⑨ a

② a ⑥ d ⑩ S_1 ✓ d

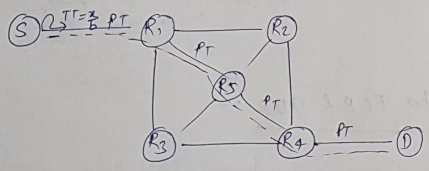
③ c ⑦ b S_2 ✗

④ d ⑧ a (255.255.252.0) S_3 ✗

S_4 ✓

⑪ a ⑬ b ⑭ d ⑮ b ⑯ b ⑰ b ⑱ d ⑲ b ⑳ c ㉑ a

⑫ c



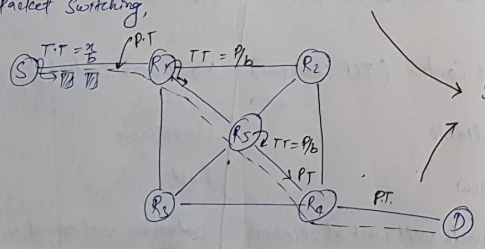
Circuit set up Time = 's' sec

Propagation delay = 'd' sec/hop

1 hop = 'd' sec

'K' hops = Kd sec ⇒ $\boxed{s + \frac{x}{b} + Kd}$ Ans

If it was Packet Switching,



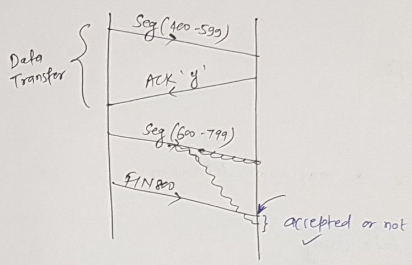
$S > (K-1)\frac{P}{b}$

$x = q \times P$ P: Packet size

q: No. of packets. $\frac{x}{b} + Kd + (K-1)\frac{P}{b}$

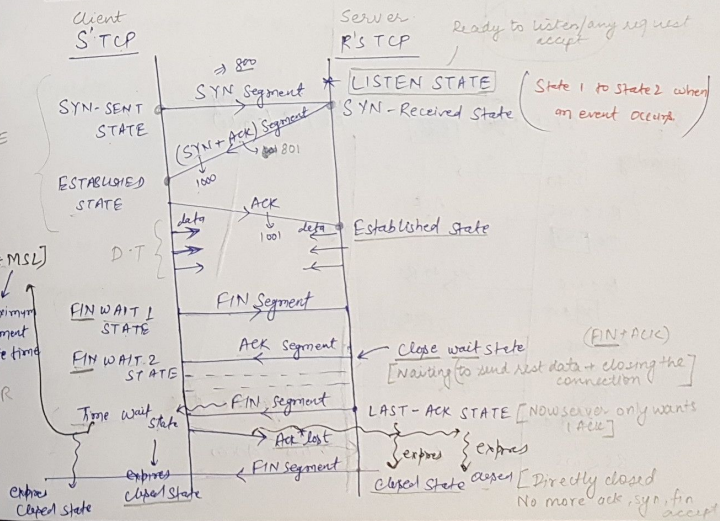
㉒ ㉓ ㉔

eg



Whenever a FIN segment is transmitted, a timer is started. Before that timer expires, receiver can accept delayed segment or lost segment.

State Transitions of TCP :-



TCP ⇒ Full Duplex Operation

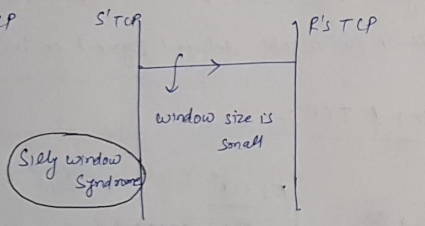
S'AL

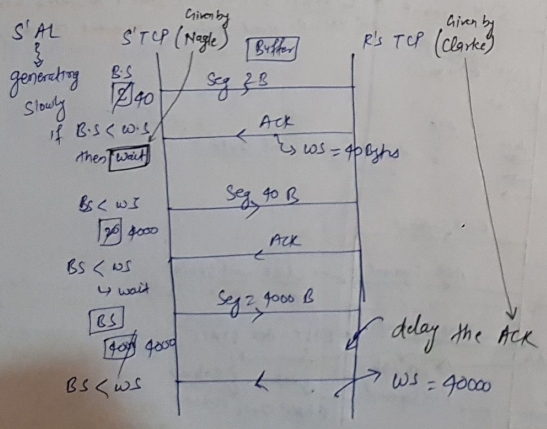
S'TCP ⇒ [$2^{16} * 2^{14}$] RFC

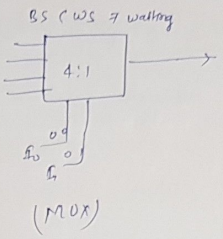
large size ⇒ maximum utilization

S'AL → generating data slowly

small data



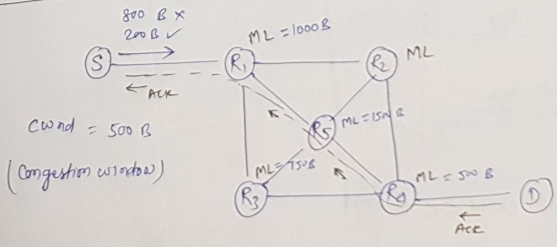




→ When the applications are generating the data slowly, 'Nagle' suggested that to send the data as it is and start buffering the remaining data. Once the ACK is reached to the sender, buffer size will be compared with window size. If it is less sender will wait until the buffer size is equal to the window size and then start sending the data.

→ Clarke suggested that, delay the ACK. So ~~parallely~~ parallely, window size will increase along with that buffer will also going to increase so ~~the~~ the next time more data will be transmitted.

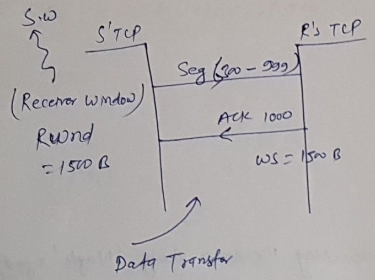
Congestion Policies of TCP :- (cwnd < Rwnd)



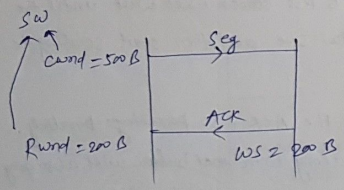
ML = Max Limit

If more data than the ML value is given to the router, data will be dropped as Router will be congested.

(i) TCP is connection oriented

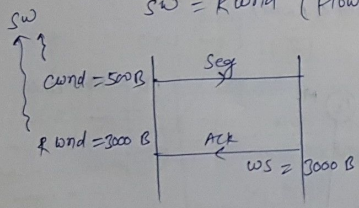


$SW = \min(cwnd, Rwnd)$



If $Rwnd << cwnd$

$SW = Rwnd$ (Flow Control Policies of TCP)



If $cwnd << Rwnd$

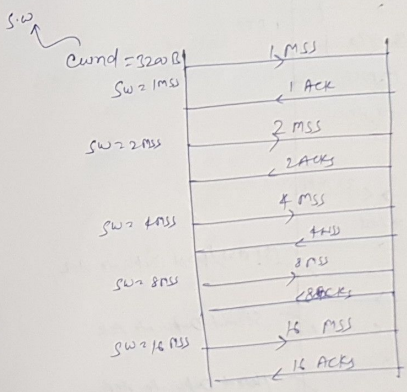
$SW = cwnd$ (Congestion Policies of TCP)

Congestion Policies of TCP :-

1. Slow Start Algorithm
2. Congestion Avoidance
3. Congestion Detection

1. Slow Start Algorithm :- (Exponential Algorithm)

Condn: $cwnd << Rwnd$ | Applied by TCP.



SS Threshold $= \frac{1}{2} *$ Congestion Window

$= \frac{1}{2} \times 3200 = 1600$

MSS : Maximum Segment Size

Initially, Sender window Size,

$SWS = 2^0$ mss

After 1 RTT, $SWS = 2^1$ mss

2 RTT, $SWS = 2^2$ mss

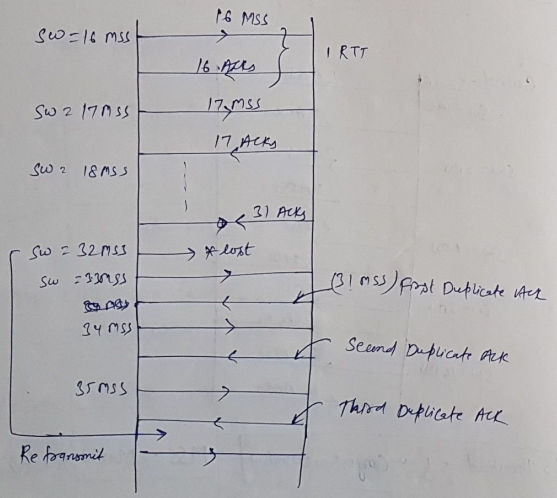
n RTT, $SWS = 2^n$ mss $\Rightarrow$ Exponential

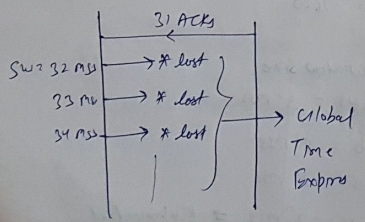
→ Increase of Slow Start Algo, the increase of sw size is based on the number of ACKs.

→ Initially, SS Algorithm increases Exponentially SS Threshold.

(2.) Congestion Avoidance Algorithm:

(Additive Increase Algorithm)





(3.) Congestion Detection :- (Multiplicative Decreasing)

Data is lost and after three duplicate ACKs, data is accepted.
(Weak Possibility of congestion)

$SW = \frac{1}{2} * Present\ Window$

Data is lost continuously until the global timer expires ⇒ Strong possibility of congestion.

SW = 1 MSS

Slow Start Algorithm

(Threshold = $\frac{1}{2}$ * Present window)

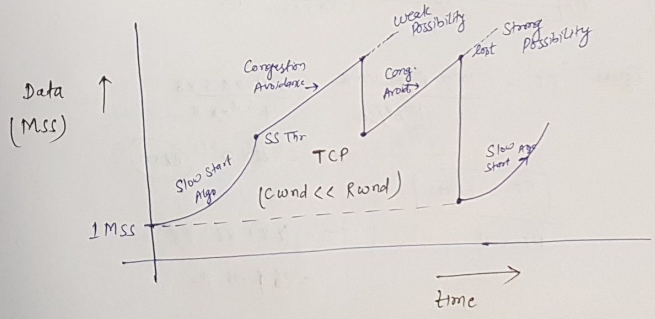
eg SW = 100 B ← Slow start

200
400
800
1600 ← Congestion Avoidance
1700
1800 * lost
≡ ← weak possibility

900
1000
1100
1200
1300
1400 * lost
≡ Strong possibility

100 Bytes ← Slow start (700)
200
400
700 ← C.A.

cwnd < Rwnd



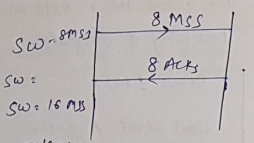
Q. Present Sender Window Size = 800 B

1 MSS = 100 B

Slow start Algo is used.

What is next sender window size ?

Soln:



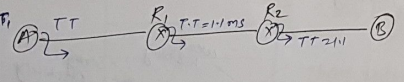
$= 16 \times 100$

$= 1600$ B Ans

Q. Consider the store & forward packet switched network given below (Ignore Processing Time, Propagation Time & Queuing Delay)

BW of each link is 10^6 bits/sec. A user on host A sends a file of size 10^3 bytes to host B through routers R_1 & R_2 in three different ways. In the first case a single packet containing the complete file is transmitted from A to B. Each packet contains 100 bytes of header.

Soln:



Case 1: Ignore $TT = \frac{1000\ B + 100\ B}{10^6\ B/sec} = \frac{1100\ B \times 8}{10^6\ B \times 8\ B}$

$= 8.8 \times 10^{-6+2}$ 8.8 ms

$TT = 1.1$ ms

$PT = 0$

$\therefore TT = 8.8 + 8.8 + 8.8$

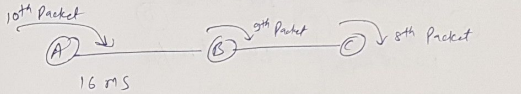
$= 26.4$ ms Ans

(ii) File is split into 10 equal parts :-

No. of bytes in each packet $= \frac{1000 \text{ bytes}}{10} = 100$ bytes

Header = 100 bytes

TT of 1st Packet $= \frac{100\ B + 100\ B}{10^6 \text{ bit/sec}} = \frac{200 \times 8}{10^6} = 1.6$ ms



$= 16 + 1.6 + 1.6$

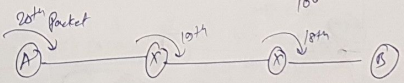
$= 19.2$ ms

(iii) File is divided into 20 equal parts :-

Each Packet Size $= \frac{1000 \text{ bytes}}{20} = 50$ Bytes

$\therefore$ TT of 1st Packet : $\frac{(50 + 100) \text{ Bytes}}{10^6 \text{ bit/sec}}$

$= \frac{150 \times 8}{10^6} = 1.2$ ms

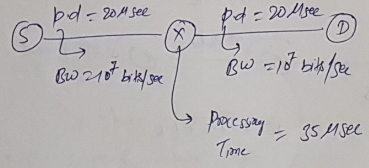


$24 + 1.2 + 1.2$

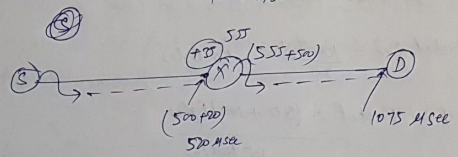
$= 26.4$ ms

Q Two hosts are connected via a packet switch with 10^7 bits/sec. links. Each link has a propagation delay of 20 msec. The switch begins forwarding a packet 35 msec after it receives same. If 10000 bits of data are to be transmitted between two hosts using packet size of 5000 bits, the time elapsed between transmission of first bit of data & reception of last bit of data in msec ——?

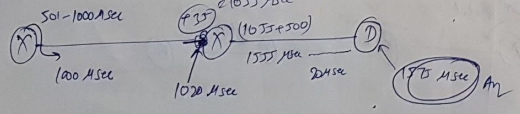
Soln:



1st Packet, $\Rightarrow TT = \frac{5000 \text{ bits}}{10^7 \text{ bits/sec}} = 500 \text{ msec}$

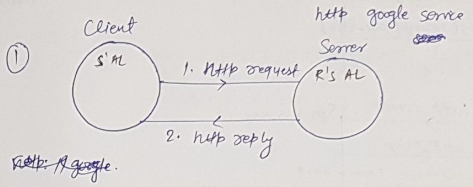


2nd Packet,



Application Layer

HTTP Protocol :- Port No: 80



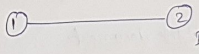
http://www.google.com

URL : Unified Resource Locator

② Synchronous Protocol

③ Client-Server Protocol

It is known as Synchronous Protocol because the clock of the client should be synchronized with the clock of the server

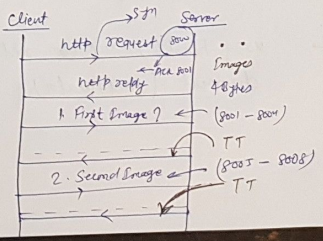


④ Persistent http connection

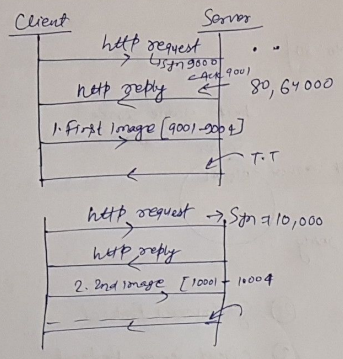
⑤ Non Persistent http connection

Persistent http connection :-

User friendly

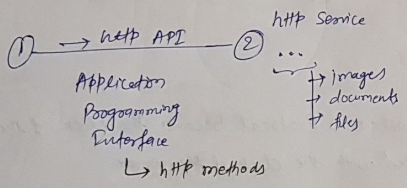


Non Persistent http Connection :-



for every data, a fresh connection is required.

⑤



get() :
using get(), we can retrieve the document.

put() :
using put(); we can modify the content in the document.

post();
using post(); we can place the modify document in the server

head();
using head(); we can retrieve the information about the document (meta data).

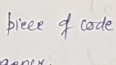
http	Connect()	https	trace()
80		443	route()
	reliable & Secure		

Connect();
When connect(); is used, data will go via secured channel in encrypted form.

⑥ http is a stateless protocal.

Client will not save any info about server. Once connection is closed.

Cookies :- → piece of code,
→ Fast Response
→ Authorization



→ Cookie is a piece of code that is transmitted by the server or the mediating agency.

→ The advantage of cookies is faster response & authorization.

05/08/22

Simple Mail Transfer Protocol (SMTP) →

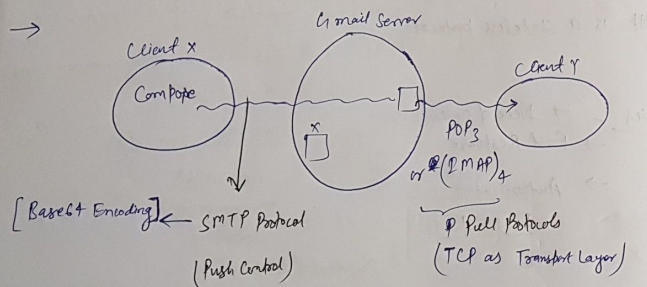
→ SMTP is a Text Based Protocol but we can graphical data also with the help of MIME extension.

↓

(Multimedia Internet Mail Extension).

→ Port 25

→



POP_3 → Post office Protocol (Port: 110) (Accessible in only 1 system) (No longer in use)

$IMAP_4$ → Internet Message Access Protocol. (Accessible in multiple systems) (Port: 143)

→ SMTP combined with POP_3 or $IMAP_4$ is known as Client to client Protocol with the mediation done by mail Server.

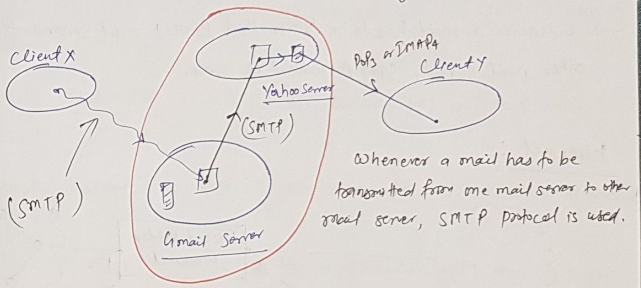
→ SMTP combined with POP_3 or $IMAP_4$ is Asynchronous Protocol bcz when client is sending the data, other client need not to be online.

→ In case of POP_3, only 1 mail account is created on a single device, whereas in $IMAP_4$ a single mail account can be created in multiple devices with proper authorization.

→ In case of $IMAP_4$, mails are kept in hierarchy so that the searching time is less.

→ Security to the mails has been provided by $IMAP_4$ i.e; this protocol will scan the attachment files before the file gets downloaded.

→



Whenever a mail has to be transmitted from one mail server to other mail server, SMTP protocol is used.

Base 64 Encoding: 0-63 = 000000 → 0 ... 111111 → 63

Base 64 ⇒ (A-Z) ⇒ (0-25)

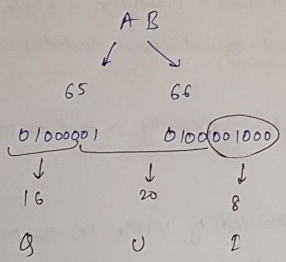
(a-z) ⇒ (26-51)

(0-9) ⇒ (52-61)

+, / ⇒ 62, 63

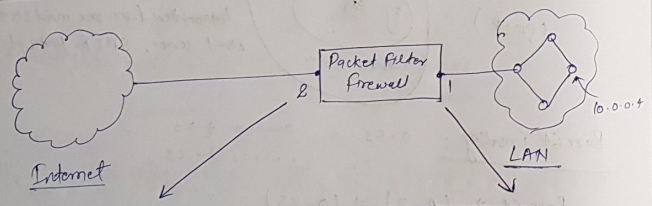
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51

[Subtract -1 from each value]



→ Whenever a mail has to be transmitted from 1 mail server to the other mail server, SMTP protocol is used.

Firewall :-



* : Any value

	Interface	S.IP	S.Port	D.IP	D.Port
1.)	2	144.16.0.0	*	*	*
2.)	2	*	*	10.0.0.4	*
3.)	2	*	*	*	23 → Port of TELNET
4.)	1	*	*	*	80

→ Packet filter firewall is a firewall which blocks or forwards the data by observing the Transport layer and Network Layer Headers of the content.

→ There is no concept of Ideal Firewall. Every firewall will work according to the design principle of that organization.

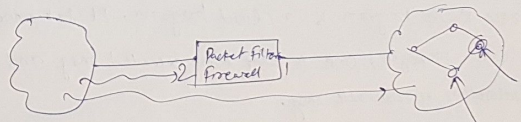
① Packets coming from a particular source IP i.e; 144.16.0.0 are blocked i.e; a particular network is blocked.

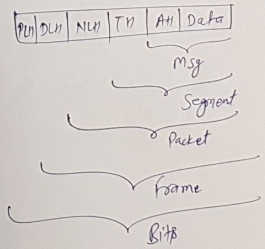
② Packets destinated to 10.0.0.4 are blocked bcz this system is used for internal LAN only.

③ Packets destinated to Port 23 are blocked i.e; a Telnet service is blocked.

④ Packets destinated to Port 80 are blocked i.e; HTTP service is blocked.

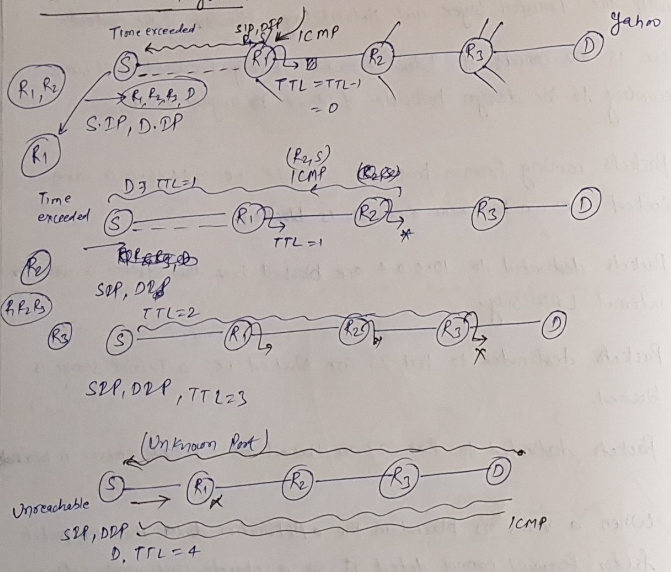
→ When a virus is placed in the Application data then the packet filter firewall cannot detect it, so a separate anti virus software is required.





YTS

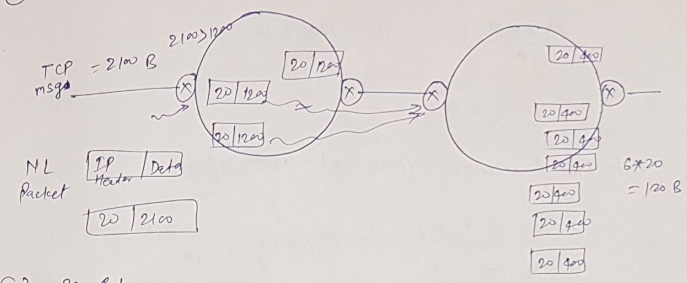
Trace Route Program :-



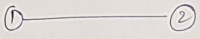
Trace Route Program is a client program. It takes the help of 2 ICMP messages, one is ~~time~~ time exceeded msg and other one is destination unreachable msg.

Workbook Chap-6

(20)



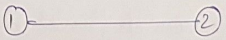
(21) 20 Bytes



Serial Data Transfer

(i) Synchronous Serial Transfer

(ii) Asynchronous Serial Transfer



BW = 1200 bits/sec

In synchronous serial transmission, 3 8-bit sync characters are included in 30 8-bit information characters and the bandwidth of the channel is 1200 bits per second then what is the data rate of receiver?

Sol:

24 sync bits ⟶ 240 bits

24 × 1200 ⟵ 1200 bits

2400

10

120 sync bits

Data rate of receiver = (1200 − 120) = 1080 bits/sec

1 char = 8 bits ⟹ 1080 × 1/8 char/sec

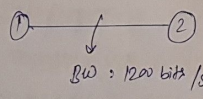
1/8 char = 1 bit

= 135 char/sec

→ ① In synchronous serial transmission, sync characters are added for group of characters.

② These sync bits are only there to provide synchronization. These bits will not be taken by the receiver.

Asynchronous Serial Transfer :-



BW : 1200 bits/sec

Q. In Asynchronous Serial Transmission, one start bit, 2 Parity bit and one stop bit are added for every character then what is the data rate of the receiver if the BW of the channel is 1200 bits/sec, ?

1 char = 1+2+8+1 = 1 start bit + 2 parity bits + 1 char + 1 stop bit

1/12 char ⟵ 1 bit

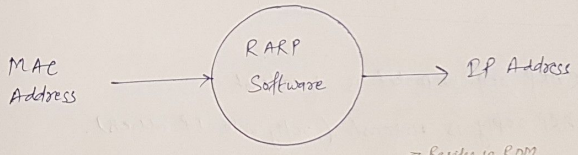
data rate of receiver = 1200 bits/sec = 100 char/sec

= 1200/(1+8+2+1) char/sec = 1200/12 char/sec

In Asynchronous Serial Transmission, extra bits are added for every character. These extra bits are treated as the part of data.

RARP Protocol :

(Reverse Address Resolution Protocol):

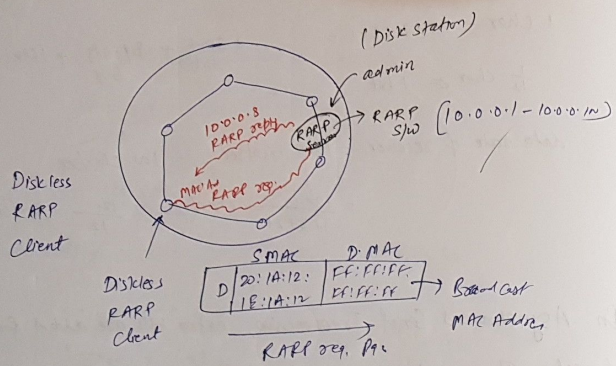


→ Resides in ROM

→ In Hard disk

Diskless Station (No Harddisk) → MAC Address, IP Address ✓ ✗

Disk Station (with Harddisk) → MAC Address, IP Address ✓ ✓



20:1A:12:1E:1A:12

Mapping Address (to get the info of which IP is assigned to a particular MAC Add)

MAC Add	IP Add
20:1A:12:1E:1A:12	10.0.0.8

→ RARP req. packet is broadcast

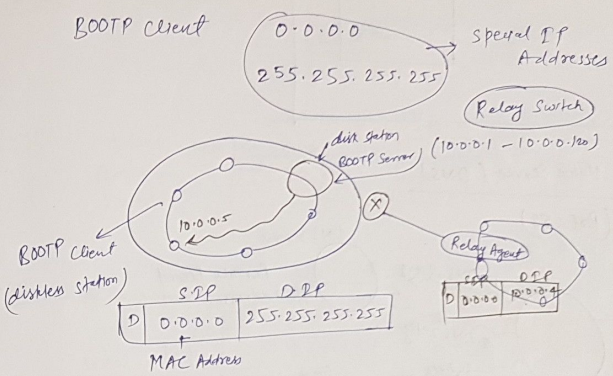
→ RARP reply is unicast (reply with IP address).

→ Even the systems are not having any Harddisk still we can assign IP addresses to the systems at run time using RARP protocol.

Drawback :

For 'n' LAN networks 'n' RARP servers are required so cost is more.

BOOTP Protocol :-



→ Both RARP and BOOTP protocols are static binded protocols, where as DHCP is the both static & as well as dynamic based protocol.

→ DHCP ~~work~~ protocol works at the Application Layer

→ The ports which are used by DHCP protocols are 67 & 68. Both are fixed ports.

→ Whenever a DHCP client is requesting for an IP address, the DHCP server will go the IP address, Subnet Mask, Default Gateway, Local DNS server

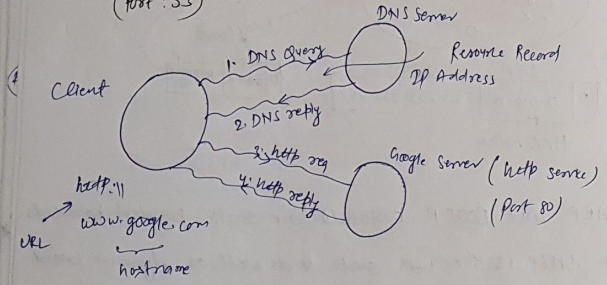
DNS: Domain Name Service

Root Server

Top

Domain Name Service (DNS):

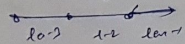
(Port : 53)



Root Server
Top level Domain Server
Authoritative Server
Local DNS Server

DNS Server ⇒ 127 levels

www.google.com

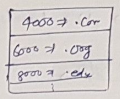


www.kernel.org

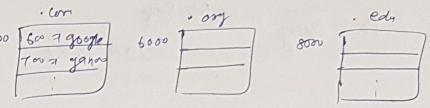
www.yahoo.com

www.iit.edu

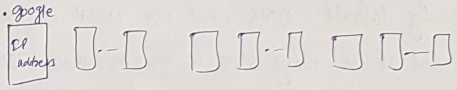
level-1 Root Server

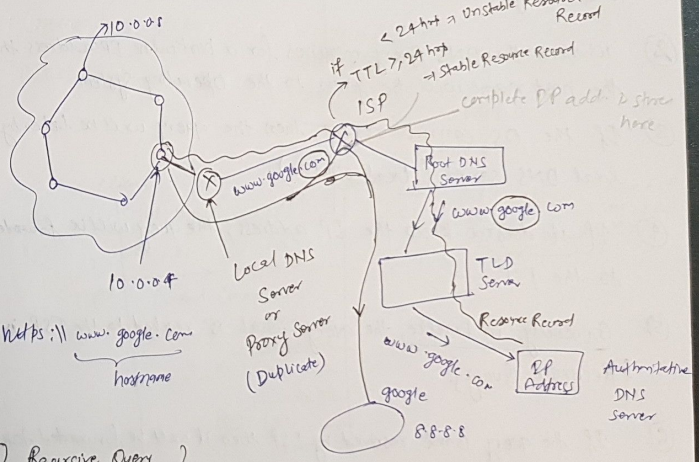


level-2 Top level Domain Server



level-3 Authoritative dns server





① Recursive Query

② Iterative Query

DNS Query ⟶ 127 Levels

DNS Query ⟶ (> 512 Bytes) ⟶ TCP as T.L

DNS Query ⟶ (≤ 512 Bytes) ⟶ UDP as T.L

~~File Transfer~~

① By default, DNS will use UDP as Transport layer Protocol but if the query size is greater than 512 Bytes, it uses TCP as Transport Layer Protocol.

② Whenever the DNS Query requires for a particular IP address then the host name will be given to the Operating System.

③ If the OS cannot resolve, then the query will be taken by local DNS server (local router).

④ If it does not know the IP address, the query will be forwarded to the ISP.

⑤ Generally, in practice, the query which is reached to the ISP is a {Recursive Query}.

⑥ If the query is not resolved by ISP then it will be forwarded to the Root Server.

⑦ The Root server will give the reference of the concerned TLD DNS server then the concerned TLD DNS server will give the reference of Authoritative DNS Server.

⑧ Generally, in practice, the queries which are reached to the Root servers and TLD servers is called {Iterative Query}.

File Transfer Protocol (FTP) :-

Active FTP :-

(1) Downloading the file from authorized server.

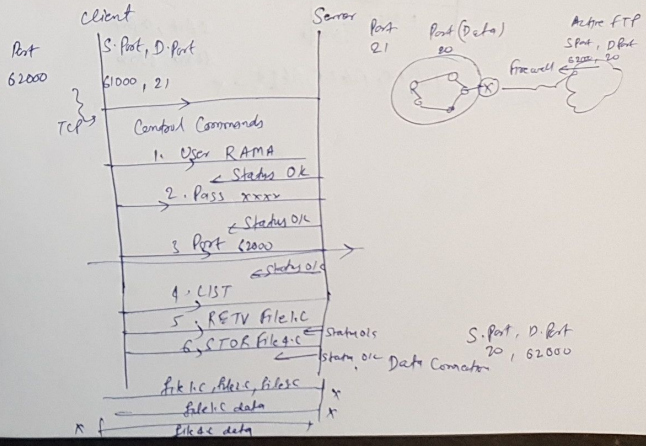
(2) Two Connections → Control Connection (Control Commands) ⇒ Port 21
Two Connections → Data Connection (Data Transfer) ⇒ Port 20

(3) Command ⇒ 4 char

(4) Out of band Connection

Bidirectional Connection

File 1.C
File 2.C
File 3.C
File 4.C



(1) Active FTP supports Bidirectional Connection i.e; even the connection is established from one side, data can be transmitted in both the directions.

(2) FTP supports out of band connection i.e; if the commands are given the control connection then reply might be coming from the data connection.

Passive FTP :-

Control Port	Data Port	
Port 21	62000	File 1.c File 2.c File 3.c