C.N

Subnetting in classful Add.

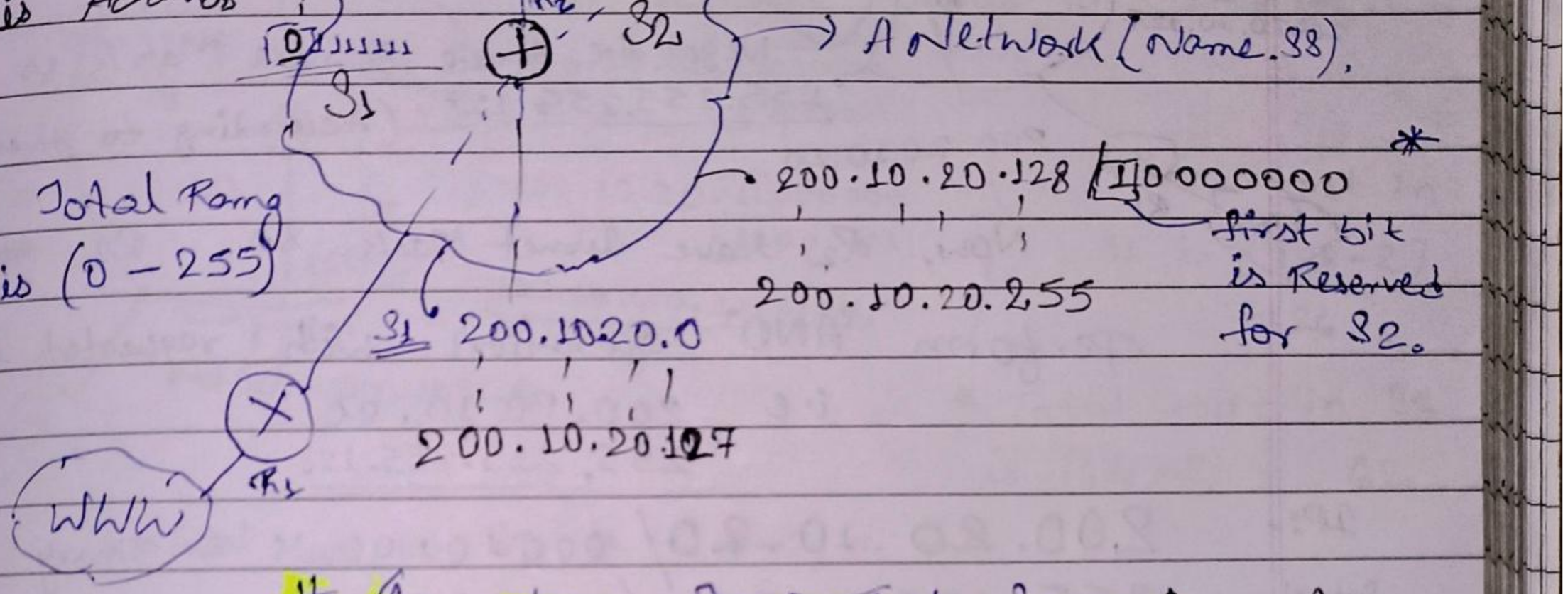
PAGE NO.: 79 RBP
DATE: / /

* **Subnetting** :- Dividing the big network into small networks.

Let :- 200.10.20.0 is Address

first '0' is Reserve for (S_1)

Need Subnet mask to send data in (S_1) or (S_2)

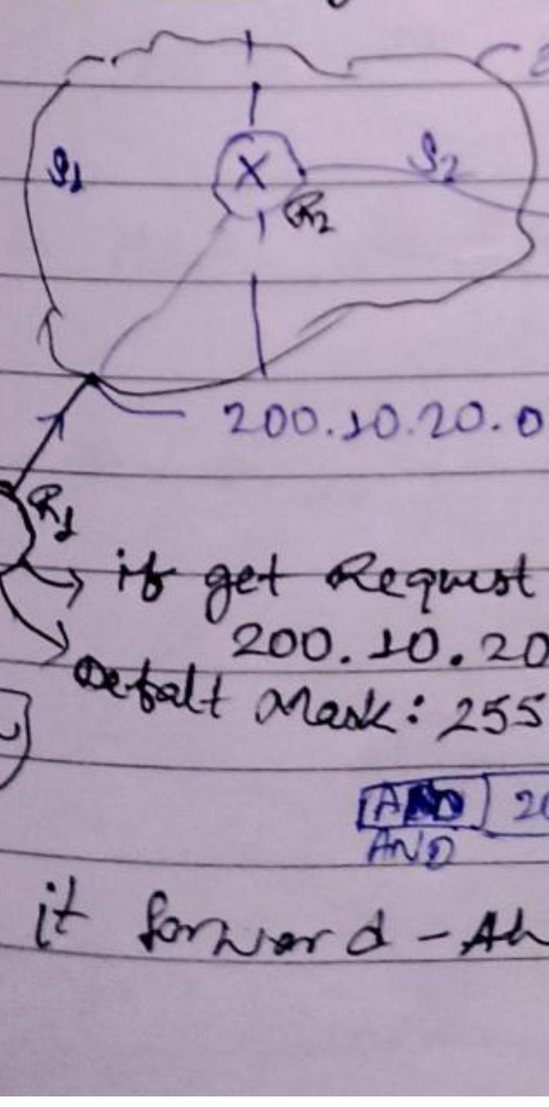


a, Total Rang is (0 - 255)

b, # In above Scenario A Network of class C, is did dividing in two part So, we have total Range (0-255) (0 to 255)/2. S_1 = 0 - 127, S_2 = 128 - 255 it by using Subnetting concept.

* We can perform

* **How to get Subnet mask** :- (1) we know class C have Default Mask :- 255.255.255.; in Last 8bit we have to put ('1') for No. of reserved bit. So, In above we reserved first bit '0' or '1' for ('S1' or 'S2')



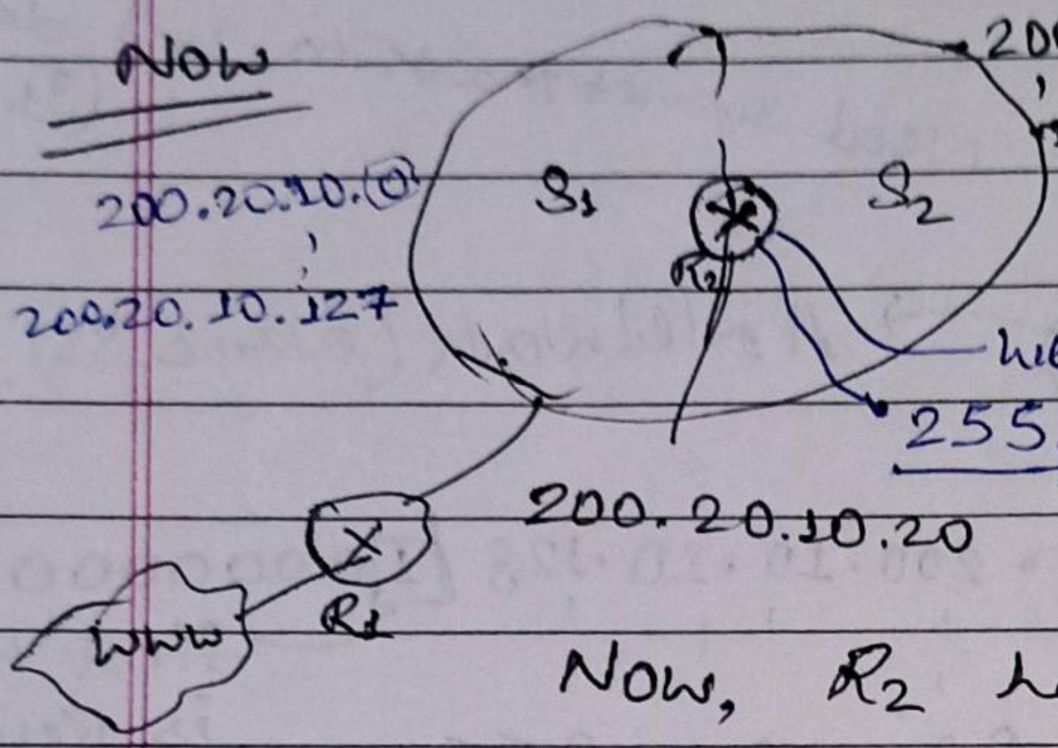
Now

255.255.255.10000000

255.255.255.128 ; it will assign to (R_2)

PAGE NO.:
DATE: 06/01/

Ex Lets take a Example :- A Request with 200.20.10.20 - IP address



we got the Subnet Mask is ⇒ 255.255.255.128 (According to given Q)

Now, R_2 have Subnet Mask 80, R2 will perform 'AND' operation with requested IP.

i.e 200.20.10.20

255.255.255.128

IP:- 200.20.10.20/ 00010100 : In Binary

Subnet Mask 255.255.255.128/ 10000000

'AND' 00000000

So Data will be forwarded to the (S1) Because 200.20.10.0 is (S1's) Network ID.

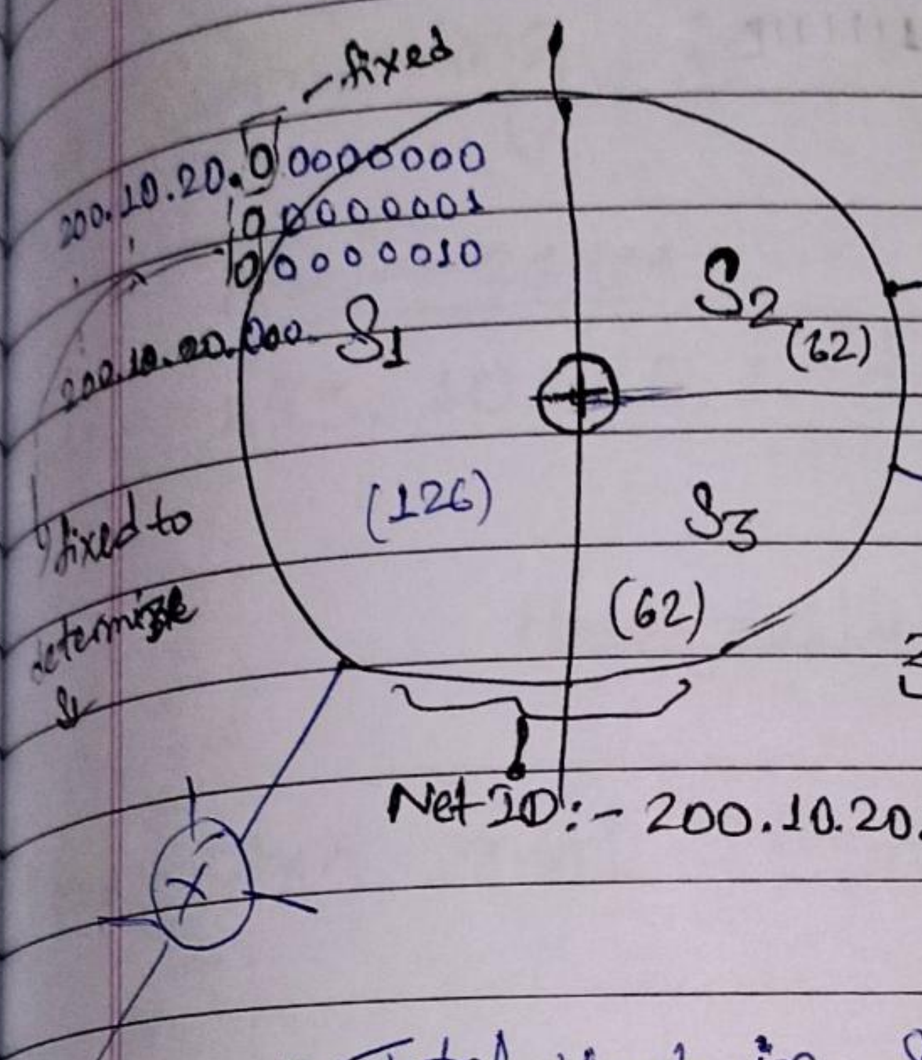
IP address = Network ID + Host ID

Variable length Subnet Masking (VLSM)

PAGE NO.: 80
DATE: / /

▷ It allows to divide a Network according to your choice / use, It mean n can be variey.

▷ All Subnet mask can have varying size



: A Network Divide in 3-part

26bit fixed

200.10.20.10000000
1 0000001

200.10.20.11000000
:11000001
:
200.10.20.11111111

* Total Host in S1 is (128-2) = 126

* Total Host in S2 is (64-2) = 62

* Total Host in S3 is (64-2) = 62

▷ Subnet Mask :- (*) It depends on No. of bits Reserved for any Network in 'S1', (*) And defined class (A-C)

S1 is class-C, ⇩ Default Mask.

255.255.255.11000000, :- (*) Reserved bits will be '1'

S2:- 255.255.255.11000000

S3:- 255.255.255.11000000

▷ Host identification/Network will decide the value of Subnet Mask 'AND' IP address =

Q:- IP:- 200.10.20.55 :- 255.255.255.00110111

S1

Classless Subnetting (CIDR)

PAGE NO.: 81
DATE: 06/08/22

* 195.10.20.128 /26 ↳ No. of Network bits
↳ Host ID = 32 bit − 26 = 6 bit

⇒ Subnetting in Classless Interdomain Routing (Subnetting In CIDR)

N/W ID bits :- 26 bit — Host ID

1st:- 195. 10. 20. 10|000000 : Binary

⇓

Host possible $2^6 = 64 = (64-2) = 62$ (Broadcast, Net ID)

Note:— Never change or manipulate Network bits.

Step 2nd:- Then most significant bit will be 'fixed' So ⇒ OF Host ID ⇒

Fixed ('0' or '1')

10,0|00000
000001
000010
|
195.10.20.10 0 11111

N/W 64 bit:

usable (30)	usable (30)
S_1 (32)	S_2 (32)

3) first ID of 'S1' is 195.10.20.128/27 to 195.10.20.159/27

* Because Now No of fixed bits is (27)

Eg:- 'S2' again the 'S2' most significant bit of Host ID will be fixed.

So, :- 195.10.20.10|1|00000
100001
000010
|
|
|

* Because we used '0' for (S1) No '1' are available now.

So,

Subnet 'S2' :- 195.10.20. 10|1|11111

⇓

195.10.20.160 − 191/27 (No. of fixed bits)

CIDR Numericals

DATE: 06/08/21

Q. classless interdomain (CIDR) receive a packet With address 131.23.151.76. The Router's routing table has following entities:-

•	Prefix	Output Interface
1.	131.16.0.0/12	3 ✗ Wrong explained below ⇨
2.	131.28.0.0/14	5
3.	131.19.0.0/16	2
4.	131.22.0.0/15	1 ✓

Q. Packket will be forwarded to which interface——

Sol'n * we have to Do 'AND' operation b/w 'interface' (/n) and given id (131.23.151.76) :-

1st :-131.23.151.76

/12 :- 11111111.1111D000.00000000.00000000 } AND Operation

131. ⇦ value

given :- 131.00010111.151.76

interface :- 255.11110000.0.0

AND ⇨ 131.16.0.0

* This is matched with option '1' So Answer is O/P Interface is '3'.

Try another ✗

2:- 131.23.151.76

~~14~~ :- 11111111.11111100.00000000.0

'AnN' :- 131.00010100.0.0

⇩

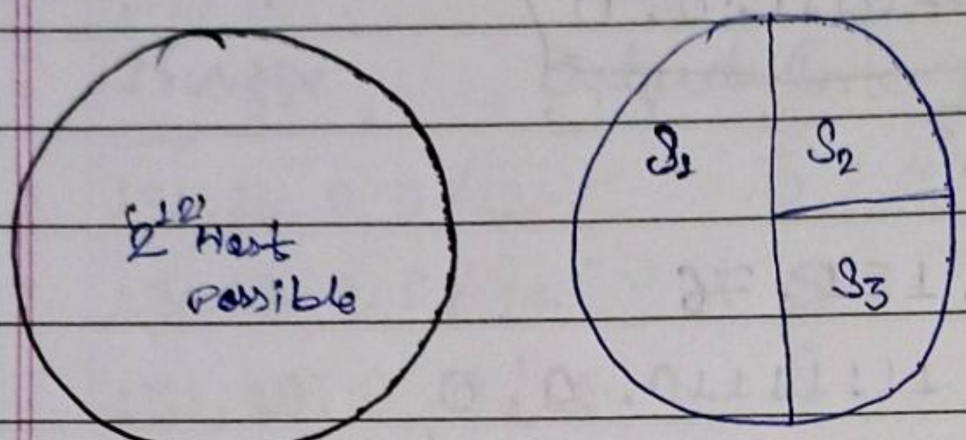
131.20.0.0 Not correct ✗

C.N
M=5

Variable Length Subnet Masking IN CIDR

PAGE NO.:
DATE: 06/08/22

- Variable Length Subnet Masking in classless = CIDR



245.248.128.0/20

* Network id :- 245.248.10000000.00000000 as /20 is given
* Host id :- 32 - 20 = 2^{12}

1st step To divide we have to fix most significant bit of Host bits (12).

S_1 245.248.1000 0000.00000000
8bit 8bit
fixed 000.00000001
0000.00000010
. . . . . .
245.248.1000 0111.11111111

⇨ Range of (S_1) = 245.248.128.0 (21) to 245.248.135.255 (21) direct Bc-

Note: \21 is subnet Mask of S_1.

Step:- S_2 = 245.248.1000 0000.0 (1) 000 0000
8 + 8 + 5 = 21
zero.

we taken '1' at 21st bit, because '0' is used for (S_1).
Next we have to divide S_2 in two part S_2 & S_3
So, again most significant bit of Host ID will be reserve.

C.N
M25

ARP - Address Resolution Protocol - Layer2

RFC 826

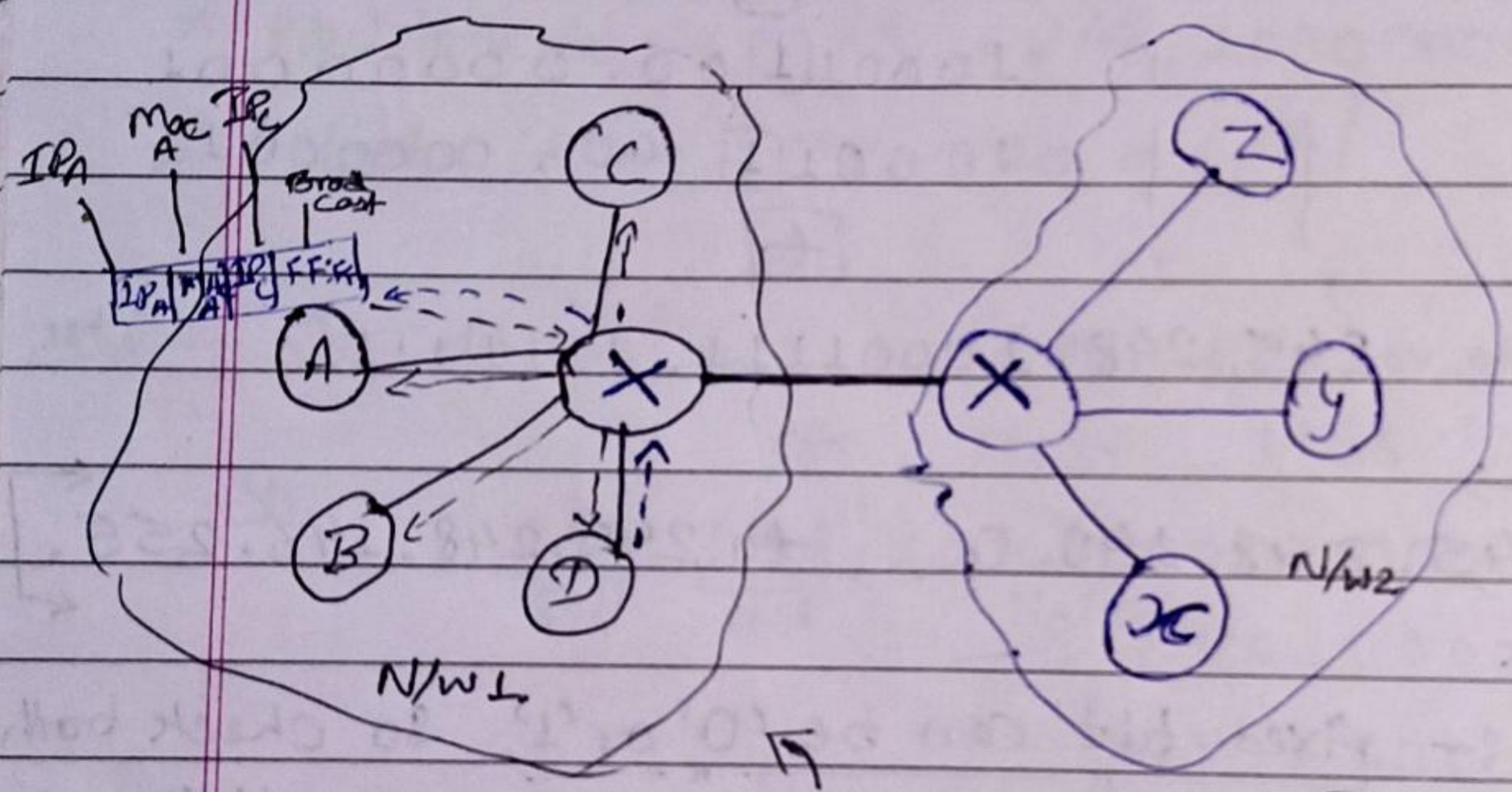
PAGE NO.:
DATE: 07/08/22

* IP ⟶ Mac * Logical ⟶ Physical.

⇒ ARP is a communication protocol used to find the MAC address of a device from its IP address. It used in LAN or ethnet network.

* Types OF ARP.
  - Proxy ARP
  - Gratiuitos ARP
  - Reverse ARP (RARP).
  - Inverse ARP.

NIC holds MAC Address.



* ARP Does always Broadcast

* A want to communicat with (D)

* Possible Communication in ARP
  1. Host to Host (H→H)
  2. Host to Router (H→R)
  3. Router to Host (R→H)
  4. Router to Router (R→R)

Note:- Broadcast: ARP Request and Unicast: ARP Reply/Response

* Communication Table :-

ARP Packet Format :-

Hardware type (Ethernet or ..)		Protocol type (IPv4 or v6)
Hardware Length (48 bit)	Protocol Length (4B)	Operation (Req. – 1)(Reply – 2)
Sender H/w Address (6 Bytes for Ethernet)		
Sender Protocol Add. 32 bit (4 B for IP)		
Target H/w Address (MAC)		
Target Protocol Address (IP)		

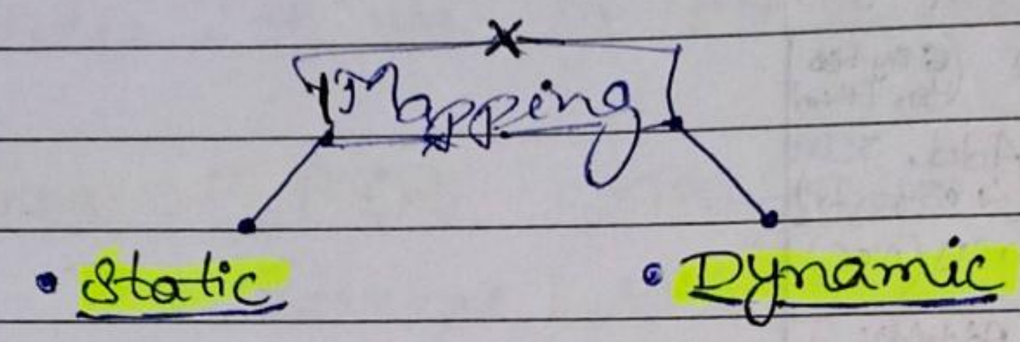
C.N
M-5

Address Mapping

ARP RARP IARP Proxy. GARP

PAGE NO.:
DATE: 07/ 02/22

* Address Mapping - internet is made of a combination of physical N/w Connected together by internetworking device such as routers.

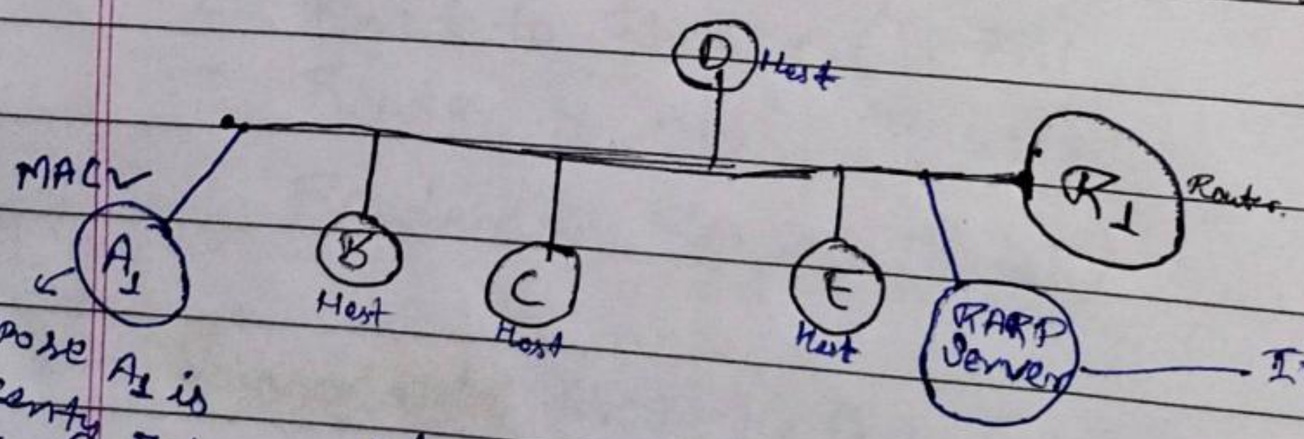


▷ In Static, it creates a table that contains a Logical address with a physical Address.

▷ Dynamic - When a machine knows one of two addresses (Logical or physical) through Dynamic ~~memory~~ mapping, it may use this protocol to find the other one address. Done by ARP or RARP.

▷ RARP (Reverse Address Resolution Protocol :-

• In RARP, it find IP address (of given MAC) just (MAC → IP) reverse Or ARP.



* RARP Request Packet ↓

MAC ID (A)	IP. ADD. 0.0.0.0

— To get IPID. ✓

RFC. 903

PAGE NO.: 85

DATE: 7/08/

* RARP Server :- (It contain all connected Node's IP with MAC) Static Table

MAC	IP
M_A	IP_1
M_B	IP_3
:	:
M_A	IP_A

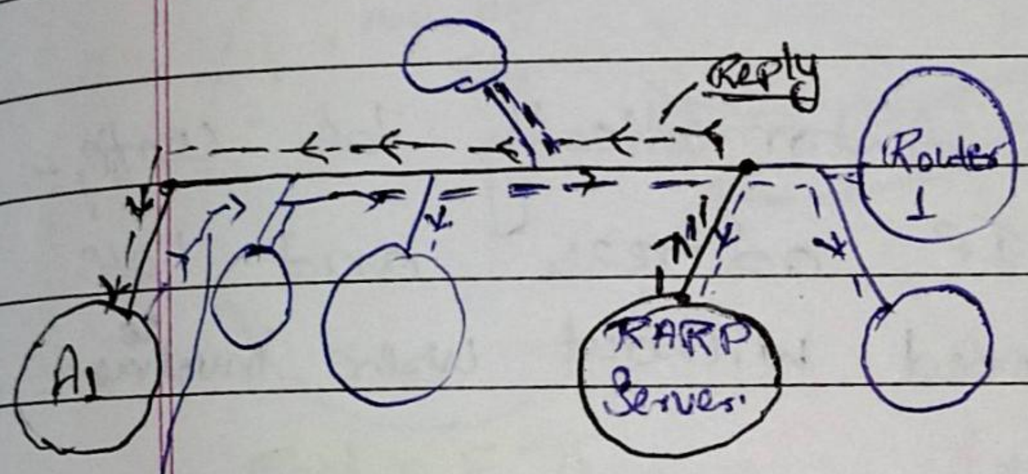
* How A_1 will request :-

Network N. Layer :- | MAC_{A_1} | IP: 0.0.0.0 |

DLL Data link : | MAC_{A_1} | 0.0.0.0 | M_{A_1} | FF:FF:FF:FF:FF:FF |

MAC ID For Broadcast.

Data link converts packet into frame, we know



* Request, Received by All connect Nodes.

* But, Responce (unicast) Done by RARP server.

→ RARP will reply with A_1's IP Address by using / helping of static Table.

RARP Not in use Nowadays because we have better option as BOOTs and DHCP

C.N
M-5

BOOTP

PAGE NO.:
DATE: 07/8/22

⇒ The Bootstrap protocol is a Networking protocol used to by a client to Optaining IP address from a server.

* It designed to Replace "RARP" protocol.

⇒ Now, Bootstrap is also going to be Replaced by DHCP, Its more flexible. (DHCP)

↳ It's Lets anetwork user Automatically be configured to receive an IP address and have an Operating System booted without user involvement.

* No disk Required. * It supports the use of motherbo

RFC 2131

DHCP

- Used for Broad N/W (Large No. of Host)
- ~~Internet used~~ Broadly used Nowadays

PAGE NO.: 86
DATE: 07/08/22

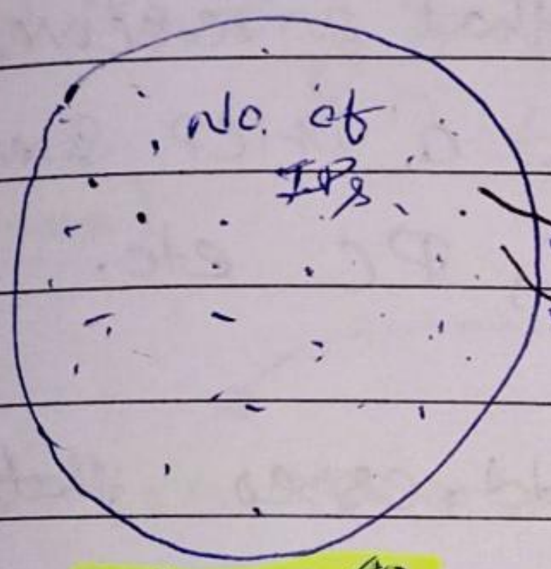
- Dynamic Host ~~Control~~ Configuration Protocol.

▷ It hold dual-Nature type table :- Half Static & Half Dynamic Table.

Static :-

MAC	ID
M_1	I_1
M_2	I_2

MAC	IP	Lease Time	
M3	I3	10min	Dynamic
M4	I4	12min	



* Here, DHCP contains Static and also Dynamic table, idea is behind Dynamic table It holds or assign IPs for particular (lease Time) and After that time Host should have to Request 'Renew' message to the DHCP for Stay connected. If DHCP don't get 'Renew' from Host side than it remove that Host from table & release IP for (pool of IPs) means that IP will move to (pool) & idle for configuration.

Components of DHCP :-
- DHCP Server
- DHCP client
- IPs pool
- Subnet
- Lease
- DHLP relay

C.N
Mod 5

DHCP

PAGE NO.:
DATE: / /

▷ **DHCP Server**: It is networked device running the DHCP service that holds IP addresses and related configuration information. This is typically a server of a router but could be anything that acts as a hosts, such as an SD-WAN appliance.

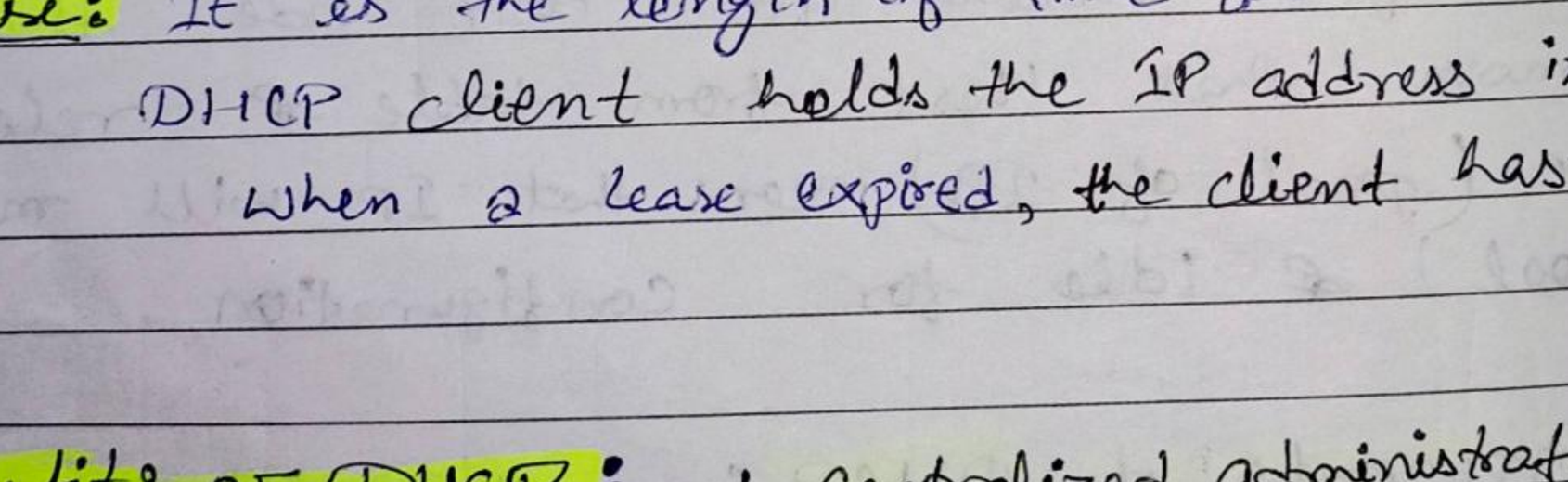
▷ **DHCP client**: It is endpoint that receives configuration info. from a DHCP server. It can be like laptop, IOT, PC etc.

▷ **IP Add. pool**: It is the range of addresses that are available to DHCP client

▷ **Subnet**: It is the partitioned segments of the IP networks. It is used to keep Networks Managed.

▷ **Lease**: It is the length of time for which a DHCP client holds the IP address info., When a lease expired, the client has to 'renew'.

* **Benefits OF DHCP**: 1. Centralized administration of IP configuration.
2. Dynamic Host config.
3. Seamless IP host config.
4. Flexibility and scalability.



Forwarding and Unicast, Routing protocols.

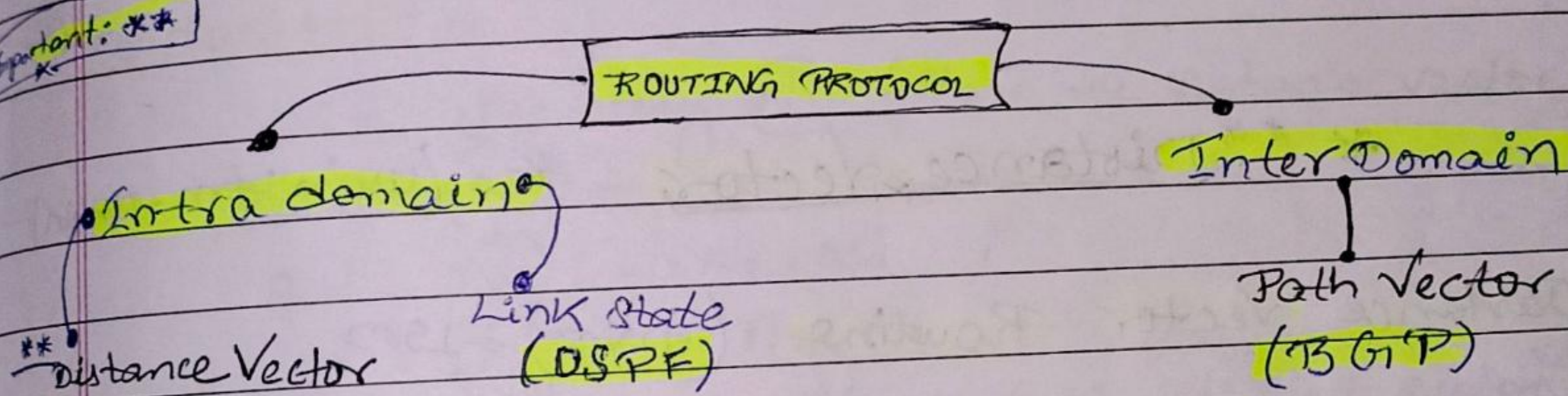
PAGE NO.: 87
DATE: 7/08/22

- Important Role of Network Layer is 'Forwarding' the packets.

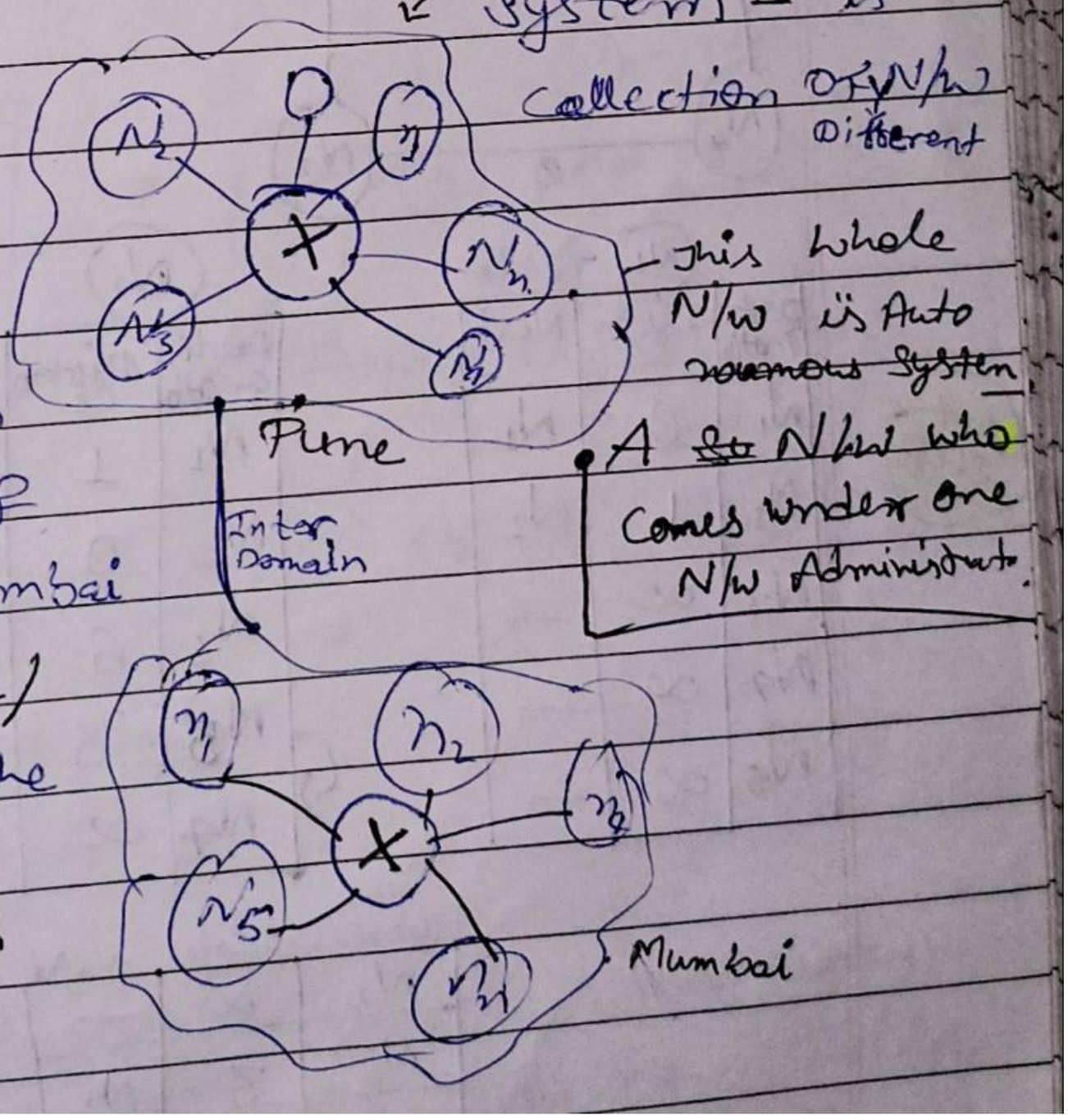
- To make Dynamic Table, it using Routing protocols.

↳ Routing protocol is set of rules for communication b/w Nodes And Router.

Important: **



Internally we divided the Internet in Autonomous System - is collection of N/w different



- Inter Domain Decides:- How to share/ communicate two Autonomous System as given on right side fig. Pune & Mumbai

* If we have to communicate/ shares the data within the Autonomous System is decides 'Intra-Domain'

DATE: 7.08.22

* Distance vector implements through (RIP) - Real Routing info. protocol is used to share Data/message within 'Intra-Domain'

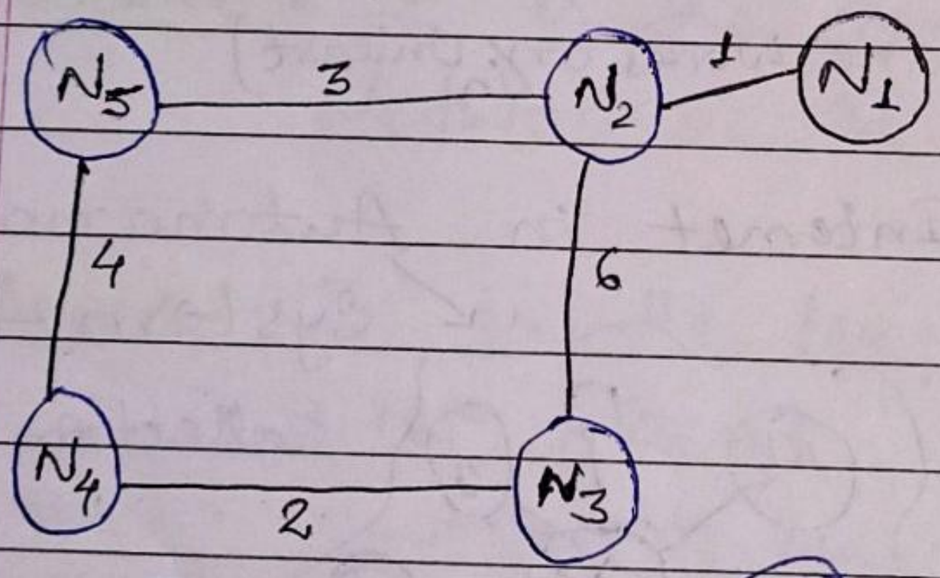
⇒ Open Shortest path first (OSPF) is work on 'Link state'.

⇒ Border Gateway protocol is work on 'Link state'

Note - RIP, OSPF, BGP are Used for 'Unicast' only

* **Distance Vector** * (Use in intra-domain)

* Distance Vector Routing (DVR) = 1980



1) We have to maintain Shortest Path Distance table b/w Nodes for share Data/Comm.

2) * Each & every Routers/Node knows the No. of Nodes are connected in that N/w

1st step

N1 Table

Destination	Distance	Next
N_1	0	N_1
N_2	1	N_2
N_3	∞	—
N_4	∞	—
N_5	∞	—

N2

Destination	Distance	Next
N_1	1	N_1
N_2	0	N_2
N_3	6	N_3
N_5	3	N_5
N_4	∞	—

N3

Destination	Distance	Next
N_1	∞	—
N_2	6	N_2
N_3	0	N_3
N_4	2	N_4
N_5	∞	—

N4

Destination	Distance	Next
N_1	∞	—
N_2	∞	—
N_4	0	N_4
N_5	4	N_5

Dest.	Dista	Next
N_1	∞	—
N_2	3	N_2
N_3	∞	—
N_4	4	N_4
N_5	0	N_5

First iteration is Completed

* only neighbor * only distance vector

* Actually each Nodes at Starting point only known their neighbour Nodes & their Distance.

* Each nodes will share their 'Dist' column/ array to only neighbor, After completed 1st step.

eg:- $N_1 \longrightarrow N_2$: N_1 Share Distance sheet with N_2 only.

• Same as $N_2 \rightarrow N_1, N_5, N_3$ because These all are their neighbor.

Conclusion :-

at N_1 only N_2 (Share the Distance vector)
at N_2 ---> N_1, N_5, N_3 (")
at N_3 ---> N_2, N_4 (")
at N_4 ---> N_3, N_5
at N_5 ---> N_4, N_2 (Share, N_5 get Distance vector of N_4, N_2 table)

How to Update Values/Data :-

for (N_1) :-

1	1
2	0
N_2 3	6
N_4	∞
5	3

New (N_1) table

Dest.	Dista	Next
N_1	0	N_1
N_2	1	N_2
N_3	7	N_2 N_3
N_4	∞	—
N_5	4	N_2, N_5

○ - neighbor

* N_1 to N_2 and $N_2 \rightarrow N_1$
$= 1 + 0 = 1$

* N_1 to N_2 and N_2 to N_3
$= 1 + 6 = 7$

* $N_1 \rightarrow N_2$ and $N_2 \rightarrow N_4$
$= 1 + \infty = \infty$

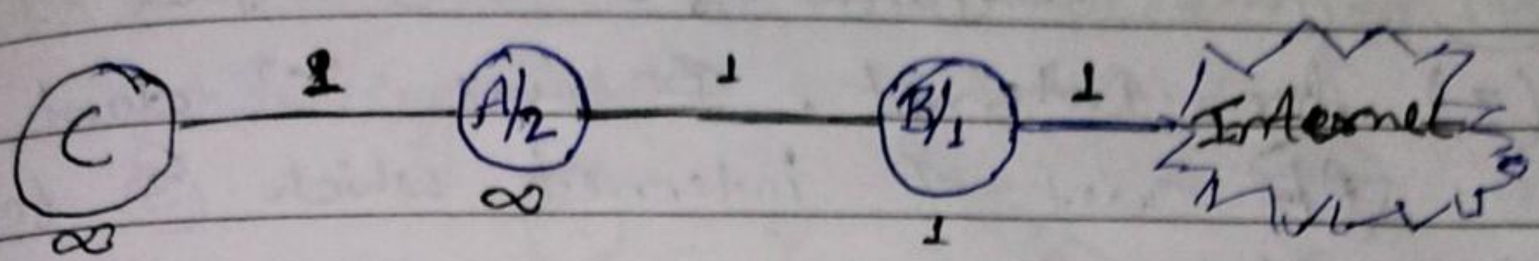
* $N_1 \rightarrow N_2$ and $N_2 \rightarrow N_5$
$= 1 + 3 = 4$

- In first 'Hello' Broadcast message is maintained the all connected Nodes's Routing Table with/in Shorest Distance path. It work parallely

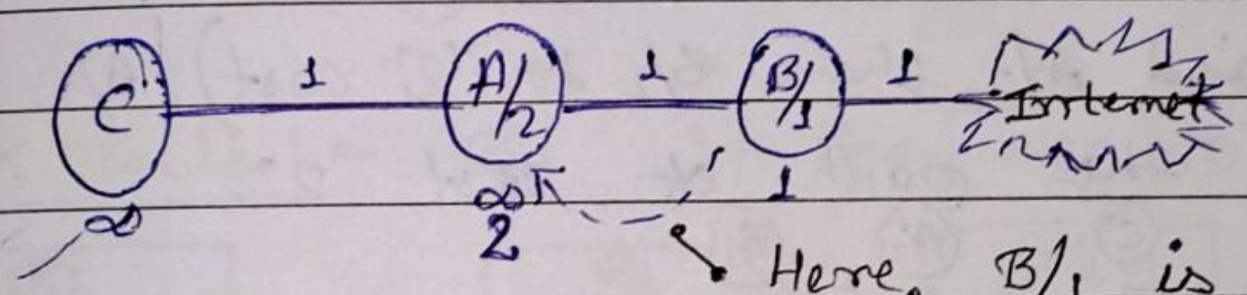
Count to Infinity Problem

PAGE NO.: 83
DATE: / /

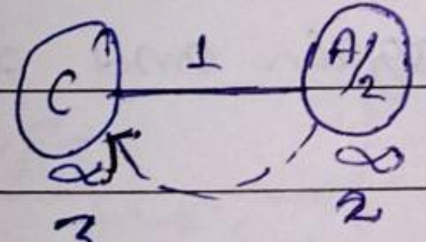
eg:-



- B/1 : is connected to A/2, and Internet (Both are neighbor.)
  So, B/1 can connect with internet at 1 cost.
- Same A/2 : is connected to 'B/1' and 'C' (Both are neighbor) '1' cost.
  But, A/2 don't know where is internet initially
  ↳ C is also don't know where is 'internet'.



B/1 shares the cost of 'Internet' i.e 1 + 1 = 2



:- Now A/2 same works as a neighbor of 'C' & share the cost of Internet
= 2 + 1 = 3

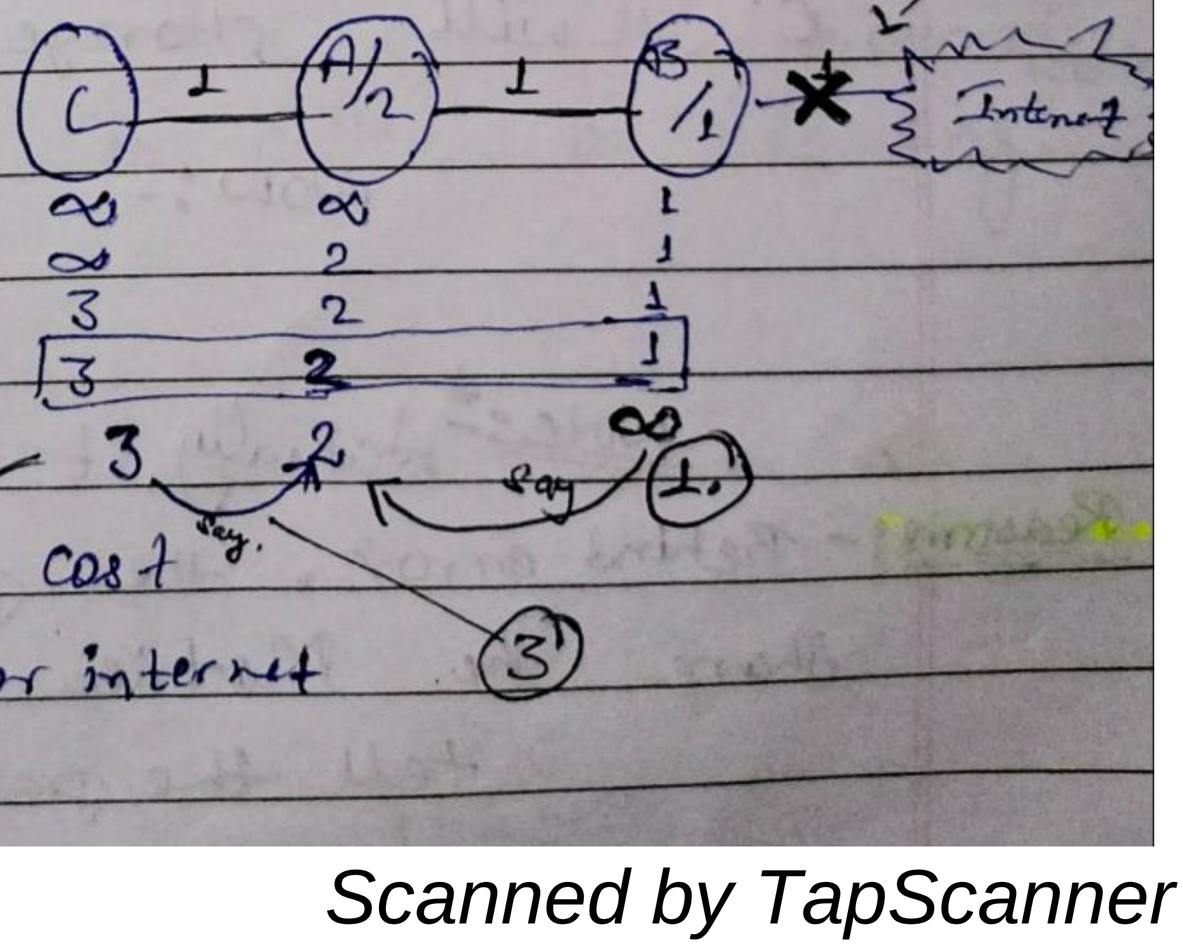
* Final Normal case:-

	C	A/2	B/1
	∞	∞ ←	1
	∞ ←	2	1
	3	2 ←	1
Final	3	2	1

* Special case/worst :-

- Due to some Reason connection of Internet break.

Now,

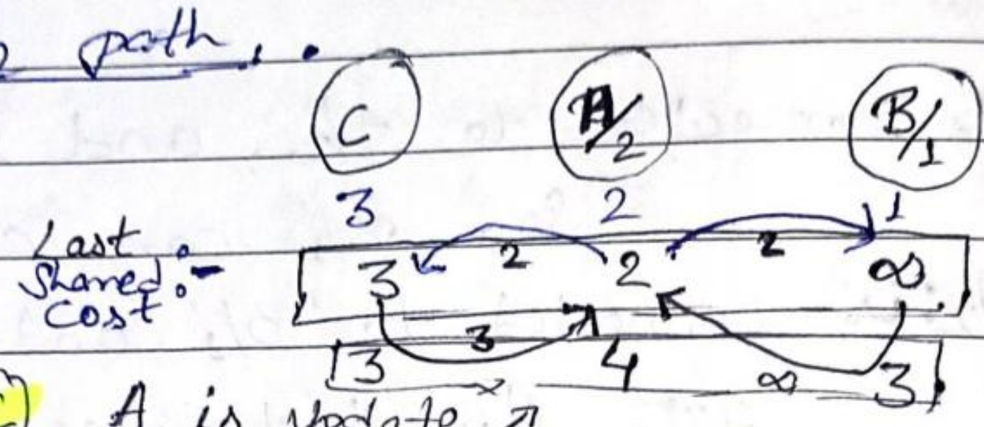


* 'B/1' know that path is break (using 'Hello' msg) So, it change the cost (1) to (∞)
(1) Now, B shared updated cost that am Unable /(∞) cost for internet to the (A/2).

Infinit Problem in DVR

PAGE NO.:
DATE: 07/08/22

(3) But (A/2) get response from 'C' that I have path cost (3) for Internet. Because 'C' dont know that (A/2) cost of internet which (3) for (C) is via A/2 path.

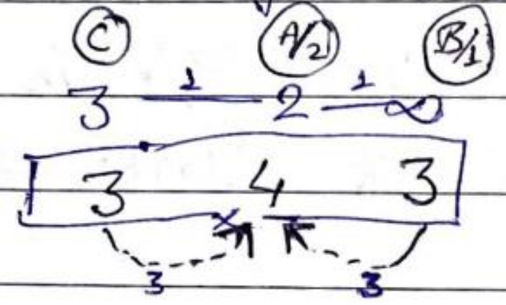


* According to (C) A is update ↗

⇒ Parallely At a same ~~the~~ time (When (B/1) share to A/2 'ω' cost and A/2 share B/2 for '2' cost) A/2 again don't know the path of cost '2'.

So,

Now

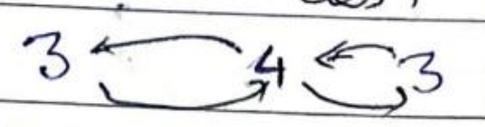


Same ~~thing~~ process happening again and again

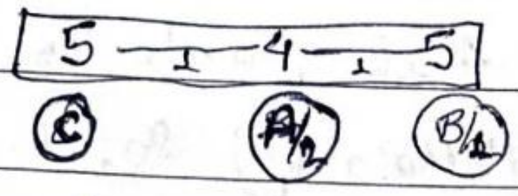
So, ~~Int next~~

* (A/2) get respose for cost from (B/2) and (C) (3) & (3) respectively. But 'A/2' to 'C' or 'B/2' is '1' (given) So it already '4' (A/2 will ~~not~~ Changed

Then Same time A/2 is shared their cost i.e 4 to both neighbor then B/2 and C will change the cost again.



Now :-



Note :- * Actually it going to be infinity (∞).

Reasons :- Behind error, the problem is they A, B, C only share the Matrics value of cost, (they don't tell the path (via) to each-other. So it occured.

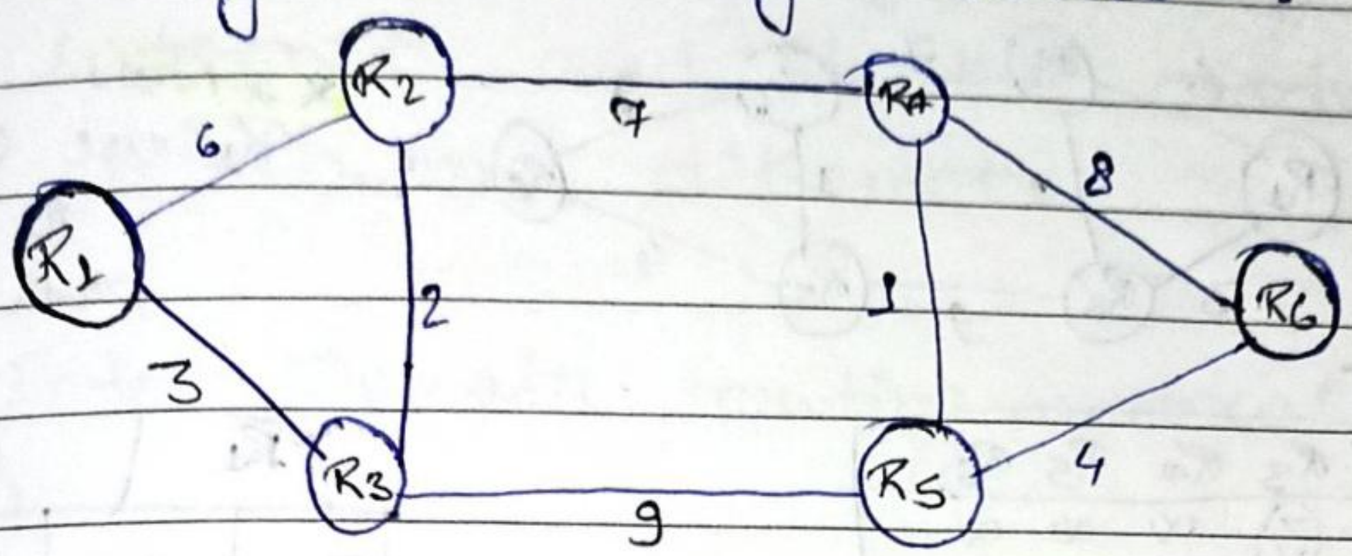
Link State

Dijkstra Algo used

ROUTING

PAGE NO.: 30
DATE: 07/08/22

⇒ DVR, Link State etc are used to make/made Routing table by 'Router'.



⇒ Initially All connected Routers (of N/W) is make a Link State Table.

Step 1

* Link Table :- By sending "Hello" Msg to ~~Ever~~ All. It maintain neighbor/distance.

R1	
R2	6
R3	3

R1	
Seq. No. TTL etc	
R2	6
R3	3

R2	
R1	6
R3	2
R4	7

All are Link Table

R3	
Info.	
R1	3
R5	9
R2	2

R5	
R3	9
R4	1
R6	4

R6	
info.	
R4	8
R5	4

R4	
Info	
R2	7
R5	1
R6	8

This is available in all Table ($R_1 - R_n$)

Step 2

* Flooding :- Each router sends the information to every other router on this internet work except its neighbors. is called as flooding.

Border Gateway Protocol (BGP)

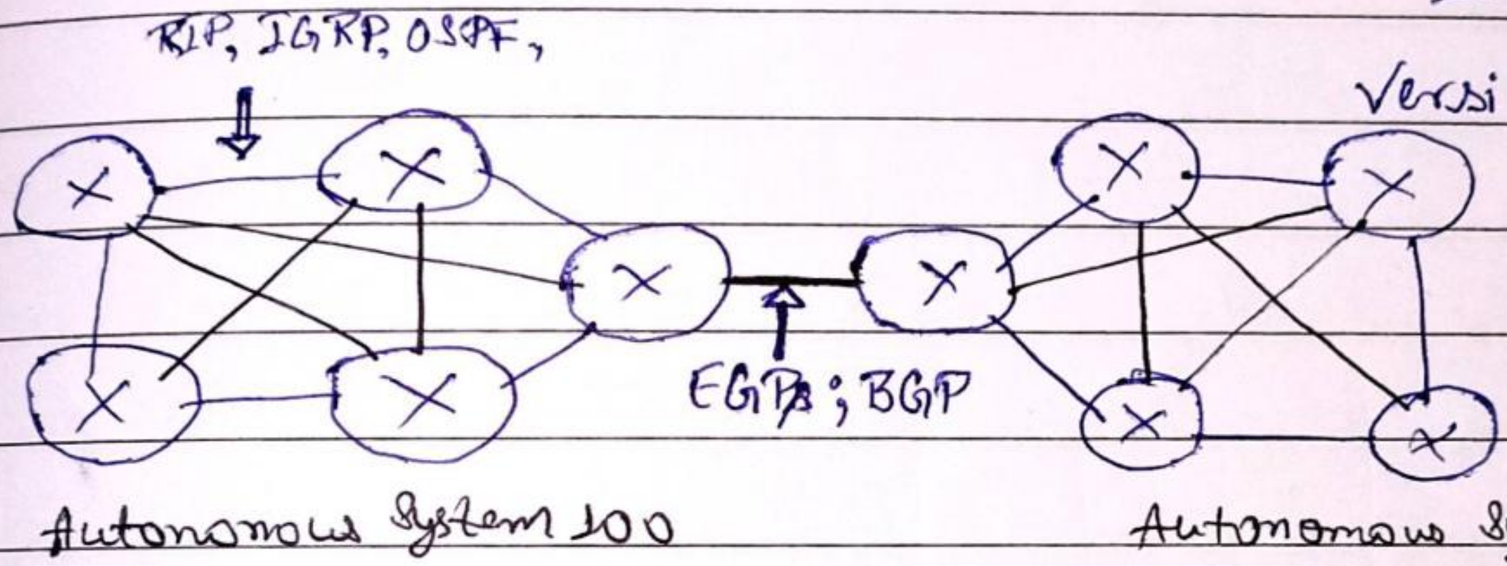
PAGE NO.: 31
DATE: 7 / 08 / 22

- BGP is used to Exchange routing information for the internet and is the protocol used b/w ISP which are different.

* Inter-Domain routing protocol.

* First Network was ARPANET.

* BGP version 4:- It is used current version of BGP (RFC 1771)



Features *:-

- Open Standard
- Exterior Gateway Protocol
- Inter AS-Domain routing
- Supports internet
- classless
- path Vector

* BGP Packet Format *

MARKER (32)		
LENGTH (16)	TYPE (8)	

1). Marker is a 32-bit field which is used for the Authentication purpose
2). It is 16 bit field defines the total Length of the message, including Header
3). Type, is an 8-bit for type of Packet.

* Types of Autonomous System (AS):-

1. Stub AS
2. Multihomed
3. Transient
4.

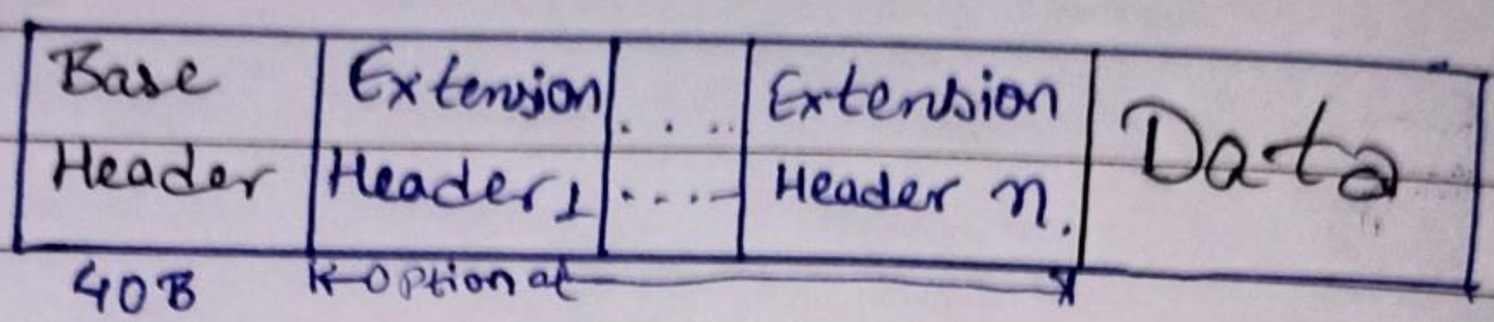
M
CN=5

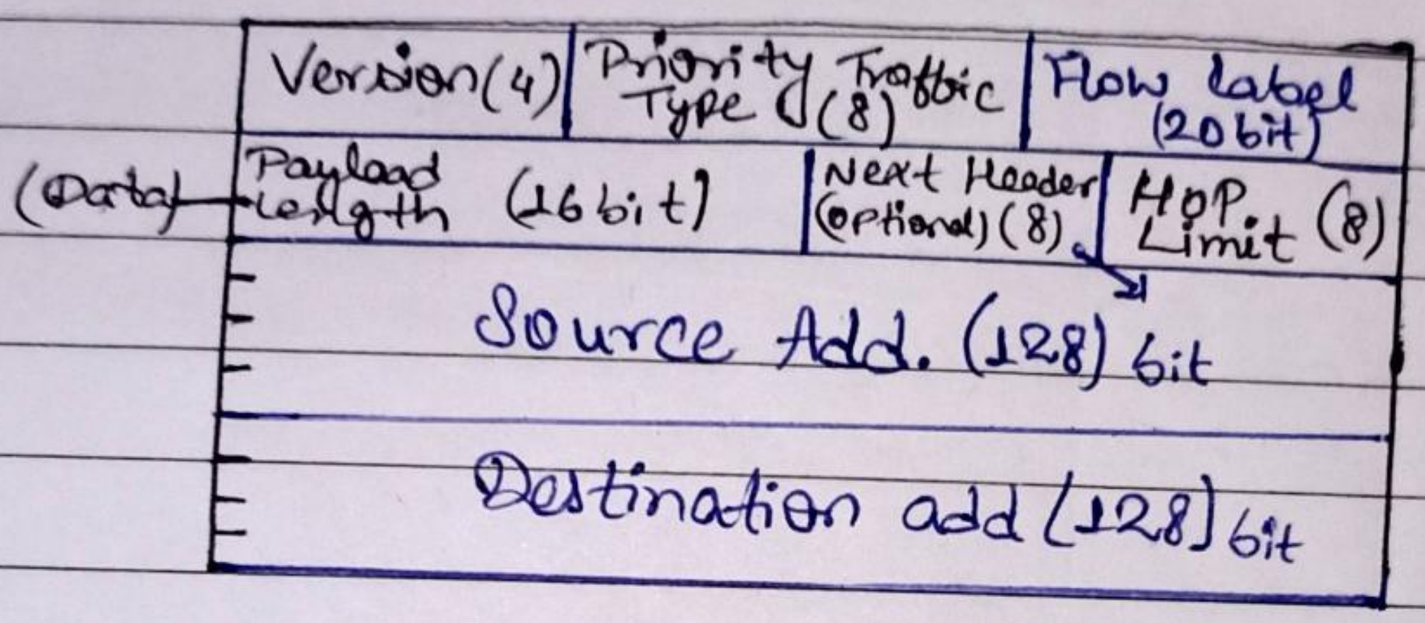
IPv6 (128) HEADER

Data from Service

PAGE NO.:
DATE: 13/0

* No. of IPs Possible :- 2^{128} =
  * Hexadecimal * (:)





Base Header :- 40Bytes (320bits)

Extension headers :-

	Values
1. Routing H.	(43) decimal
2. Hop by Hop	(0) "
3. Fragment H.	(44) "
4. Authentication H.	(51) "
5. Destination H.	(60) "
6. Encapsulating security	(50) "
7.	

- **Version** – It define Version of i.e IPv6 = (0110)
- **Priority** – It eliminate congestion give priority to any
- **Flow-level** – It use for Real-time, by a source label the packets belongs to the same flow in order to request special handling by intermediate IPv6 routers

- payload length/Data — It contains Data (size can be 65536) (0-65535)B.
  - ** But additional Feature are there as "Jumbo Grams" it allows (upto 4GB), it used with extension Header.
- Next header — It contain extension header for additional info/ Features.
- Hop limit/TTL :- This field indicates the max. No. (0- then packet will be drop.) of intermediates nodes IPV6 packet allowed to travel. It decresing at every nodes (last 0).
- Source Address :- Address OF Sender Host.
- Destination Header (Add.) :- It contain Address of Receiver Node.

Priority	Meaning
0	No Specific Traffic
1	Background Data
2	Unattended Data traffic
3	Reserved
4	Attended Data Traffic
5	Reserved
6	Interactive Traffic
7	control traffic.

Header Decription :-

1). Routing H. :- Predefined (user) path to Acheive Destin.

2). HopbyHop :- To provide all Hop (IN following Path) Some inform.

3). Fragment H. :- Dividing the packets/Data, only it done by (Source).

4). Authentication :- It work as (checksum), To keep integrity, ~~security~~ of Data.

5). Destination H :- It used for that only "Destination can read this Extension Header (Destinat.).