Mod 3. The Network Layer.

→ The network layer is the third layer in the OSI model.

→ Responsible for delivering packets from the source to the destination host across multiple networks.

Main functions of the Network layer:

① Logical Addressing:
- → Assigns IP address to devices.
- → Ensures every device on the network is uniquely identified.

② Routing:
- → Selects the best path for data to travel from source to destination.
- → Uses Routing algos & routing tables.

③ Packet forwarding:
- → Moves packet from one router to another towards destination.

④ Fragmentation & Reassembly
- → Breaks large data packets into smaller pieces mostly based on network's maximum transmission unit (MTU).
- → Reassembles them at destination.

IP   ICMP   IGMP   Error handling by ICMP

RP → ~~OSPF, B~~ OSPF, RIP, etc.

3.1

Forwarding and Routing

→ Very important ~~features~~ services provided by NL.
→ The decision of NL is based on Routing and forwarding.

Forwarding

- Forwarding is the action applied to each router, when a packet arrives at one of the interfaces.
- It is the process of moving a packet from the router's input port to the correct output port based on destination address.
  - → Happens within router.
  - → Uses forwarding table for decision.
  - → Fast operation.

Routing:

- Routing is the process of finding best path for data to travel from the source to the destination across multiple routers or n/ws.
  - → Happens between routers.
  - → Uses routing algorithms.
  - → Builds and maintain routing table.

☆ Virtual circuit and Datagram Packet Switching

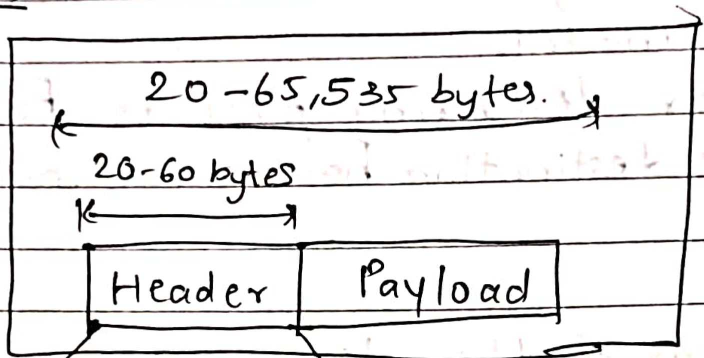
	Virtual Circuit Switching	Datagram packet switching
1	A virtual circuit is a predefined logical path established before data is sent.	Each packet is treated individually. Packets may take different paths to reach the destination.
2	It is Connection-oriented	It is Connectionless
3	Order of packets is maintained.	Order of packets may vary at receiver.
4	Packet header is smaller (only Virtual ID needed)	Packet header is bigger (full destination address in every packet).
5	Resources are reserved.	No resource reservation (shared dynamically)
6	High delay due to setup time	Low delay as there's no setup time.
7	Efficient for long and steady transmissions.	Efficient for bursty or short messages.
8	High reliability.	Lower reliability
9	Low overhead in router	High overhead in router
10	Used in ATM (Asynchronous Transfer Mode), X.25	Used in Internet (IP), Voice over IP (VoIP), etc.

X.25 → Older PS Network protocol

3.2 The Internet Protocol (IP)

☆ IP header (IPv4):

IPv4



160 bits

20 bytes

<table>
<tr><td>VER
4 bits</td><td>HLEN
4 bits</td><td>Type of service
8 bits</td><td colspan="2">Total length (TLEN)
16 bits</td></tr>
<tr><td colspan="3">Identification
16 bits</td><td>Flags
3 bits</td><td>Fragmentation offset
13 bits</td></tr>
<tr><td colspan="2">TTL
8 bits</td><td>Protocol
8 bits</td><td colspan="2">Checksum
16 bits</td></tr>
<tr><td colspan="5">Source IP (32 bits)</td></tr>
<tr><td colspan="5">Destination IP (32 bits)</td></tr>
<tr><td colspan="5">Options + Padding
(0 to 40 bytes)</td></tr>
</table>

Page No:
Date:

① Version number (VER):
The 4 bit version number (VER) field defines the version of the IPv4 protocol, which has the value of 4.

② Header length (HLEN):
The 4-bit header length (HLEN) field defines the total length of datagram header. IPv4 has variable-length header.

③ Type of Service
→ Also called as Differentiated Services Code Point (DSCP).
→ This field ~~is~~ provides features related to quality of service for data streaming or VoIP calls.
→ First 3 bits are priority bits, also used for specifying how one can handle Datagram.

④ Total Length:
→ TLEN is measured in bytes.
→ Minimum size → 20 bytes, Max → 65535 bytes. (as TLEN field is 16 bits).
→ HLEN & TLEN can be used to calculate dimensions of payload.

⑤ Identification:
→ Used to identify fragments of an IP datagram uniquely.
→ Some have recommend using this field for other things like adding info for packet tracing, etc.

Page No:
Date.

6. IP flags:

→ 3 bit fields that helps us to control and identify fragments.

Bit 0: Reserved
Bit 1: Do not fragment.
Bit 2: more fragments

7. Fragment offset:

→ Represents no. of Data bytes ahead of a particular fragment in specific Datagram.
→ Specified in terms of number of 8 bytes.

8. Time to Live (TTL):

→ 8-bit field which indicates maximum number of hops visited by datagram.
→ Each router that processes the datagram and decrements number by 1.
→ When this becomes zero, datagram is discarded by the router.

9. Protocol:

→ IPv4 header is reserved to denote that IP is used in the later portion of Datagram.
eg. 6 no. digit is mostly used to indicate TCP
17 is used to denote UDP protocol

~~10. Checksum:~~

1 → ICMP
2 → IGMP
6 → TCP
17 → UDP
89 → OSPF

(10) Header Checksum:
- 16 bit checksum field, used to check header for any errors.
- IP header is Compared to checksum value. If not matching, packet will be discarded.

(11) Source & Desintation address:
32 bit address.

(12) IP options:
- Optional field of IPv4 header used when HLEN value is set to greater than 5.
- Used for network testing & debugging.

Type of service:

			D	T	R	C	

← Precedence →   Tos bits

D → Minimize delay (1000)
T → Maximize throughput (0100)
R → Maximize reliabity. (0010)
C → Minimize cost (0001)

Normal default (0000).
(ICMP, BOOTP)

IP addressing:

- IP address is a numerical representation that uniquely identifies a specific interface on the n/w.
- IPv4 addresses are 32 bits long. This allows a maximum of 2^{32} unique address.
- Address in IPv6 are 128 bits long. 2^{128} unique address.
- Binary but typically represented/expressed in decimal (IPv4) or hexadecimal (IPv6) to make reading easier for humans.
- IPv4 address are 32 bit binary nos, consisting of two ~~subnet~~ address (identifiers) which identify network ID and host ID,
- Shown as 4 octets of nos. from 0 - 255. represented in decimal form.

eg. 192.168.0.102

00000011.10101000.00000000

Classful Addressing

	Byte 1	Byte 2	Byte 3	Byte 4
Class A	NET ID	HOST ID		
Class B	NET ID		HOST ID	
Class C	NET ID			HOST ID
Class D	~~NET ID~~ MULTICAST APP			
Class E	RESERVED.			

Class A	0 → 127	255.0.0.0
Class B	128 → 191	255.255.0.0
Class C	192 → 223	255.255.255.0
Class D	224 → 239	N-d
Class E	240 → 255	N-d

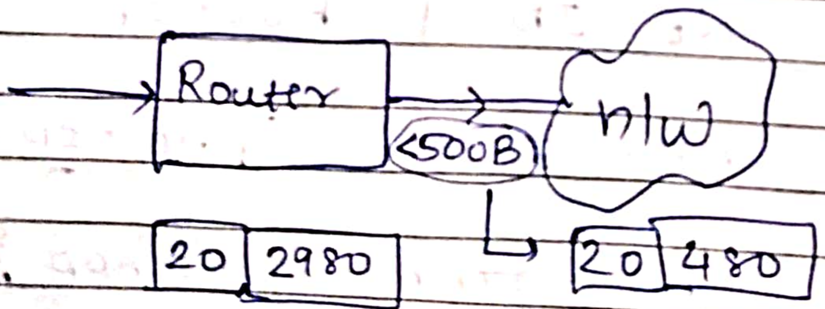
☆ IP fragmentation

Identification	Flag	Fragment offset

Res. 0	DF	MF	
0	0	0	→ Fragmentation done ~~Do not fragment~~
0	0	1	→ More fragments
0	1	0	→ Do not fragment
~~0~~	~~1~~	~~1~~	→

Q. A datagram of 3000B (20B of IP header + 2980B IP payload) reached at router and must be forwarded to link with MTU of 500B. How many fragments will be generated and also write MF offset, Total length for all.

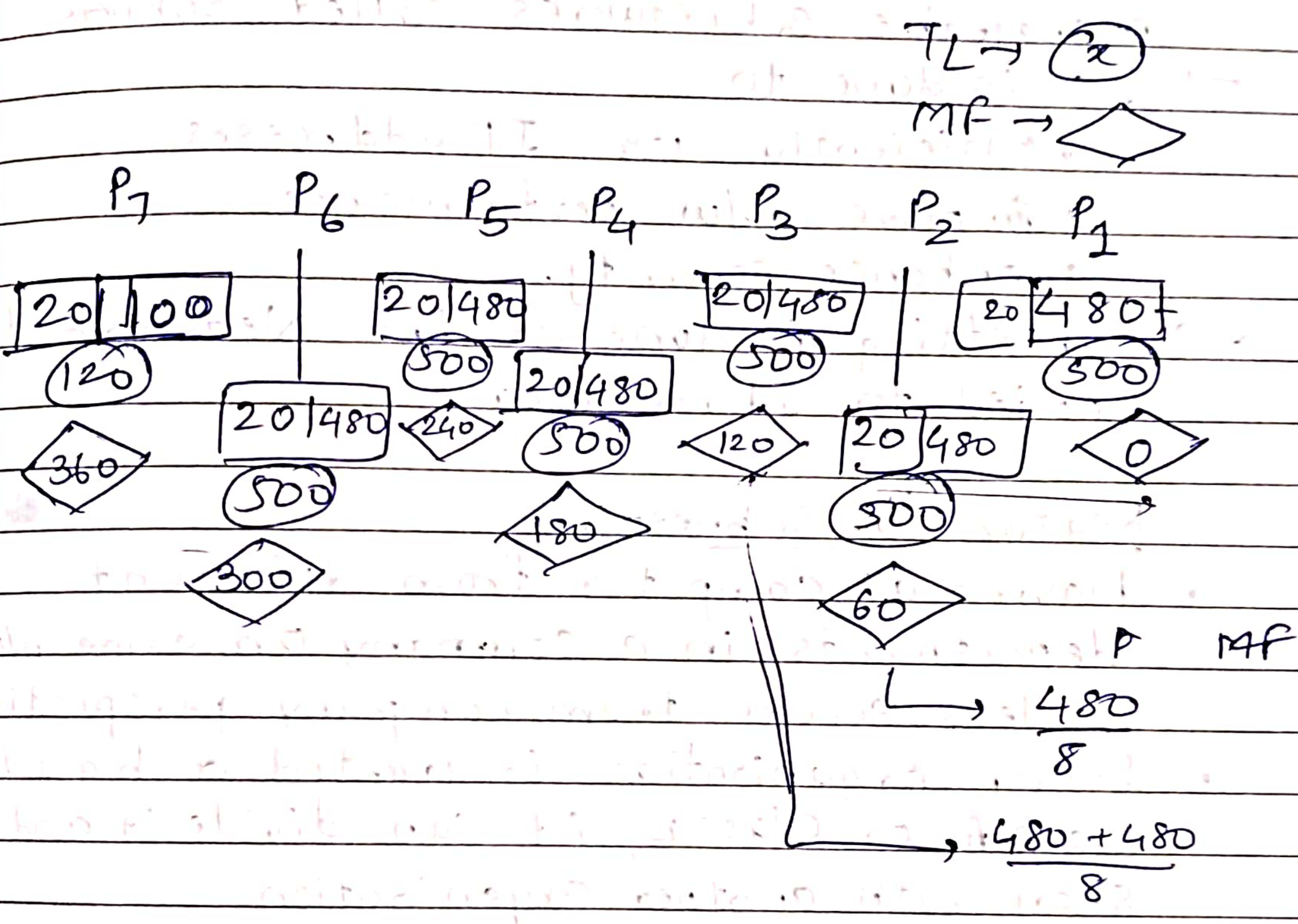
→



Fragmentation at Router

No. of fragments $= \frac{2980\,B}{480\,B} = 6.208\ldots$

No. of fragments $= 7$



Page No
Date

Subnetting

→ Subnetting is a process of dividing a large network into smaller, more manageable subnetworks called subnets.

→ It is done to:
- Efficiently use IP addresses.
- Improve n/w performance
- Enhance security.

→ Subnetting is done at the Network layer applied to IPv4 address

Reason for subnetting

- Having all computer from different departments in a company on same n/w is less secure from company perspective.
- If an organisation is granted a big n/w class A or class B, it can divide it and share with another organisation.

Disadvantages:

- Difficulty in station identification.
- Broadcast not possible (directed) from outside n/w.

Subnetting

Subnetting → Fixed length Subnetting | Variable length Subnetting

→ Same size subnets.
→ serve same no. of hosts
→ same subnet mask.

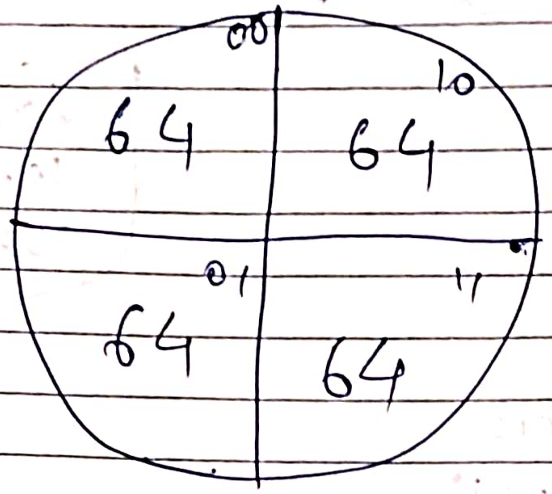
Q. Consider a n/w having IP address 200.1.2.0 Divide into 2 subnets. (256)
→ (class C).

	SN = 1	SN = 2
Subnet id →	200.1.2.0	200.1.2.128
Direct BC →	200.1.2.01111111 200.1.2.127	200.1.2.11111111 200.1.2.255
Total no. IP Add =	$2^7 = 128$	$2^7 = 128$
Range →	200.1.2.0 – 200.1.2.127	200.1.2.128 – 200.1.2.255
No. of host conf.	128−2 = 126	128−2 = 126
Range of Allocated	200.1.2.1 – 200.1.2.126	200.1.2.129 – 200.1.2.254
	128	128

$\boxed{200.1.2.0}$0000000 → 0–127
← 25-bits →   1111111

$\boxed{200.1.2.1}$0000000 → 0–127
← 25-bits →   1111111

In 4 subnets (200.1.2.0)



0

$\boxed{200.1.2.00}$ 000000

64

$\boxed{200.1.2.00}$ 111111

64

$\boxed{200.1.2.01}$ 000000 65

64

$\boxed{200.1.2.01}$ 111111

127

128

$\boxed{200.1.2.10}$ 000000

64

$\boxed{200.1.2.10}$ 111111

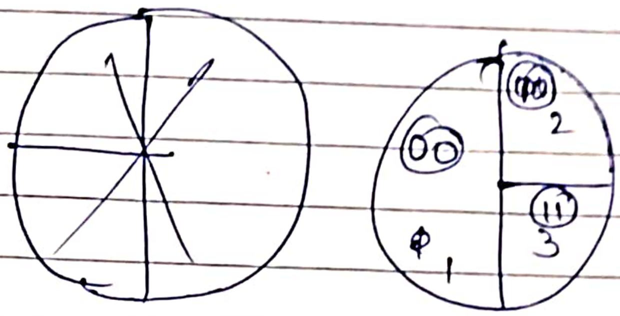
$\boxed{200.1.2.11}$ 000000

64

$\boxed{200.1.2.11}$ 111111

Variable length subnetting

Consider a big network 200.1.2.0. Subnet and divide into 3 subnets, such that first contains 126 hosts and other two 62 hosts each.



1st → 200.1.2.00 0000000 → 200.1.2.0

200.1.2.00 1111111 → 200.1.2.127

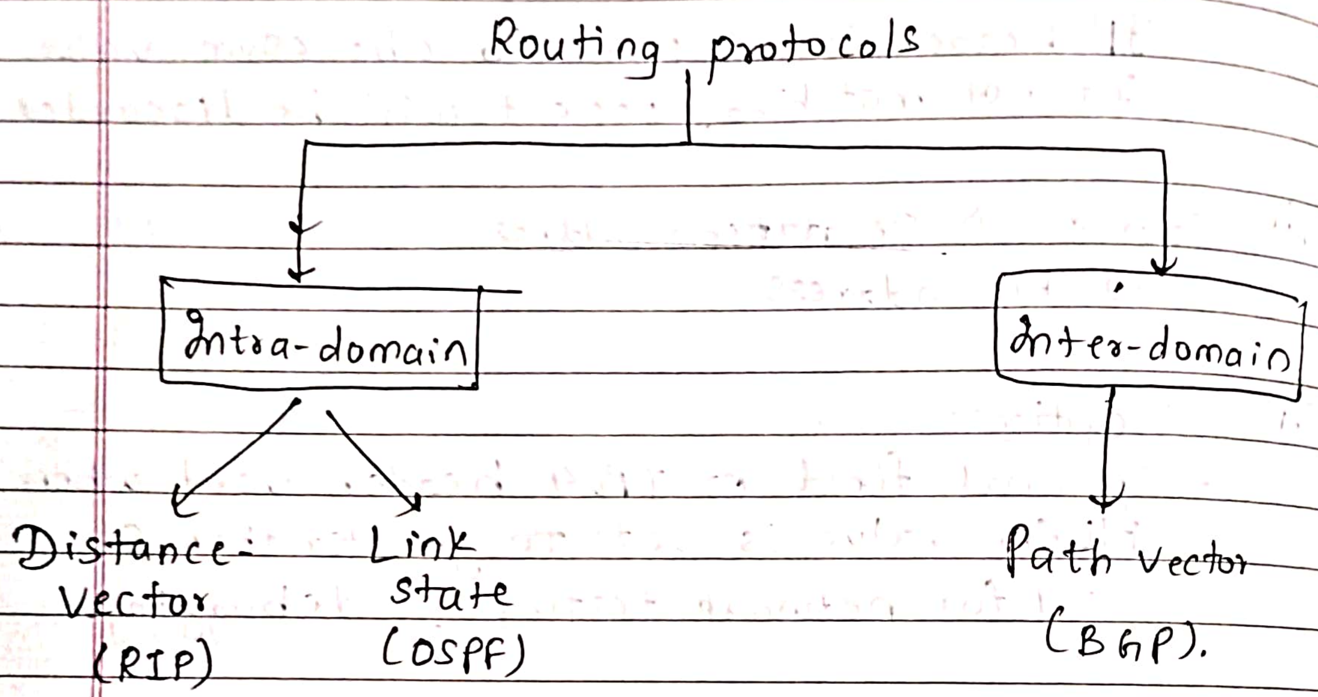
2nd → 200.1.2.10 000000 → 200.1.2.128

200.1.2.10 111111 → 200.1.2.191

3rd → 200.1.2.11 000000 → 200.1.2.192

200.1.2.11 111111 → 200.1.2.255

✩ Routing algorithms



Routing protocol is a set of instructions to be followed during routing and routers have to update the route in their ~~d~~ routing table for static and dynamic routing.

Used in original ARPANET
In internet as RIP.
~~Routing Information Protocol~~ (Introduced in 1980s
Also called Bellman Ford algo)

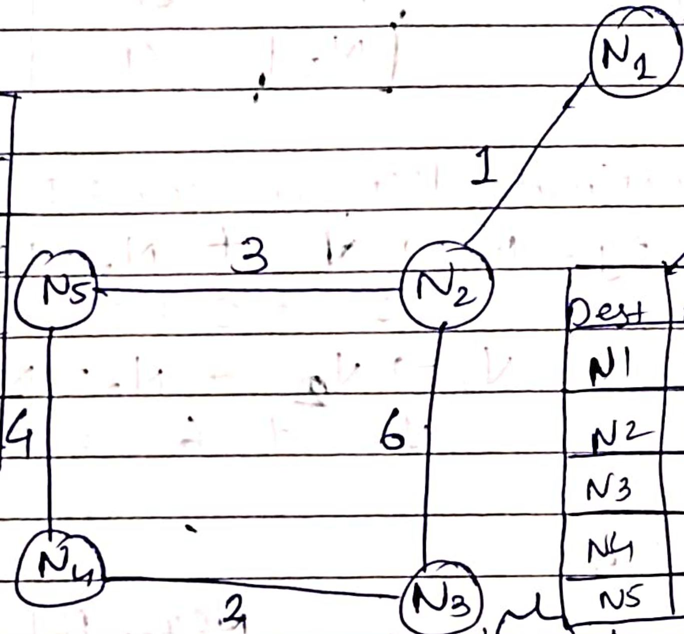
- **Distance vector routing**
- In distance vector routing, each node keeps a routing table containing the minimum distance to other nodes.
- The table includes next hop, indicating the next node to which a packet should be forwarded

N1:

Dest	Dist	Next
N1	0	N_1
N2	1	N_2
N3	∞	–
N4	∞	–
N5	∞	–

N5:

Dest	Dist	Next
N_1	∞	–
N_2	3	N2
N_3	∞	–
N_4	4	N4
N_5	0	N5



N2:

Dest	Dist	Next
N1	1	N_1
N2	0	N_2
N3	6	N_3
N4	∞	–
N5	3	N5

N4:

Dest	Dist	Next
N1	∞	–
N2	∞	–
N3	2	N3
N4	0	N4
N5	4	N5

N3:

Dest	Dist	Next
N1	∞	–
N2	6	N2
N3	0	N3
N4	2	N4
N5	∞	–

- After this, the routing table's distance vector is shared between neighbours

eg. N_1 sends to N_2
N_2 sends to N_1, N_3, N_5
N_3 sends to N_2, N_4
N_4 sends to N_3, N_4
N_5 sends to N_2, N_4

At N_1,

N_2
1
0
6
∞
3

N_1 new RT

Dest	Dist	Next
N_1	0	N1
N_2	1	N2
N_3	7	N_3
N4	∞	—
N_5	4	N5

To estimate dist in new RT,

eg. $N_1 \to N_2 + N_2 \to N_2$

$1 + 0 = 1$

$N_1 \to N_2 + N_2 \to N_3$

$1 + 6 = 7$

At N_5

N_2	N4
1	∞
0	∞
6	2
∞	0
3	4

New RT of N5

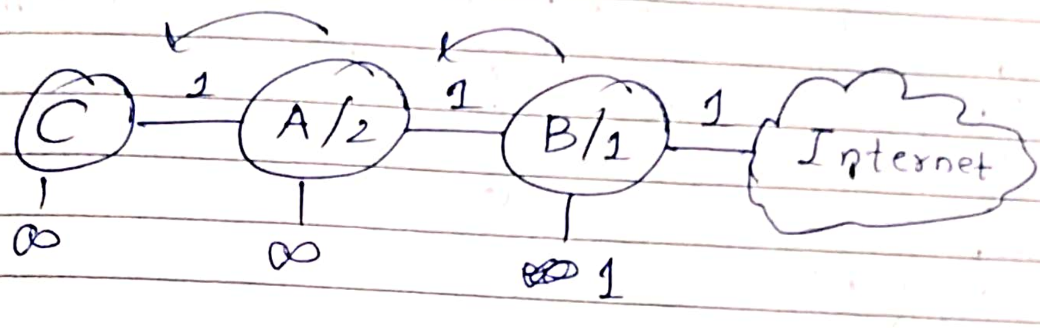
Dest	Dist	Next
N'	4	N1
N2	3	N2
N3	6	N3
N4	4	N4
N5	0	N5

Choose minimum path out of all cost

Make same for every router

can write directly too.

• Count to infinity problem in distance vector routing



cost to internet →

- In the first pass, neighbours will share the distance vector
  Here, B will sent to A/2, which is okay it shares cost 1 to reach to internet & 1 to reach A/2.
- In the second pass, (or after more than 1 pass here),

∞	∞	1	1
∞	2	1	2
3	2	1	3
3	2	1	4

Normal case

Let's suppose, internet connection between B/1 & ~~Ba~~ broke, B will know it and set ∞ internet

3 2 ∞

After this, B sends ∞ to A

3 2 ∞

C says I will take you ~~to~~ internet with cost 3, A can't realise its via A & B, & ignores B's infinity message as shorter path is via C.

For IP,
RIP
max hop
count = 15

16 → unreachable n/w

3	2	∞
3	4	3
5	4	5
5	6	5

(same happens at B).

Periodic updates
Via Broadcast
255.255.255.255

DEAD

Entire routing table is sent in updates

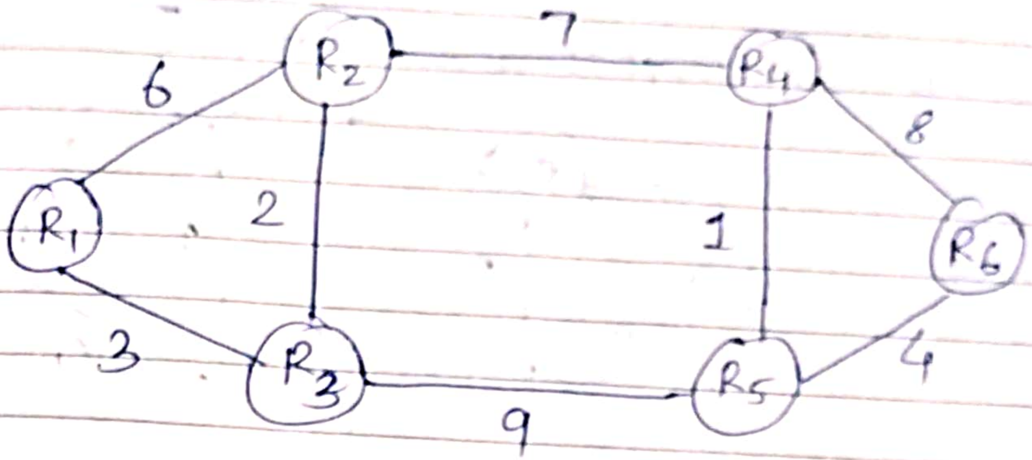
This problem occurs because we only send distance vector, ~~and~~ no by which one can't identify the route, just plays in shortest dist.

- **Link-state Routing:**

→ Link State Routing is a type of routing Strategy which uses different approach compared to distance vector routing.

→ Operates based on idea that each node within a n/w knows entire n/w's topology, which includes
  - list of nodes and links along with their type, cost (metric), and condition (up or down).

→ The routing process leverages Dijkskra's algorithm to construct the Shortest path tree from its network topology, thereby allowing each node to create its routing table.



① Link-state table

R1	
Sq no.	
TTL	
R_2	6
R_3	3

R3	
R_1	3
R_2	2
R_5	9

R5	
R_3	9
R_4	1
R_6	4

R6	
R_4	8
R_5	4

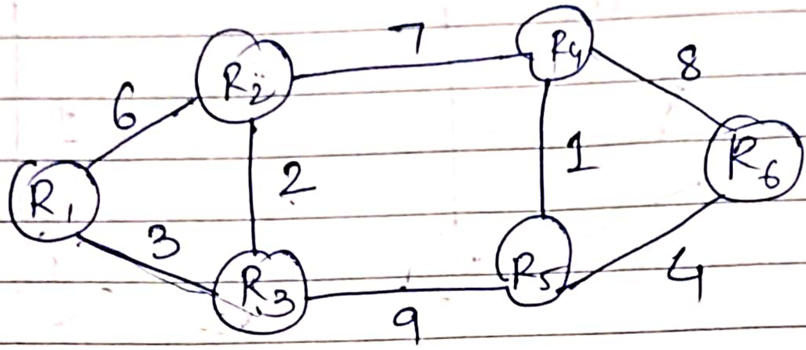
R2	
R_1	6
R_3	2
R_4	7

R4	
R_2	7
R_5	1
R_6	4

- We use flooding in LS routing.
- TTL field is used to save packet to save it from stucking in infinite loop.
- flooding: each node shares its routing table to all nodes, which leads to high BW utilization.

Page No
Date.

Using Dijkstra's algo,



R_1	R_2	R_3	R_4	R_5	R_6
0	6	3	∞	∞	∞
$R_1 R_3$	5	3	∞	12	∞
$R_1 R_3 R_2$	5	3	12	∞	∞
$R_1 R_3 R_2 R_4$	5	3	12	13	20
$R_1 R_3 R_2 R_4 R_5$	5	3	12	13	17

		Via
R_1	0	R_1
R_2	5	$R_1 R_3$
R_3	3	R_1
R_4	12	$R_1 R_3 R_2$
R_5	13	$R_1 R_3 R_2 R_4$
R_6	17	$R_1 R_3$ ~~$R_2 R_4 R_5$~~

3 tables are created ~~at~~ in LSP.

- Neighbour table.
- Topology table. (Link state table)
- Routing table