VLSM (Variable Length Subnet Mask)

Rule 1:- whenever we are going to prepare subnet mask we should go for the heighest value to lowest value

ex:- 192.168.1.0000000 $\underset{I_s}{}$

let's take 1'st subnet

- Subnet Id - 192.168.1.0
- Broadcast Id - 192.168.1.127

Subnet Mask - 255.255.255.10000000 (128)

64
32
16
8
4
2
1

ICMP Packet format

In IPv4 → No error reporting + Error correcting mechanism

Overcome by ICMP

- ① Error reporting

- ② N/w Diagnostics
  - Traceroute (Display the routing path b/w two devices)
  - Ping (Test the speed of connection b/w two devices)

ICMP

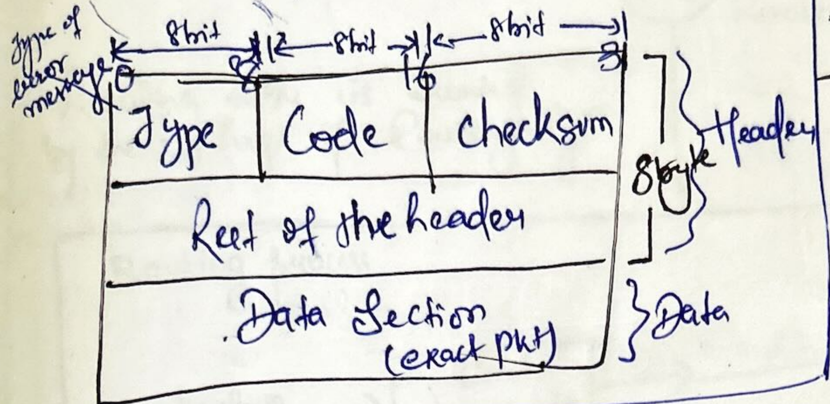
- Error Reporting Messages (Report problem that any host encounter while they are processing the pkt.)
- Query Messages (Help a host or Router to get specific Info. about another host.)

ICMP do not send data directly to ~~Nw layer~~ datalink layer It always work In Compani with Ip

IP Header	ICMP	Data

Ip — encapsulated then send to Datalink Layer

- Message carried in IP datagram
- 8 bytes of Header followed by data
- Data field in Error message carry
- Entries IP header and first 8 byte of data of IP packet that causes the error which helps in diagonsing the problem that caused the ICMP message to be generated.



Header Structure

Type - 1 byte → what type of error is happened.

Error: Destination Unreachable

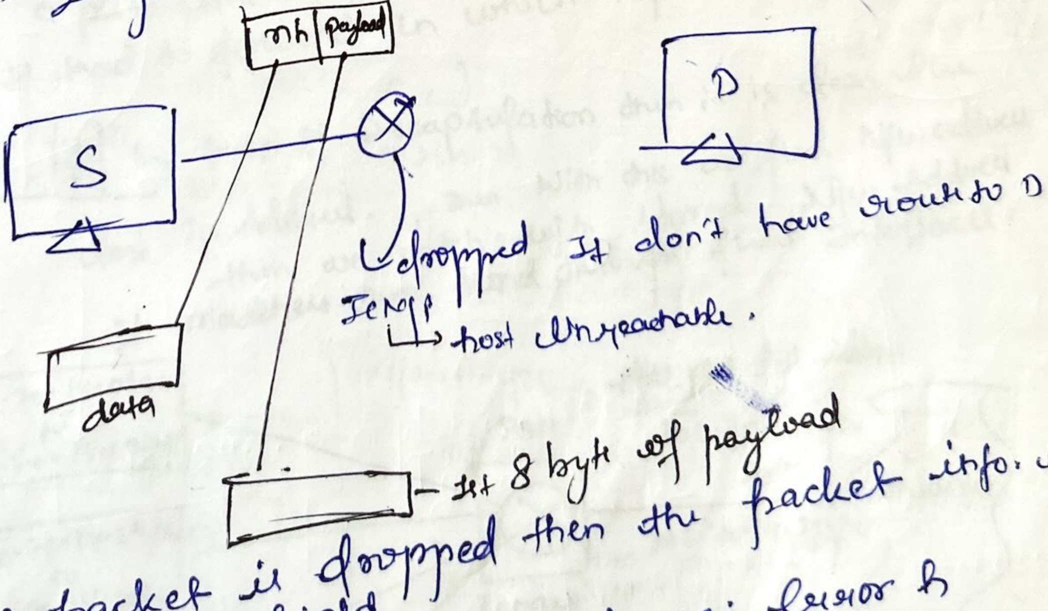
Type = 3

→ It may happen that destination port, host, network Unreachable.

Code → It describe were precisely the Error
1 byte (size)

for each port, host, N/W unique code is assigned.

Checksum → 2 byte



→ When the packet is dropped then the packet info is copied to the data field.

→ Kitna error h aur kis part mai error h yeh N/W header inform krta hai

→ 1st 8 bit of payload.

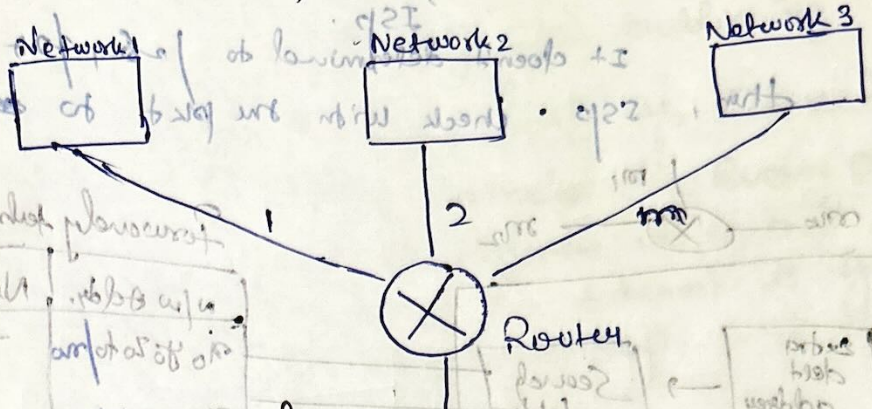
ICMP Message

Error

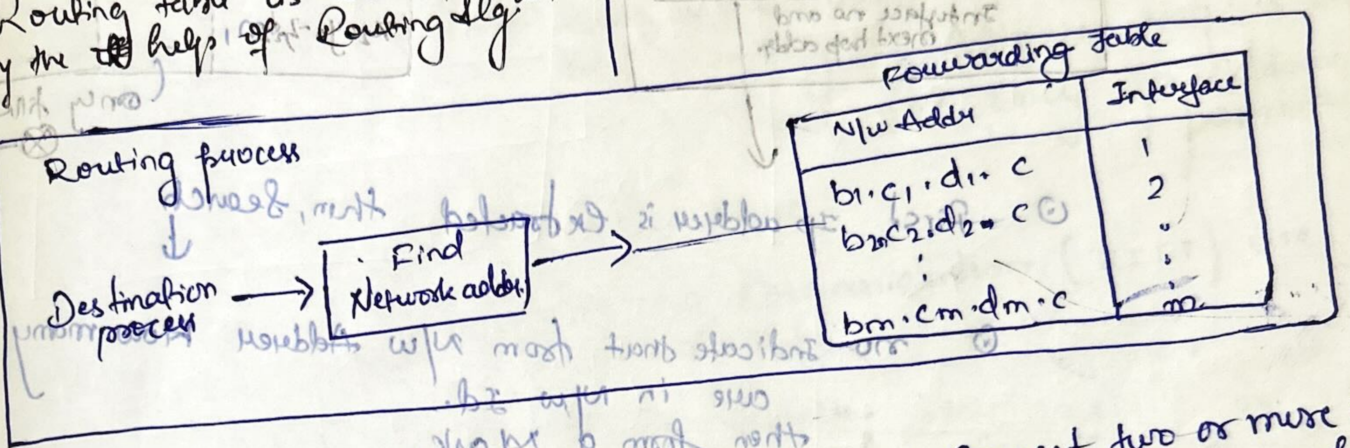
Diagonestic

(Echo, Request, Echo, Reply, Ping)
Are Example of ICMP.

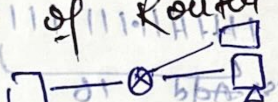
IP packet Forwarding



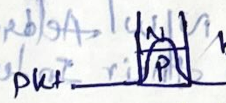
Routing table is created by the helps of Routing Algm.

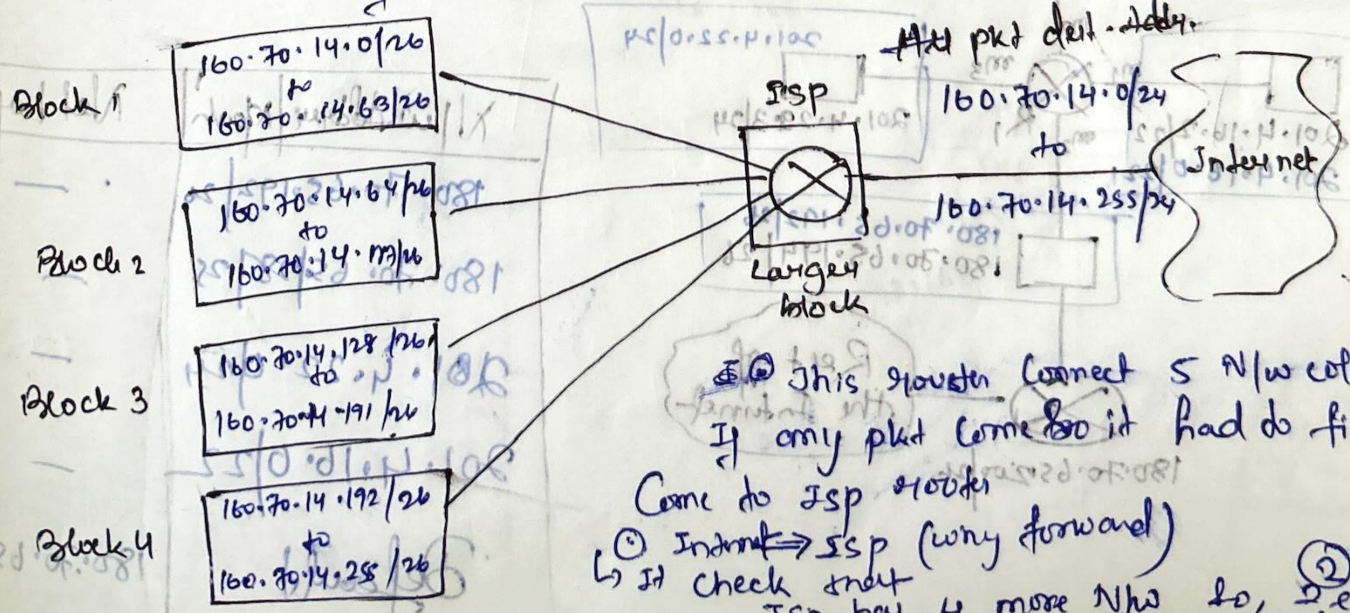


Use of Router :-



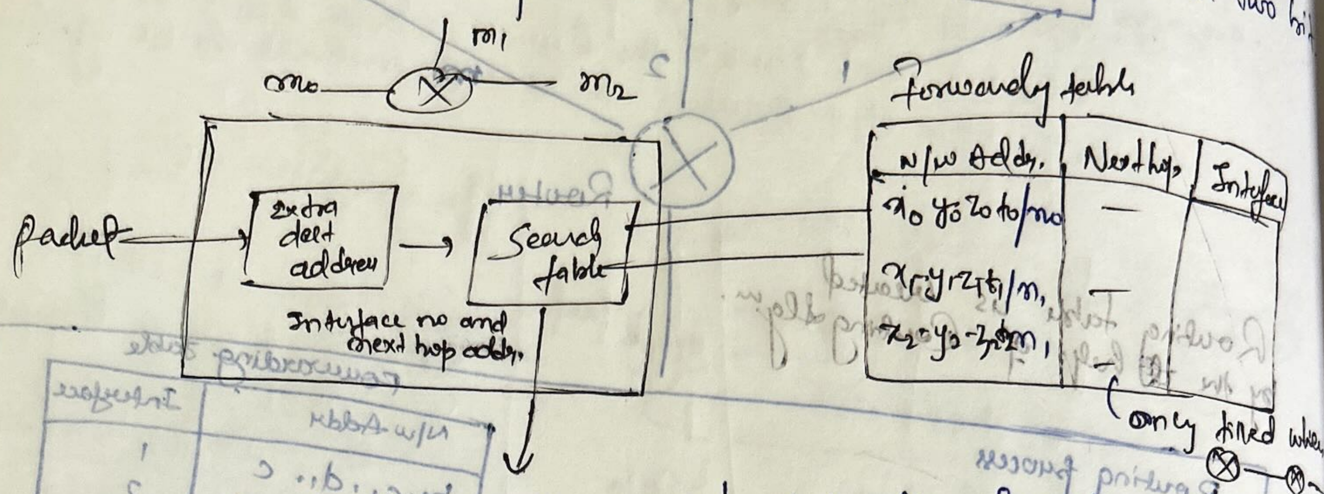
Router is useful when it connect two or more N/w for one N/w switch or hub is enough.

- when a pkt come to from N/w to this Router then, it had to forward in which N/w decided by Router.
-  pkt by help of Decapsulation then it is clean the dest. Ip Address. then with this we find N/w address then we match with stored N/w Address If matches then send through that Interface.



- This router connect 5 N/w colony If any pkt come to it had to first come to ISP router
- Internet ⟹ ISP (why forward)
  ↳ It check that ISP has 4 more N/w so, 2 bit extra from Internet.

⊙ If any pkt with /24 then send to ISP.
It doesn't determined to /26, /27 . . .
then, ISP check with the pkt to extra two bit



⊙ First Ip address is extracted then, search

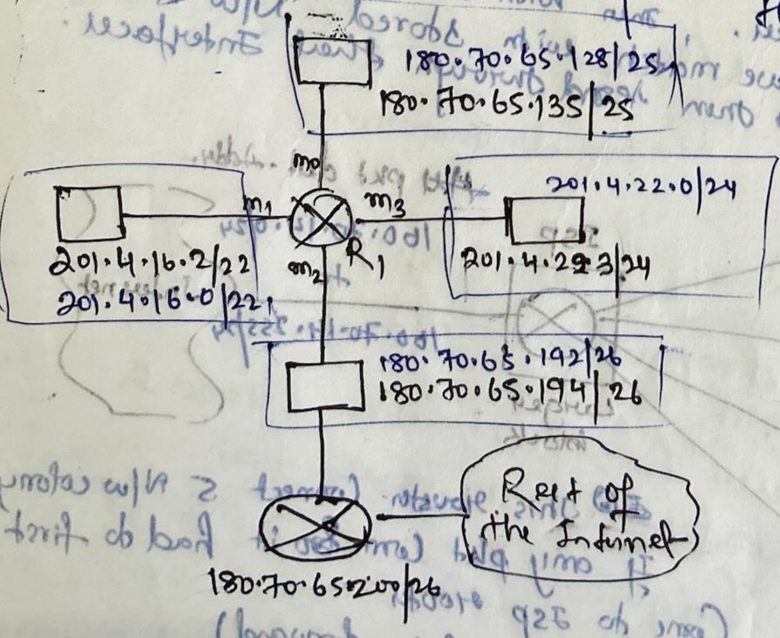
⊙ m0 indicate that from N/w Address How many bit are in N/w Id.
then form a Mask.

suppose m0 = 16   11111111.11111111.00000000.00000000

And bit with Add 16

then we ~~Mask~~ with the dest Ip Address to N/w Mask.

↳ then we find a N/w Id. then we Matches with the N/w Address (forwarding table)
then send to their Interface.



N/w Address	Mask	Next hop	Interface
180.70.65.192	26	—	m2
180.70.65.128	25	—	m0
201.4.22.0	24	—	m3
201.4.16.0	22	—	m1
Default		180.70.65.200	m2

Efficiency (η) = $G \times e^{-2G}$

G no. of station want to transmit the data

highest efficiency = $G \times e^{-2G}(-2) + e^{-2G}(1) = 0$

$= e^{-2G}(-2G+1) = 0$

$-2G+1 = 0$

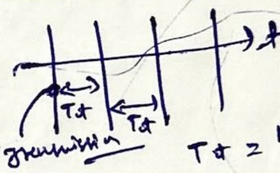
$G = 1/2$

$= 1/2 \times e^{-2 \times 1/2} = \frac{1}{2} \times e^{-1} = 18.4\%$

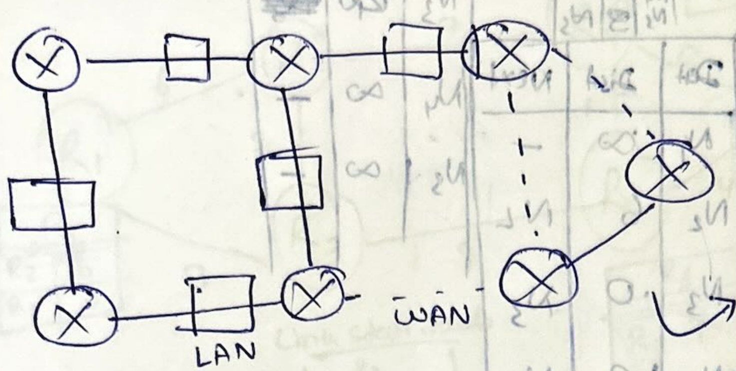
~~Pure Aloha is a simple and lovely random access protocol~~

Slotted Aloha

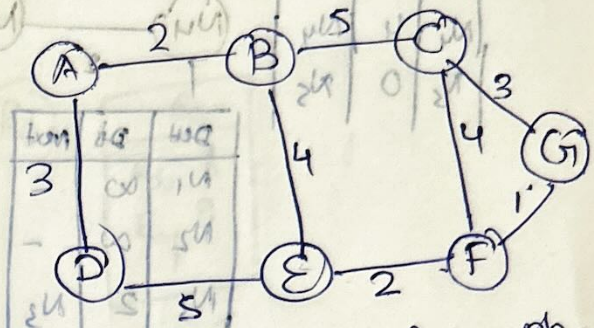
It is a variant of the classical Aloha in which user are synchronized, in the sense that they can only start transmission at the beginning of a time-slot.

Pure Aloha	Slotted Aloha
Any time transmission	 $T_t = M/Bw$ Time is divided into slot, slot = T_t At the begning of slot every one start transmission
① $VT = 2 \times T_t$	① $V_T = T_t$
② $\eta = G \times e^{-2G}$	② $\eta = G \times e^{-G}$ $\Rightarrow G \times e^{-G}(-1) + e^{-G}(1) = 0$ $\Rightarrow e^{-G}(-G+1) = 0$ $-G+1 = 0$ $-G = -1$ $(G = 1)$ so, $\eta = 1 \times e^{-1} = 1/e$ 36.8%
③ $G = 1/2$	
④ 18.4%	

Distance Vector Routing - Bellman Ford.

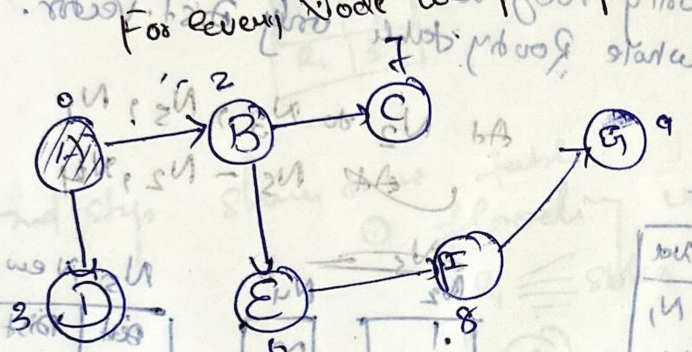


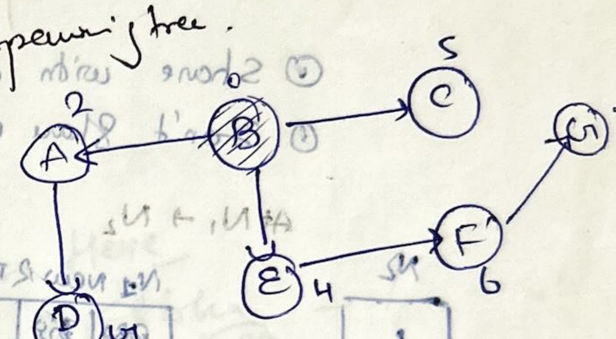
Internet



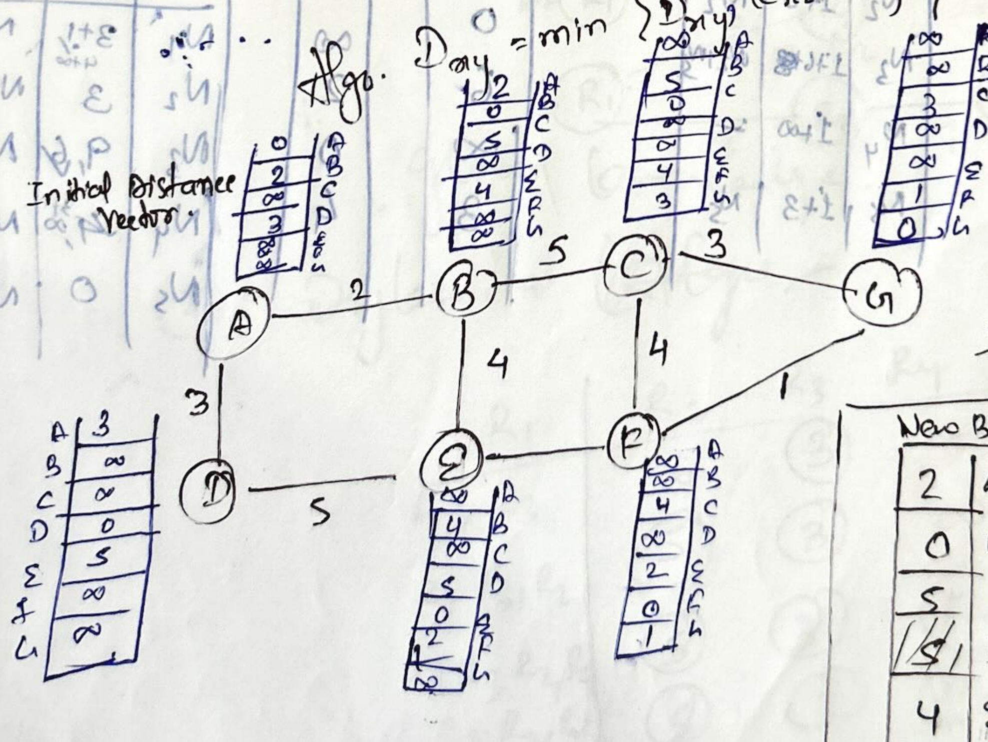
Weighted Graph.

For every Node we find minm Spanning tree.





Algo. $D_{xy} = \min\{D_{xy}, (c_{xz} + D_{zy})\}$



i) only Neighbors

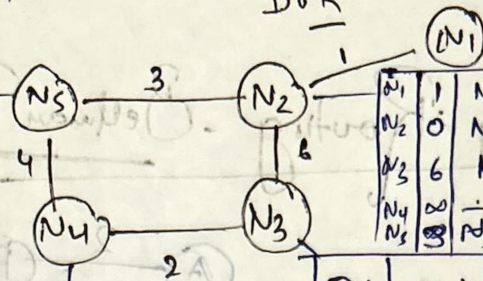
ii) only Distance vector

	New B		Old B		A
A	2	A	2	A	0
B	0	B	0	B	2
C	5	C	5	C	∞
D	5	D	∞	D	3
E	4	E	4	E	∞
F	∞	F	∞	F	∞
G	∞	G	∞	G	∞

Routing table of Router

Dest	Dist	Next
N_1	∞	-
N_2	3	N_2
N_3	∞	-
N_4	4	N_4
N_5	0	N_5

DVR



N_1	1	N_1
N_2	0	N_2
N_3	6	N_3
N_4	∞	-
N_5	3	N_5

Dest	Dist	Next
N_1	0	N_1
N_2	1	N_2
N_3	∞	[illegible]
N_4	∞	-
N_5	∞	-

Dest	Dist	Next
N_1	∞	-
N_2	∞	-
N_3	2	N_3
N_4	0	N_4
N_5	4	N_5

Dest	Dist	Next
N_1	∞	-
N_2	6	N_2
N_3	0	N_3
N_4	2	N_4
N_5	∞	-

- Share with only Neighbour only Dist. vector.
- Don't Share whole Routy table only Dist. vector.

At $N_1 \rightarrow N_2$

N_2
1
0
6
∞
3

N_1 New RT

Dest	Dist	Next
N_1	0	N_1
N_2	1+0	N_2
N_3	1+6	N_2/N_3
N_4	1+∞	-
N_5	1+3	N_5

At N_2 to N_3, N_5, N_1

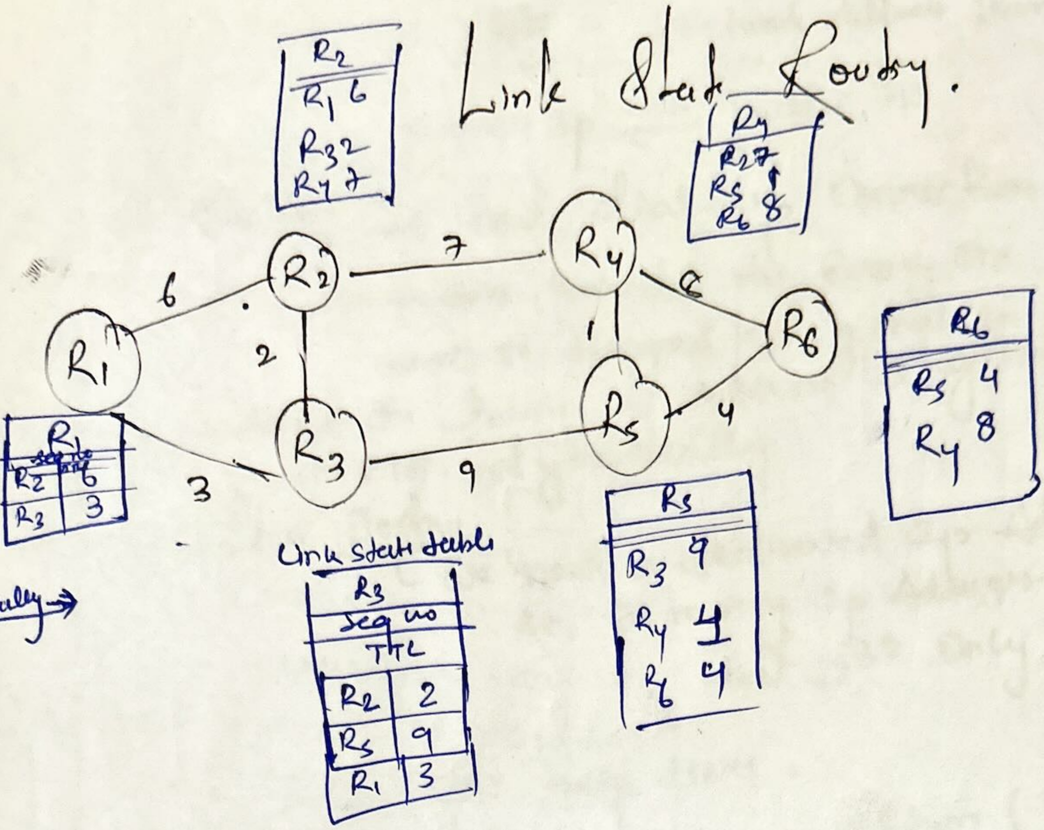
At N_5 - N_2, N_4

N_2	N_4
1	∞
0	∞
6	2
∞	0
3	4

N_5 New RT

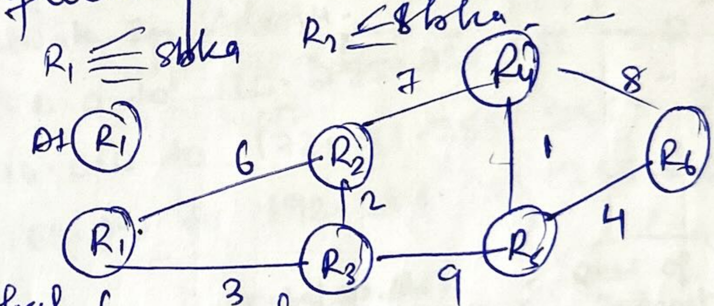
Dest	Dist	Next
N_1	3+1, 4+∞	N_1
N_2	3	N_2
N_3	9, 6	N_3
N_4	4, 3+∞	N_4
N_5	0	N_5

Link State Routing.



2nd step: share there table.

1. flooding use Here



global knowledge.

2. Dijkstra Algo -

	R_2	R_3	R_4	R_5	R_6
R_1	6	3	∞	∞	∞
R_1, R_3	5	3	∞	12	∞
$R_1\ R_3, R_2$	5	3	12	12	∞
$R_1\ R_3\ R_2, R_4$	5	3	12	12	21
$R_1\ R_3\ R_2, R_4, R_5$	5	3	12	12	16
$R_1\ R_3\ R_2\ R_4\ R_5\ R_6$	5	3	12	12	

NAT (Network Address Transfation) ②

private Ip ⇌ public Ip

In starting we had dial-up Connection
↳ Ip Address provided to every one
when It stopped using that Ip Address
~~then~~, the same Ip Address is given to someone else, dynamically.

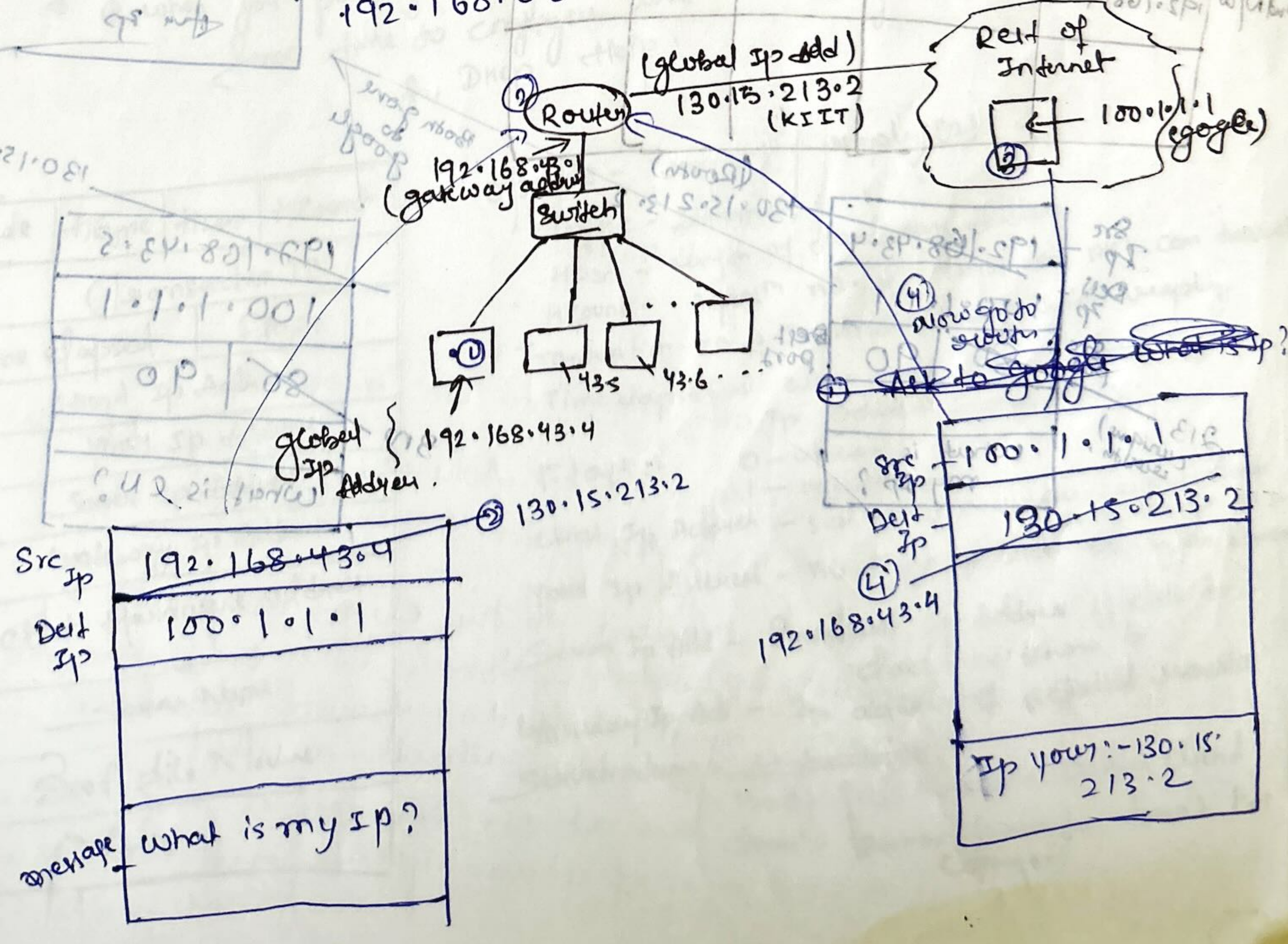
But Today
↳ we need a dedicated Ip Address
so, so many Ip Address req. is there
but 2^{32} only Ip Address possible

NAT Help Here.

Under an Organisation (KIIT) we form a private n/w

Range of private Ip Address.

10.0.0.0 to 10.255.255.255 — 2^{24}
172.16.0.0 to 172.31.255.255 — 2^{20}
192.168.0.0 to 192.168.255.255 — 2



How there Translation is done

↳ In My N/w two many global Ip Address are there suppose, two N/w ask to google ?

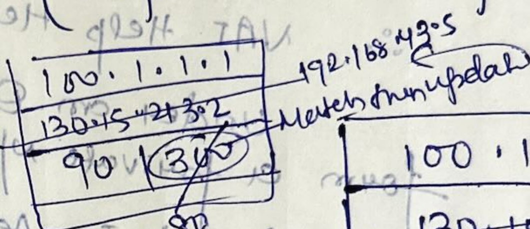
so, 2 pkt form together,

so, 2 Ans will get router from google at '4' step.

Now, How Router will distinguish which Ans or pkt go to whome?

∴ Router use port Address.

(exception i.e. Touching Tp layer)

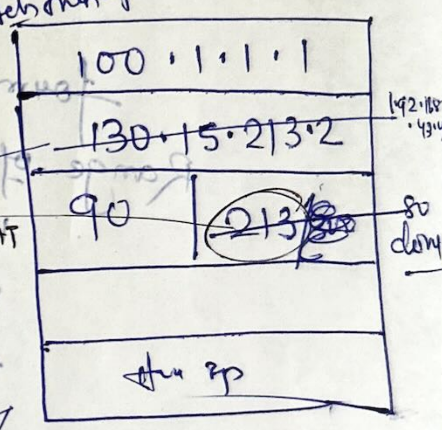


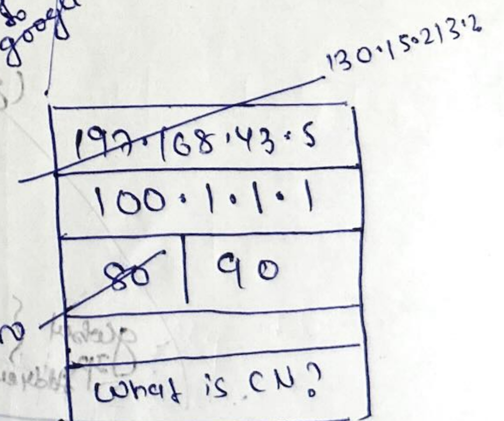
Now NAT

NAT table

	Src Ip	Src port	U. port	D Ip	D port
1st N/w	192.168.43.4	80	213	100.1.1.1	90
2nd N/w	192.168.43.5	80	300	100.1.1.1	90

Match with NAT





DHCP -

(Dynamic Host configuration protocol)

DHCP is a ~~protocol~~ N/w Managment protocol used to dynamically assign an Ip address to many devices/ nodes on a network so they can communicate using Ip

Network Admistrator
↳ Manually Assign Address to Individual Host (as users is few) ⟹

DHCP
↳ Automatically assign as user is more so, to configure it faster

① It is App layer program uses client-Server paradigm

② plug & play protocol.

DHCP is of dual Nature

MAC	IP
M_1	I_1
M_2	I_2

static

MAC	IP	Lease time
M_3	I_5	10 min
M_4	I_6	15 min
M_5	I_7	7 min

dynamic

Pool of Ip Address

* ① when you plug your comp to a New LAN then comp take some time to configure what is the Ip Address in this N/w so, DHCP Help.

opcode	Htype	HLen	H Count
Transaction ID			
Time elapsed		Flags	
Client Ip Address			
Your Ip Address			
Server Ip Address			
Gateway Ip Address			
Client Hardware address			
Server Name			
Boot File Name			
Option.			

opcode - req (1) | reply (2)

Htype - Ethernet,

HLen - Length of Hardware Address.

Hcount - maxm no. of Hops the pkt can travel

Transaction - ID → To match req. with reply

Time elapsed → when comp. start it does'nt get Ip Address Immediately.

Flags :- 0 - Unicast
1 - Multicast

Clint Ip Address - set to '0' if the client does not known yet

Your Ip Address - The client Ip Addr. sent by the server

Server Ip Add - Brodcast Ip Address if client does not know it

Gateway Ip Add - The address of default router

Server Name / ~~A 64 byte~~

Boot file Name → When client doen't know how to boot the comp.

Options format.

1. DHCP DISCOVER

→ when client join a N/w It send It and tell I am a client and looking for Ip Address

2. DHCP OFFER

→ One or more then one ~~server~~ DHCP server offer

3. DHCP REQUEST

→ client select any one and send the DHCP req.

4. DHCP DECLINE

→ Or It can also decline that offer

5. DHCP Ack

– finaly getting offer it return Ack

6. DHCP NACK

→ If it not get any more Ip Address

7. DHCP RELEASE

→ Done with work it realease that Ip Addr

8. DHCP INFORM.

→ ~~After Time Ran out~~ ~~it inform~~.

53	1	-
Tag	Length	Value

Process

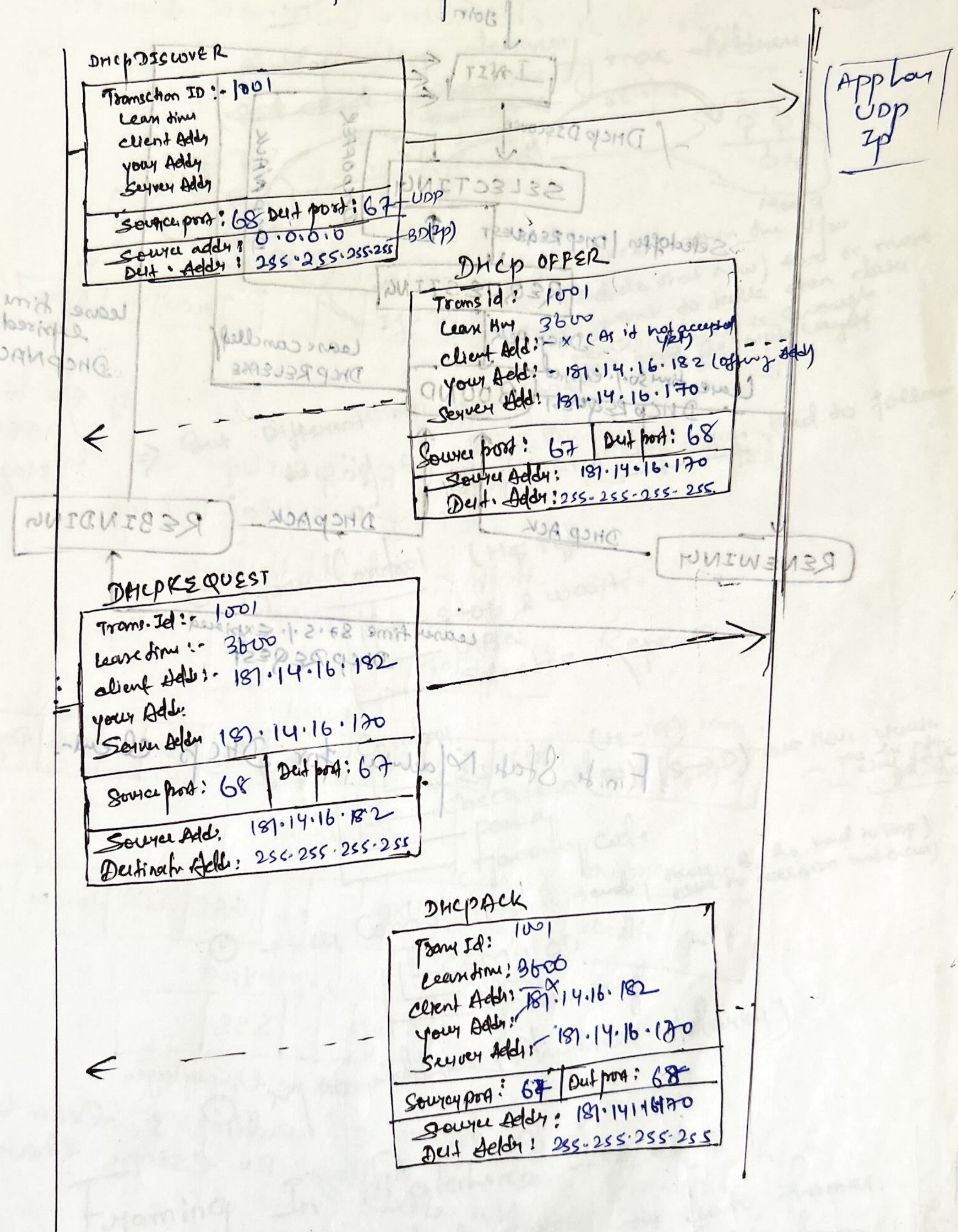
① Client / N/w requst connect to an Internet

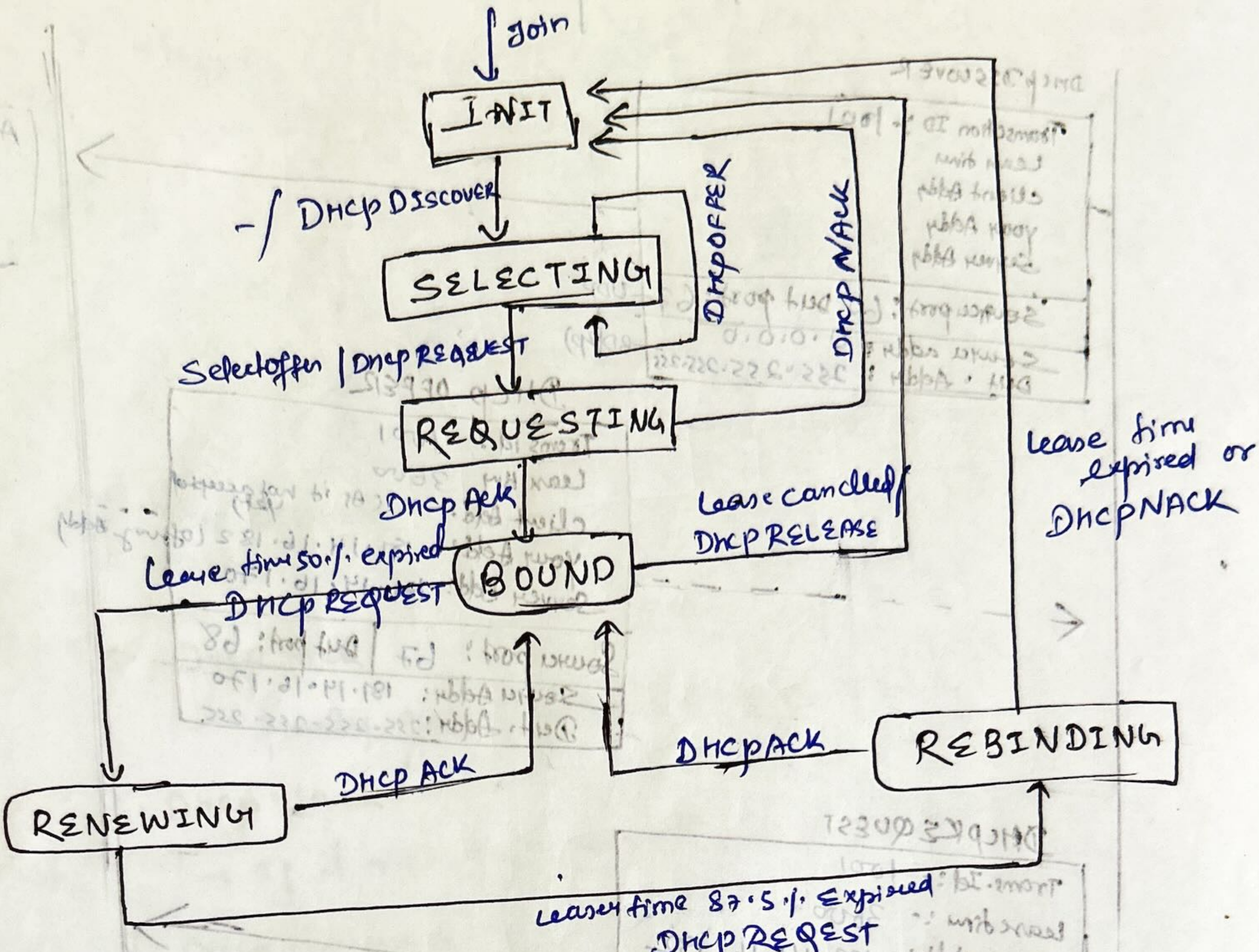
② DHCP client req. an Ip Address. Typically, Client brodcast a query for this Information

③ DHCP server respond to the client request by providing Ip server address & other configuration Information also Include time period called a lease time for which allocation is valid.

④ After the lease time at 50 % time left or 100 % time done a new req of a new ip is assigned again from pool.

client DHCP Operation Server.



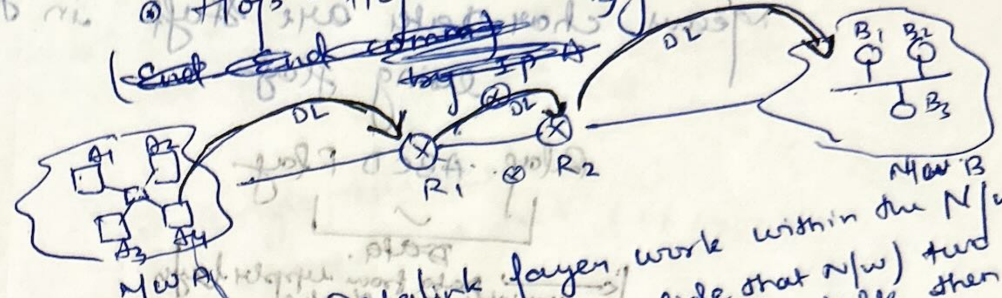


Finite State Machine for DHCP client.

DATALINK LAYER

• Hop-Hop delivery by mac Address

(~~End End ...~~)



• Datalink layer work within the N/w

If. In 1 LAN (Inside that N/w) two or more person want to talk then data link layer is enough. not need of N/w layer.

⇒ But Different N/w are there
to, if A4 $\xrightarrow{pkt}$ B1, then, first Hop-Hop had to follow.

• Flow Control (Hop Hop)
- Stop & wait
- GBN
- Selective Repeat

• Error Control (DL) (H-H)
- CRC (DL)
- Checksum (TL) (S → D) but there router me bhi pta chal jaye error
- parity
- Hamming code

• Access Control (B1 is sending then B2 B3 had to stop) due to collision not occur)
- CSMA/CD
- Aloha
- Token ring

• MAC Address (Physical Address)

Framing In Datalink Layer.

Datalink layer needs to break bit into frames. So, that each frame is distinguishable from another.

Frame in a character - Oriented protocol.

Mean char data are stuff in this by using flag

Flag ABCD Flag

Data.

Data from upper layer
variable no. of char.

Flag	Header				...			Trailer	Flag

~~Frame~~ → Flag in Data

Flag AB Flag C Flag

→ Flag A Esc Flag C Flag

If Esc in data

ABESCF

→ Flag AB ESC ESC F Flag

Byte stuffing and Unstuffing

Data from upper Layer

Esc	Flag		Esc	Esc	

↓ stuffed

Frame sent

Flag	Header		Esc	Flag		Esc	Esc		Trailer	Flag

Extra 2 bytes

Frame received

Flag	Header		Esc	Flag			Esc	Esc	Trailer	Flag

↓ Unstuffed

	Flag			Esc	

Data to Upper layer

Byte stuffing is the process of adding 1 extra byte whenever there is a flag or escape character in the text.

01111110

LSO → stuffed

0001111111 0011111 01000

↓ stuffed

Frame sent

Flag	Header	000111110110011111 0 01000	Trailer	Flag

Extra 2 bit

Frame received

Flag	Header	00011111.01100 11111 00 1000	Trailer	Flag

↓ unstuffed

000111111100 011111 01000

4

Error detection & correction.

=) Sender is sending some data but receiver is not receiving the same one so, Error occurs

101 (5) → 100 (error) (4)

- Single-bit Error
  → change in 1 bit
- Burst Error
  → more than 1 bit change

101010 → 111011

Length of error ⇒ 5

Q. If a bandwidth of a channel is 1 Gbps then for how much duration the error should last?

→ $A \xrightarrow{1\text{Gbps}} B$ $\quad 10^9$ bit - 1 sec

1 bit - $1/10^9$ sec = 1ns

Detection Method

↳ Simple parity
2D parity check
Checksum
CRC
Hamming code

} Based Redundancy.

Single parity.

↳ (Least Expensive method)

m+1 bit
↳ message bit

=) Even parity - (No of '1' even)

ex:- 1010 0
1110 1

=) It can detect all single bit error in code word.

ex:- $\boxed{11101}$ → 01101

(no of '1' bit is even so parity bit must be '0' but here '1' is there)

means, there is Error

=) Can detect all odd no. of error also

ex:- 11101 → 00001

(no of '1' = 0 so parity must be '0' but 1 is there)

So error

Hamming dist ?

for, 4 bit data word

	Parity
0000	0
0001	1
0010	1
⋮	⋮
1111	0

Valid code word — for even

Hamming dist ⇒ Take any two valid code word and perform XOR operation
same → 0 , diff → 1

ex:- 0000
1111
———
1111 — 4 is HD
Any two valid

ex:- 0101
1000
———
1101 — 3 is HD

Min^m H.D = 2 = d

00000
00011
———
00011 — 2

d − 1 — It can detect
= 1

If we change 2 bit ex:- 00000 ⇒ 11000 (Already in table)

If we change only 1 bit → 00000 ⇒ 10000 (No one matches with this in table)

CRC (cyclic Redundancy check)

↳ Based on binary division

total bit = (m + r) — no. of redundant bit

ex:- $x^4 + x^3 + 1$ — Divisor.
polynomial
Highest degree is 4

4 no. is append.

$1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x^1 + 1 \cdot x^0$

⇒ 1 1 0 0 1

↳ If already given in binary so (n−1)

```
11001 ) 1010101010 0000
        11001
        011000
         11001
        000011010
            11001
          00011000
             11001
             000010
```

append ⇒ 10101010100010

when reciever got this

```
11001 ) 10101010100010
        11001
        011000
         11001
        000011010
            11001
          00011001
             11001
             00000
```

Means no error occur

- can detect all odd error, single bit, burst error of length equal to polynomial degree
- polynomial should not be divisible with x
- also not with $(x+1)$

Hamming Code for Error detection & Correction.

7 bit — 4 bit Data
— 3 bit parity

Position	7	6	5	4	3	2	1
Bit	d_3	d_2	d_1	P_2	d_0	P_1	P_0

$2^n \rightarrow P$ -

$P_2 = d_3 \oplus d_2 \oplus d_1$

$P_1 = d_3 \oplus d_2 \oplus d_0$

$P_0 = d_3 \oplus d_1 \oplus d_0$

ex:- $d_3 d_2 d_1 d_0$
1 0 1 0

$P_0 \rightarrow 0 \oplus 1 \oplus 1$
$1 \oplus 1 = 0$

P_1 :- $0 \oplus 0 1$
$0 \oplus 1 = 1$

P_2 :- $1 \oplus 0 \oplus 1$
$1 \oplus 1 = 0$

1	0	1	0	0	1	0

Q

D_7	D_6	D_5	P_4	D_3	P_2	P_1

$P_1 \rightarrow D_3 \; D_5 \; D_7$

$P_2 \rightarrow D_3 \; D_6 \; D_7$

$P_4 \rightarrow D_5 \; D_6 \; D_7$

Even parity

ex:- 1011

1	0	1	P_4	1	P_2	P_1

$P_1 \rightarrow 1 1 1 \underline{1}$

$P_2 \rightarrow 1 0 1 \underline{0}$

$P_4 \rightarrow 1 0 1 \underline{0}$

→ 1 0 1 0 1 0 1 ✓

Now to check the errors

$D_7 \; D_6 \; D_5 \; P_4 \; D_3 \; P_2 \; P_1$
1 1 1 0 1 0 1

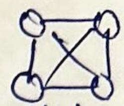
$P_1 \rightarrow$ 1 | 1 1 1 (D_3 D_5 D_7) even

$P_2 \rightarrow$ 0 | 1 1 1 (D_3 D_6 D_7) odd :- error

$P_4 \rightarrow$ 0 | 0 1 1 (D_5 D_6 D_7) even

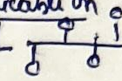
MAC (Multiple Access protocol)

Not applicable on



Mesh topology bcz they are not sharing a single link

applicable on



- Random Access protocol
  - Aloha *
  - CSMA
  - CSMA/CD (Collision Detection) *
  - CSMA/CA (Collision Avoidance)
- Control Access
  - polling
  - Token passing
- Channelization
  - FDMA
  - TDMA

Random Access protocol :- A, B, C (all station have same superiority that is no station has more priority than another station. (Any station) can send data depending on medium state (idel or busy) & no fixed time of sending data.

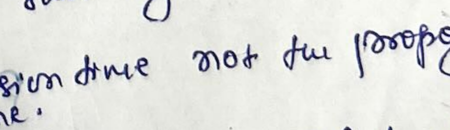
- There is no sequence of sending

Control Access :- Only one station send at a time. It grant permission to only one node at a time to transmit the data.

Channelization protocol :- Freq Band and time is divided into channel and one by one channel is given to transmit ..

PURE Aloha

- It is a Random Access protocol due to which collision may occur
- It has Ack ex:- $A \xrightarrow{d} C$, $C \xrightarrow{A} A$ if Ack not recieved to A mean's collision occur then it wait to 2 MSL then again send data.
- It is LAN based protocol.
- ∴ We Consider only Transmission time not the propogation time.
- Vulnerable time is a length of time in which there is a possibility of collision. (2 × Trans time)



$T_t = \frac{M}{Bw} = \frac{1000}{100} = 10$ m/sec

collision occur