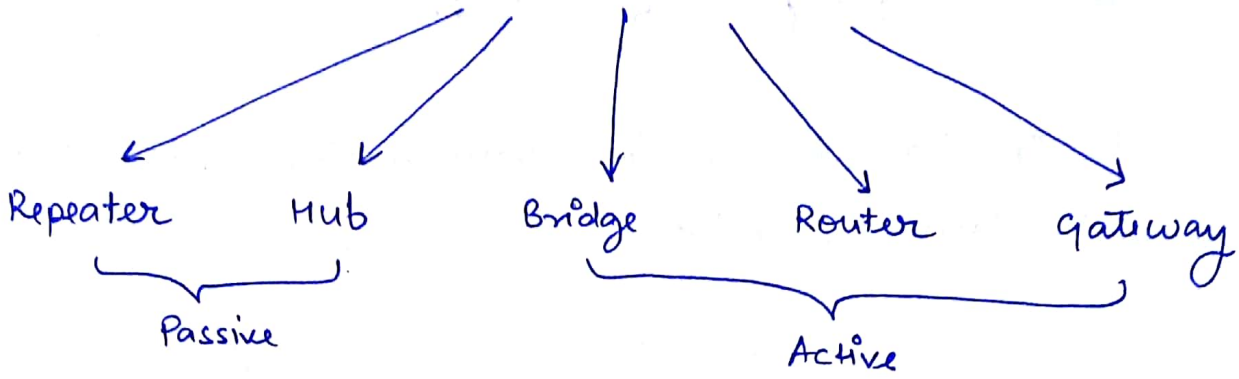
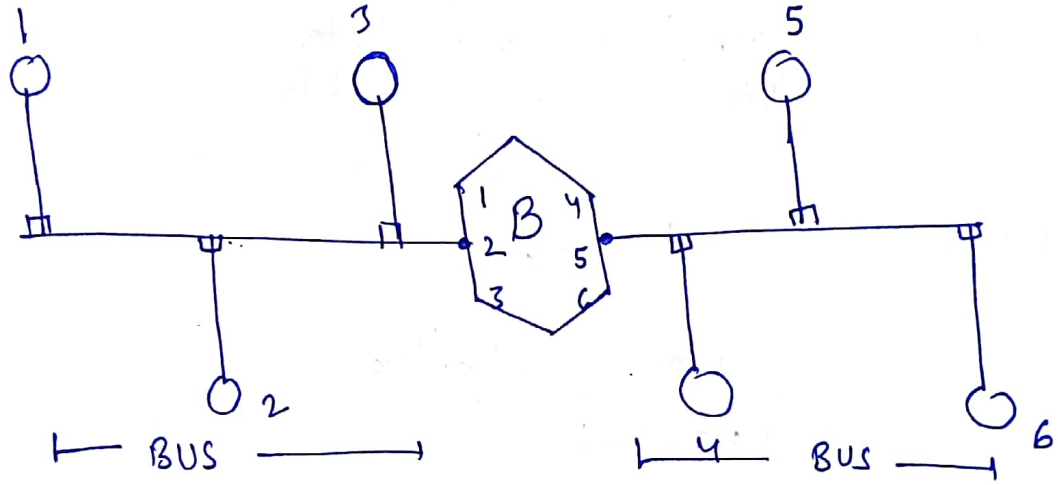
Networking devices



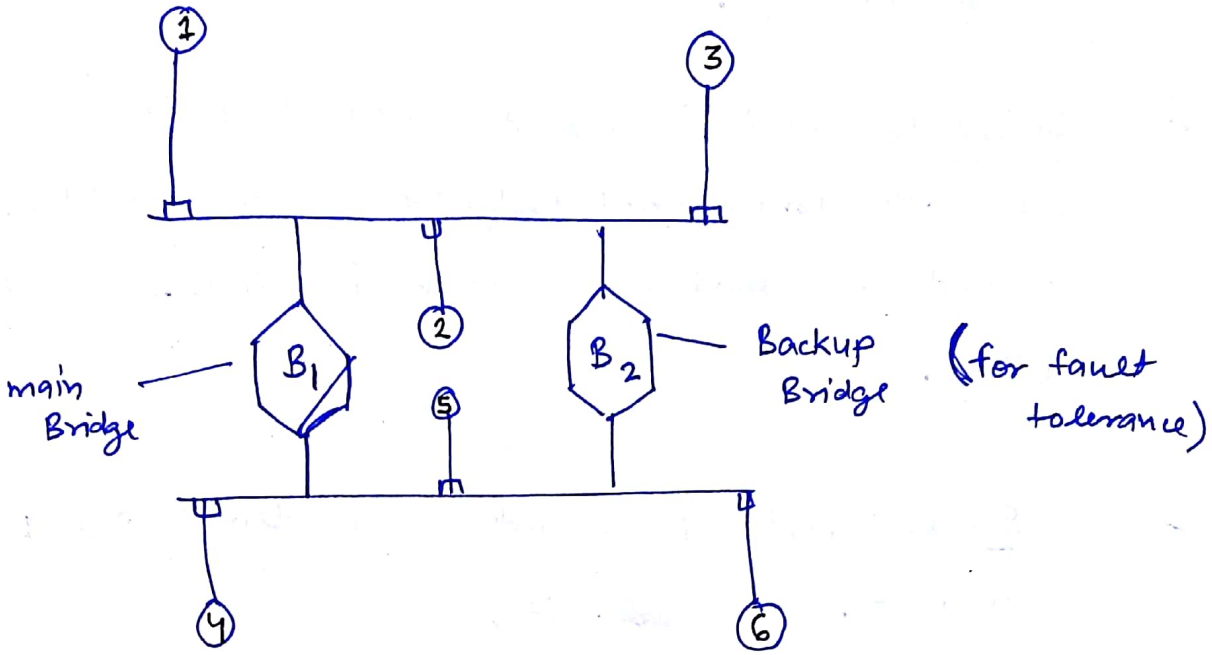
Bridge :-

- It is a LAN device which is used to connect similar LAN topologies.



- Its operation is based on MAC address.
- Initially the "bridge table" is empty.
- Functions of a Bridge are :
  - ↳ Learning
  - ↳ Forwarding
  - ↳ Blocking

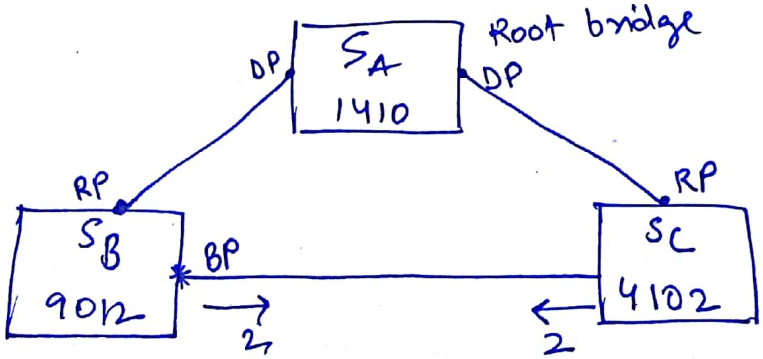
- Once Bridge know the complete information, then it is treated as converge and stable.



- When we connect more than one Bridge ↳ loop possibility of problem is developed during Broadcasting, as we know Bridge is not a Broadcast domain seperator. So the Graph should be converted into tree using spanning tree protocal (IEEE 802.1C).

Spanning Tree Protocol :-

i) Bridge having the least MAC address will becomes root bridge.



- Root port is a port which has the least cost path from non-root bridge to root-bridge. It is used for sending the data.

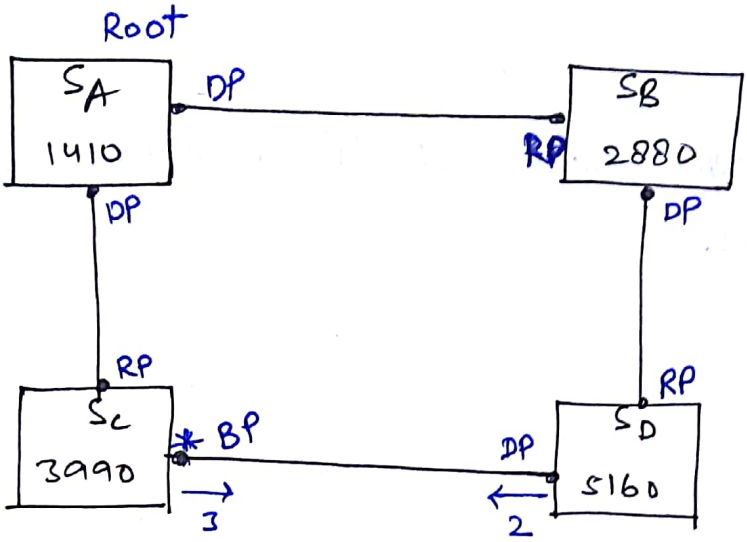
- Designated port is a port which is having least cost path from root bridge to non-root bridge. It is used for sending configuration files by the root bridge.

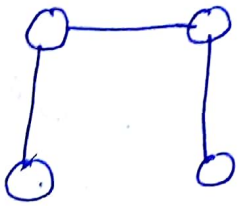
- Blocked port is a port which temporary disabled the port. For it,

BP → assign that port which has highest cost path from non-root to root

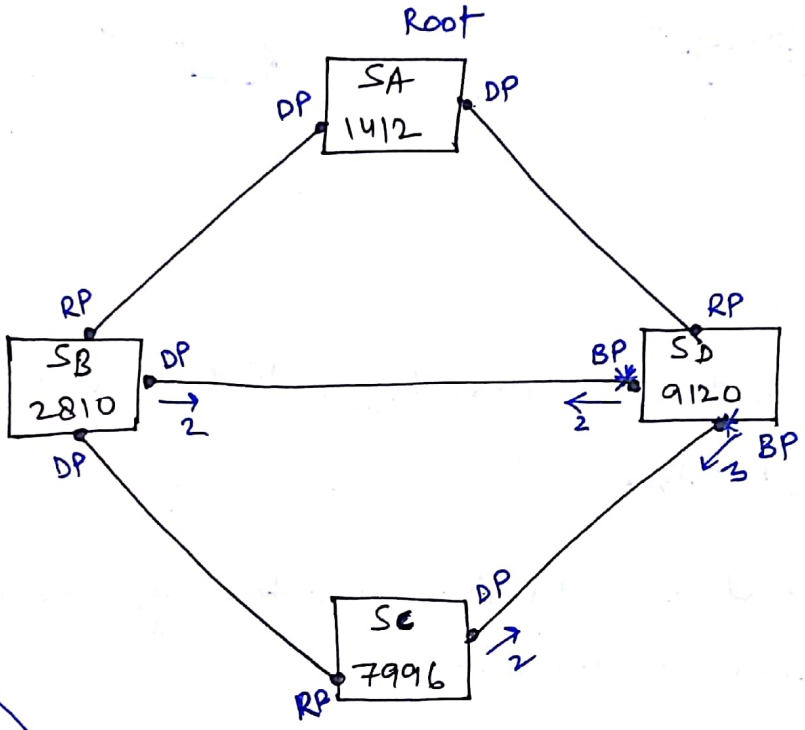
```
if (cost is same for more than one port)
{
    compare MAC of those Bridge;
    highest MAC Bridge port is assigned finally;
}
```

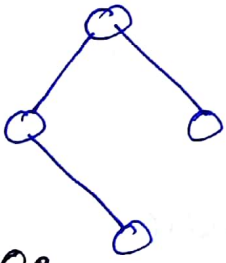
Q.



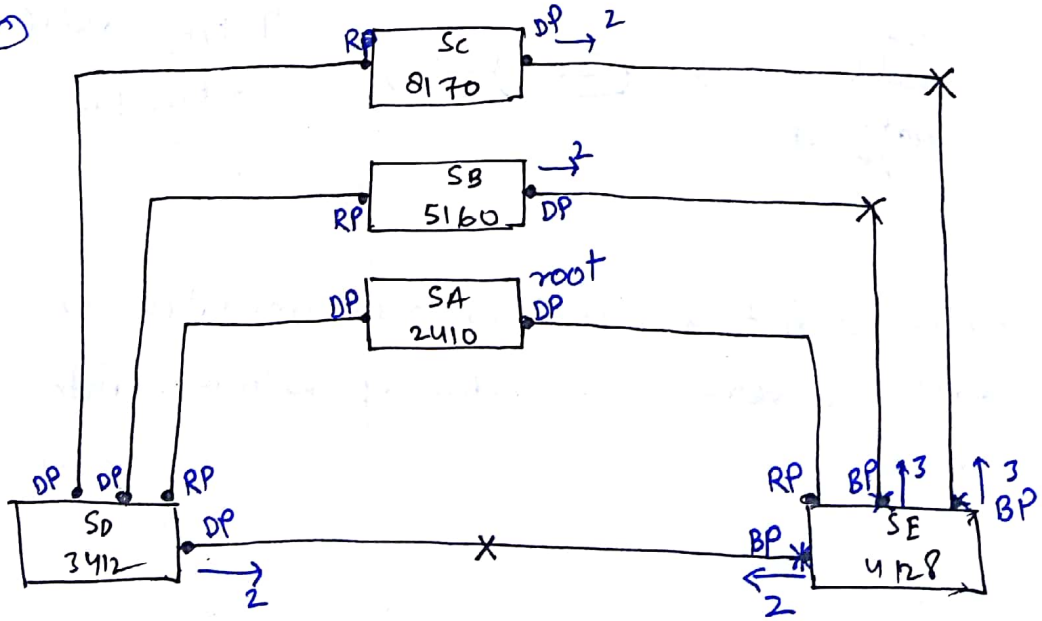


Q.



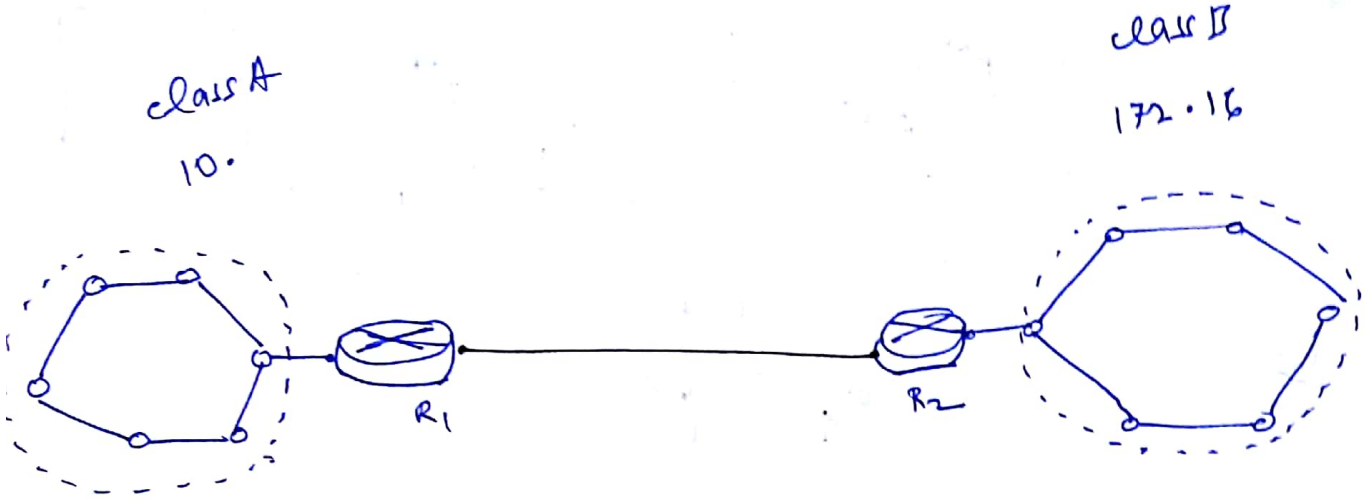


Q.

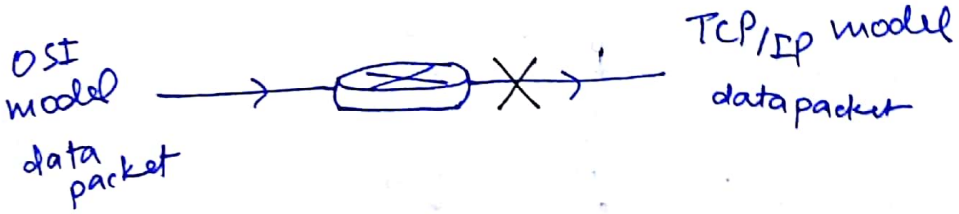


Router :-

- It is a WAN device and its operation is based on IP addresses.



- Router is used for connecting dissimilar networks or different networks.
- It is broad cast domain seperator by defaul as well as collision domain seperator.



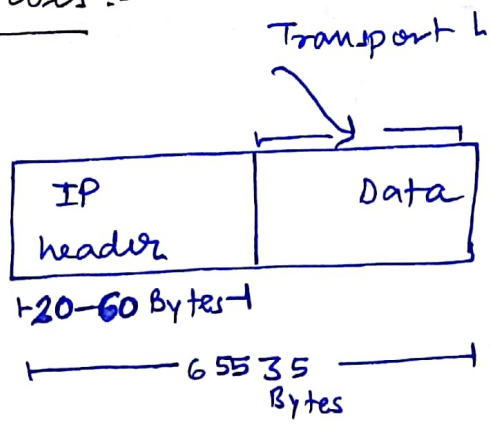
- Router is not a multi-protocol converter because it can't convert one modal of network into another modal.

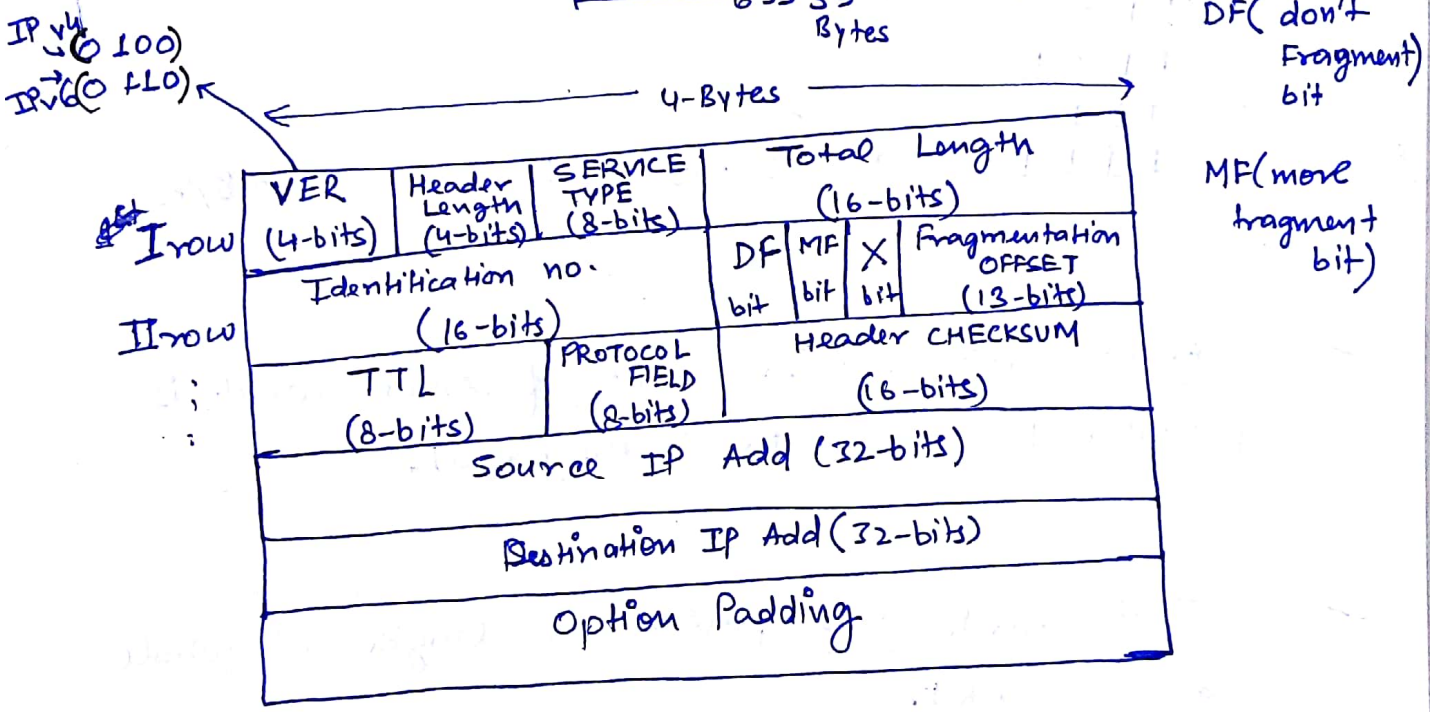
- Gateway is a highly sophisticated router & it act as multi-protocol convertor.

Network Layer Protocols :-

IP - Protocol

↳ Packet =





VER

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

- Header length is going to indicate the size of the Header i.e available in the packet

0 0 0 0 ┐
0 0 0 1 │
0 0 1 0 │ X dont' care
0 0 1 1 │
0 1 0 0 ┘

0 1 0 1 ⟶ 5 rows ⇒ 5 × 4 Bytes = 20 Bytes
0 1 1 0
0 1 1 1
1 0 0 0
1 0 0 1
1 0 1 0
1 0 1 1
1 1 0 0
1 1 0 1
1 1 1 0
1 1 1 1 ⟶ 15 rows ⇒ 15 × 4 Bytes = 60 Bytes

- SERVICE TYPE indicates type of service which is provided by the router to the packet.

- Total Length bits provide the length of whole IP packet.

Since it is of 16-bits so maximum length of IP packet when it has 16 1's so,

$$2^{16} - 1 = 65535 \text{ Bytes}$$

Q. Total length bits are –

. 0000001111111

H-length : 1111

Size of data = 9

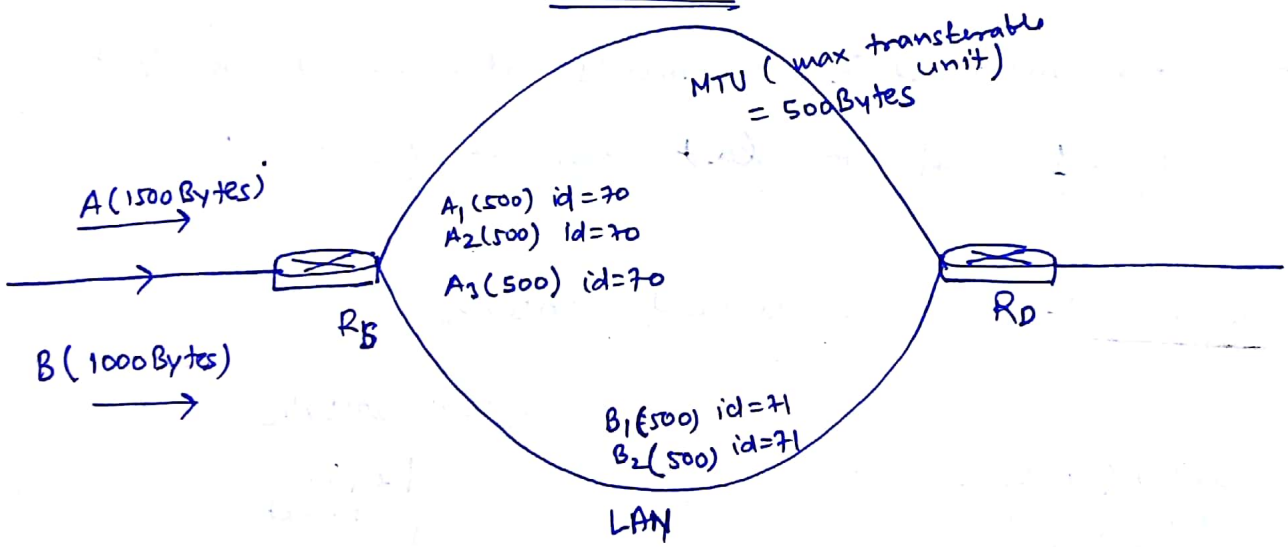
Size of packet = 127 Bytes

Size of header = 15 rows

= 15 × 4 = 60 Bytes

So, Data = Packet – header

= 67 Bytes



- Fragments belonging to same packet will be given same identification number (id), so that the destination router can easily combine them.

- if DF bit = 1 ⇒ packet
  = 0 ⇒ fragment

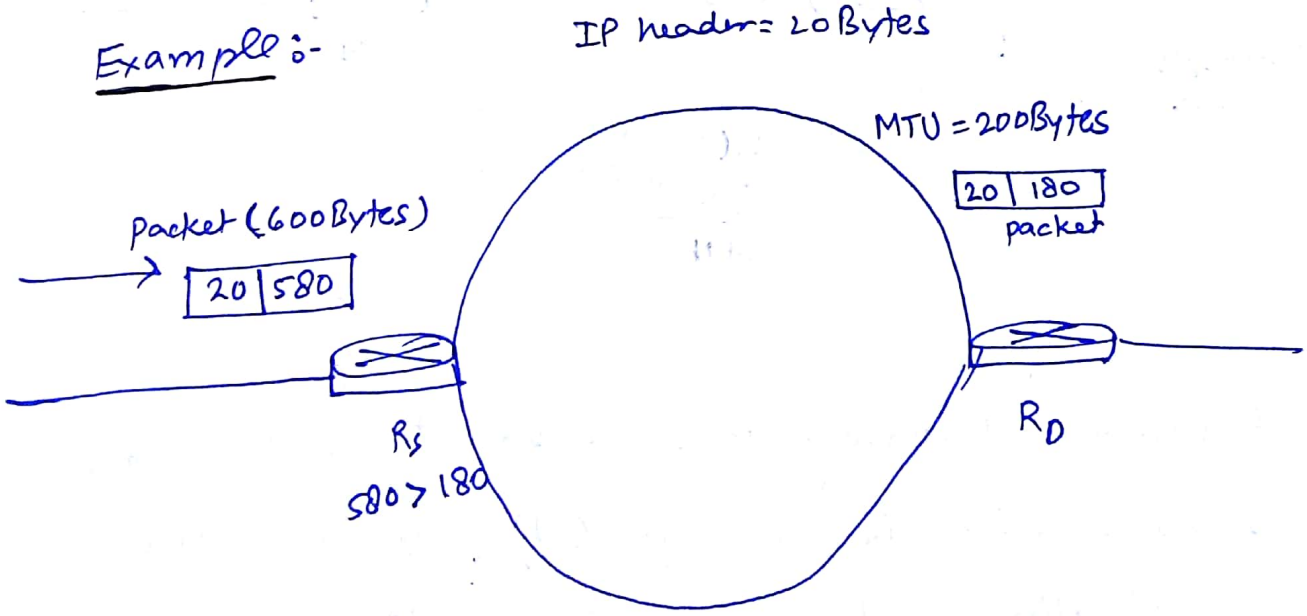
Packet A (1500 Bytes) → Fragment A_1 (500),
→ " A_2 (500)
→ " A_3 (500)

Fragments

	id	DF	MF
A_1	70	0	1
A_2	70	0	1
A_3	70	0	0

- All intermediate fragments starting from first MF = 1 and for last fragment MF = 0.

Example :-

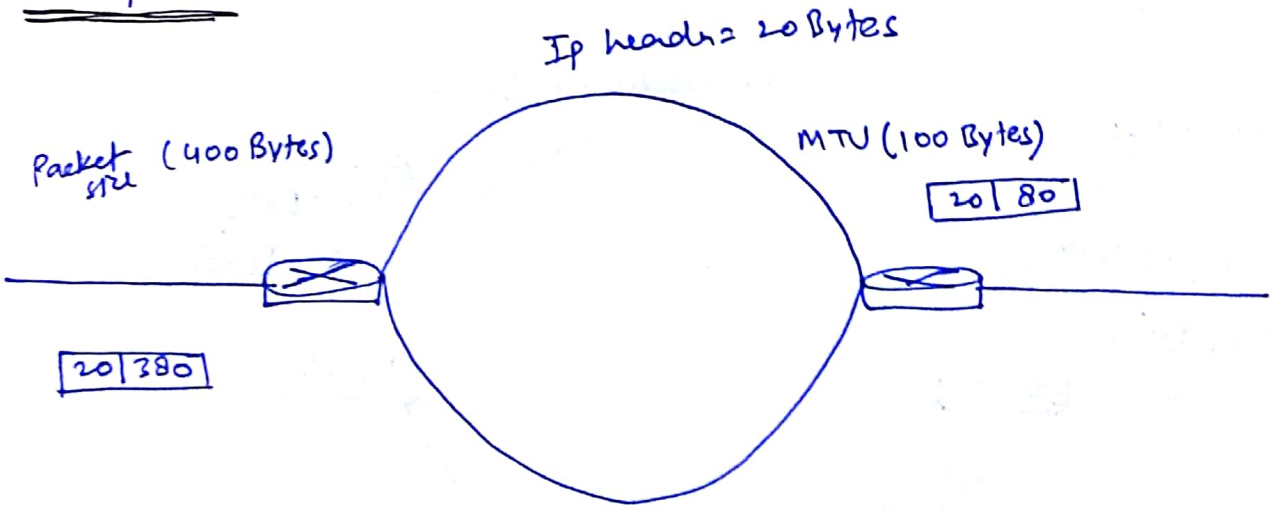


no. of fragments = $\frac{580}{180} \simeq 4$

	I frag	II frag	III frag	IV frag
Id	90	90	90	90
DF	0	0	0	0
MF	1	1	1	0
Fragment Bytes	20 | 176 (multiple of 8 < 180)	20 | 176	20 | 176	20 | 56 (52+4 padding bits)
Fragmentation offset	(0-21)	(22-43)	(44-65)	(66 - 72)

- Fragmentation offset = Fragmentation Bytes / 8

Example-2 :-



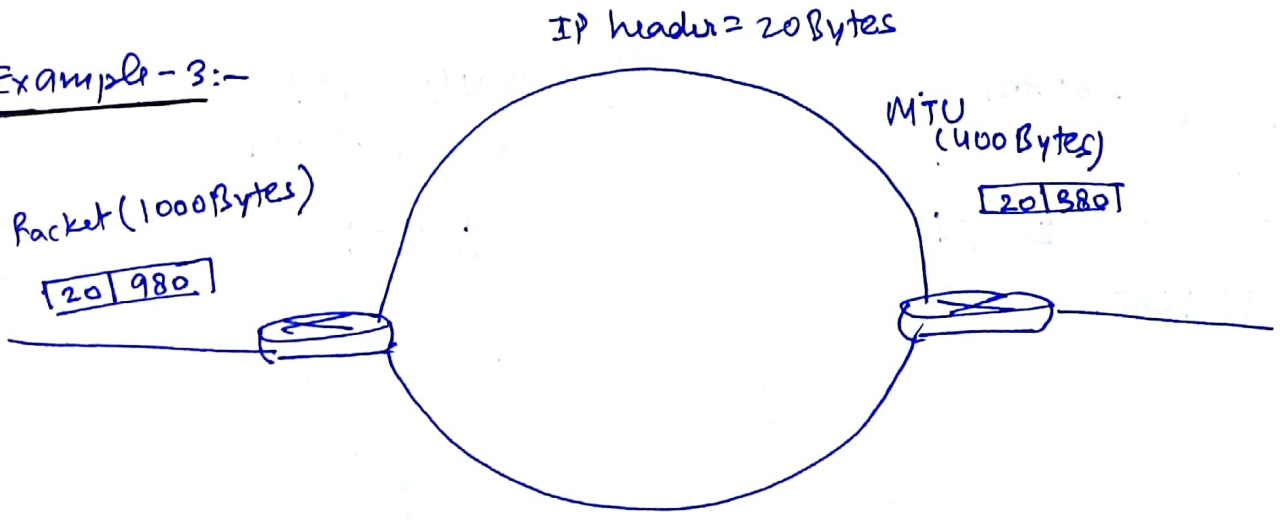
no. of fragments = $\frac{380}{80} \cong 5$

$$\begin{array}{r} 380 \\ -320 \\ \hline 60 \end{array}$$

	Frag I	Frag II	Frag III	Frag IV	Frag V
id	80	80	80	80	80
DF	0	0	0	0	0
MF	1	1	1	1	0
Frag Bytes	20 | 80	20 | 80	20 | 80	20 | 80	60+4 → 20 | 64 (padding)
Frag offset	(0-9)	(10-19)	(20-29)	(30-39)	(40-49)

- Packet Header is given to all fragments with some change in values.

Example-3:-



no. of frames = $\frac{980}{380} \cong 3$

$\frac{376}{752}$ $\quad$ $\frac{980}{752}$ $\quad$ $\frac{752}{228}$

	Frag I	Frag II	Frag III
id	70	70	70
DF	0	0	0
MF	1	1	0
Fragment Bytes	20 | 376	20 | 376	20 | 232 (228+4)
Fragment offset	(0-46)	(47-93)	(94-122)

Q: Fragment offset are given as (0, 30, 60, 90). IP header = 20 Bytes. All header are of equal size. Calculate Fragment size, and Packet size.

Fragment offset diff = 30

so, size of Fragment = $20 + \frac{30 \times 8}{}$

$= 20 + 240$

$= 260$ Bytes

Since there are four fragments so,

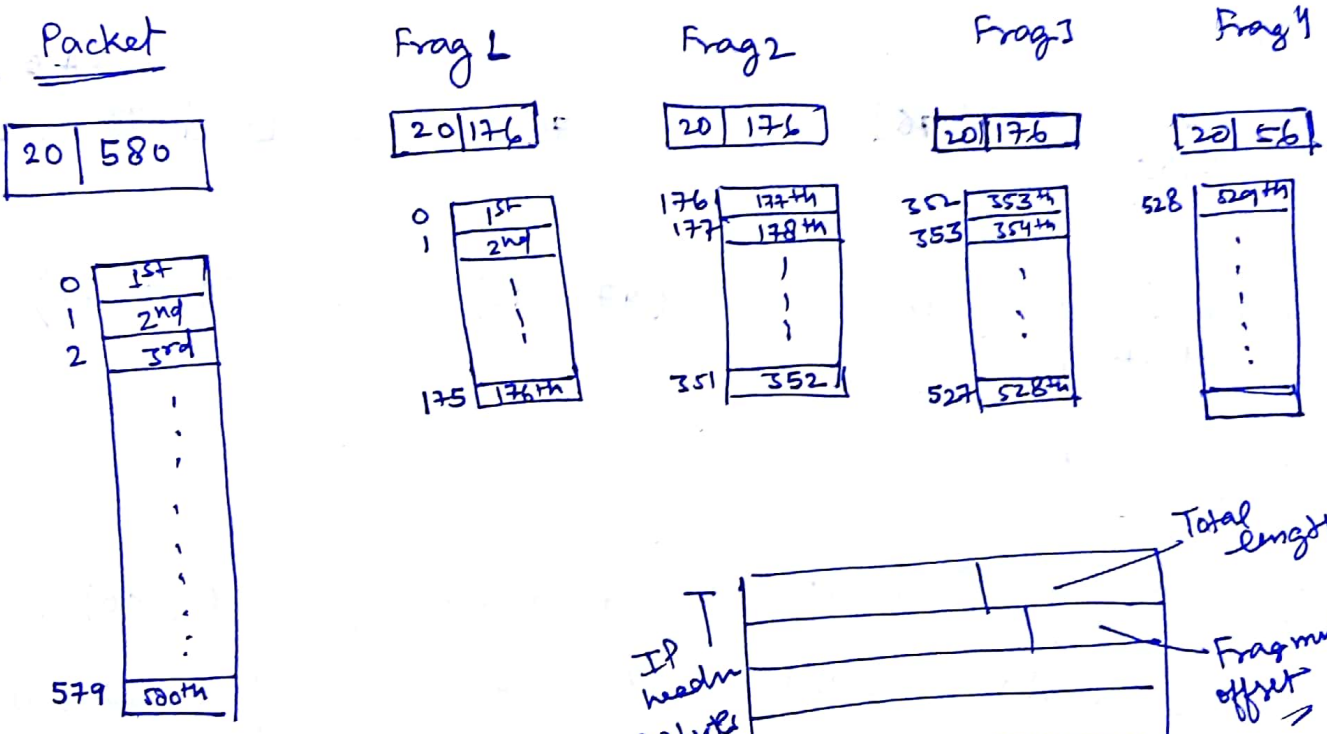
size of packet = 240×4 = 960 + IP header

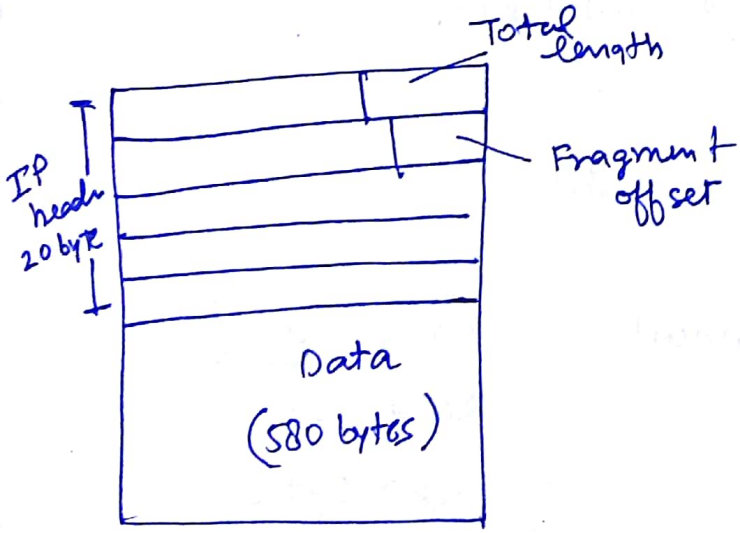
= 960 + 20

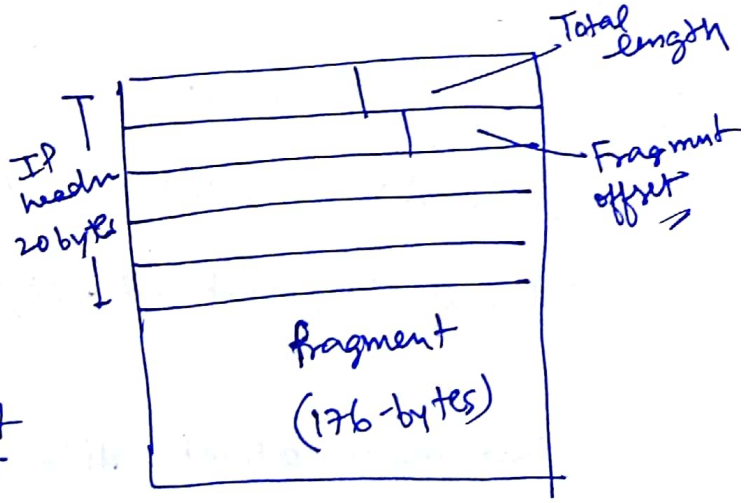
= 980

IP Packet = | 20 | 960 |

← 980 bytes →







- "Total length" of a packet defines packet length whereas, Total length in a fragment defines no. of bytes or fragment length.

- Fragment offset × 8 will give starting address of fragment.

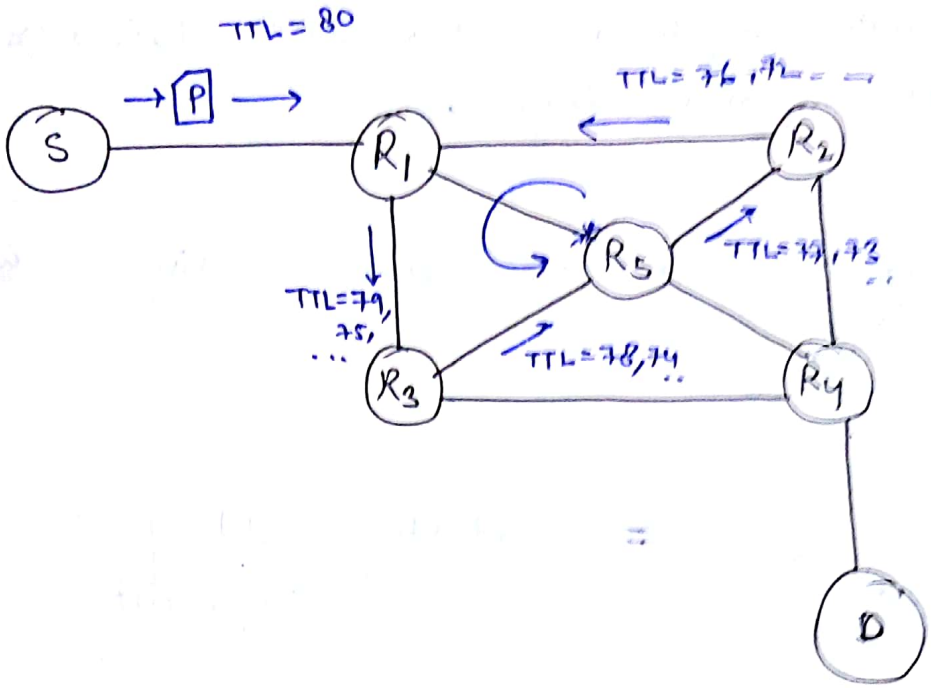
(Fragment offset × 8 = starting add of fragment)

- If any padding bits are added that can be removed at the destination with the help of MF bit. Because for the last fragment MF value is 0.

- Whenever a packet is fragmented it can be further fragmented. If a smaller MTU occurs in the network.

- From source - to - destination the ID value for the fragments of a same packet will remains same.

Identification



- Due to break in Link (R_1—R_5) routing tables disturbed and it is possible that some packet moves in a loop ($R_1 - R_3 - R_5 - R_2 - R_1$) , .

- Thus TTL (time-to-leave) is used to find out if any loop exist or not.

- whenever the packet is forwarded by a router the TTL value is decremented by 1.

- when TTL become 0 , then next router will drop it .

- ICMP will take the source IP from the dropped packet and informs to source by sending "time exceeded message".

Protocol Field -

- It indicates type of application of which the packet belongs to.

* IP protocol is a connection-less, unreliable and best effort delivery protocol. i.e IP doesn't provide error control.

↳ From end-to-end TTL value will change for a packet or a fragment at every hop (next router).

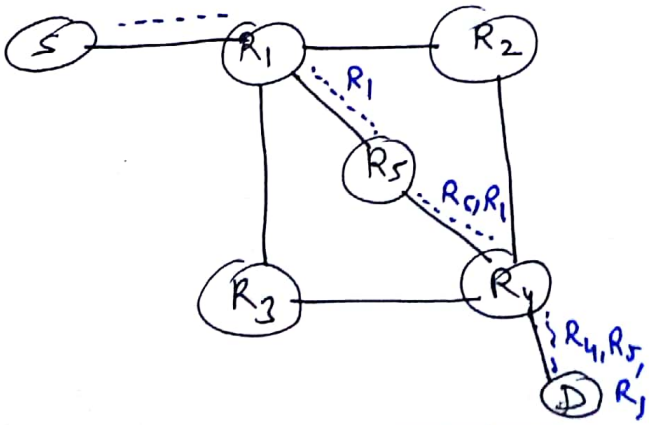
Header Checksum -

- It is provided only for the header because for the data error control already provided by TCP in Trans-port layer, and processing time at router is less so forwarding time will less.

- IP header is provided a checksum so that packet will reach correct destination if it reaches.

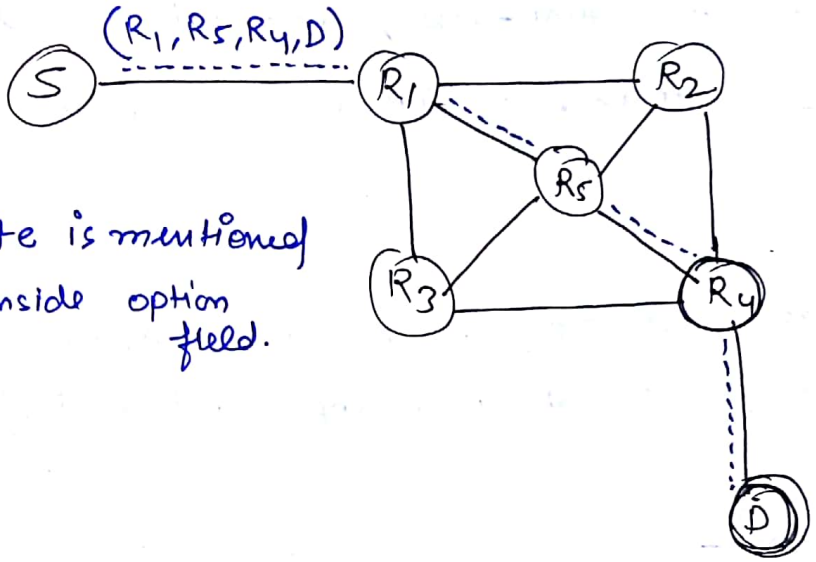
Options & padding

↳ Record route option :-



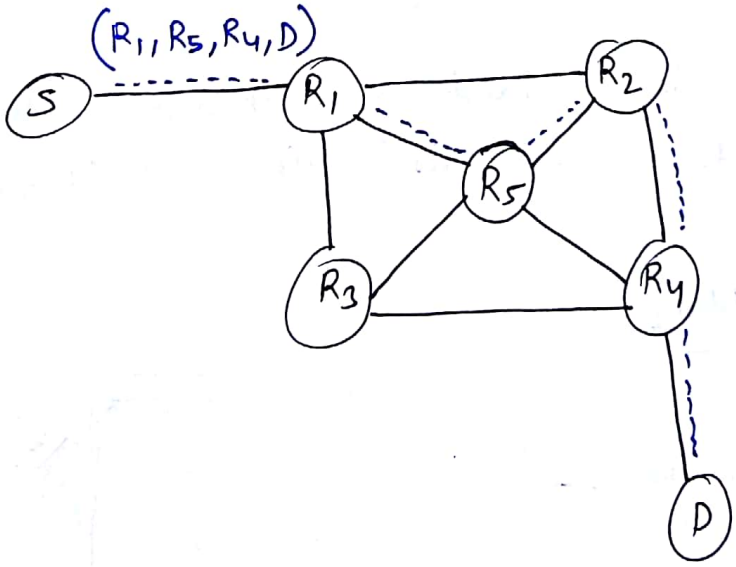
- Record route option is used to trace the path from source to destination.

↳ Source routing option :-



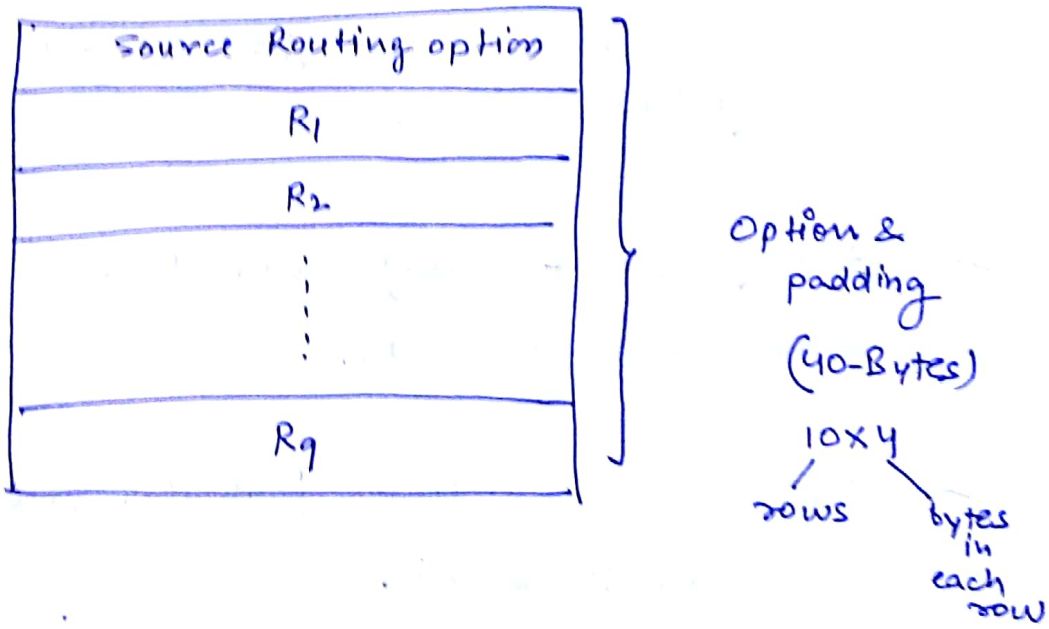
* route is mentioned inside option field.

- If the packets are strictly following the path i.e specified by the source, it is known as strict source routing.



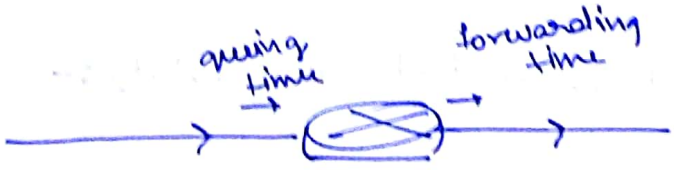
- Along with the path i.e mentioned by the source, if some other paths are visited, then it is known as Loose source routing.

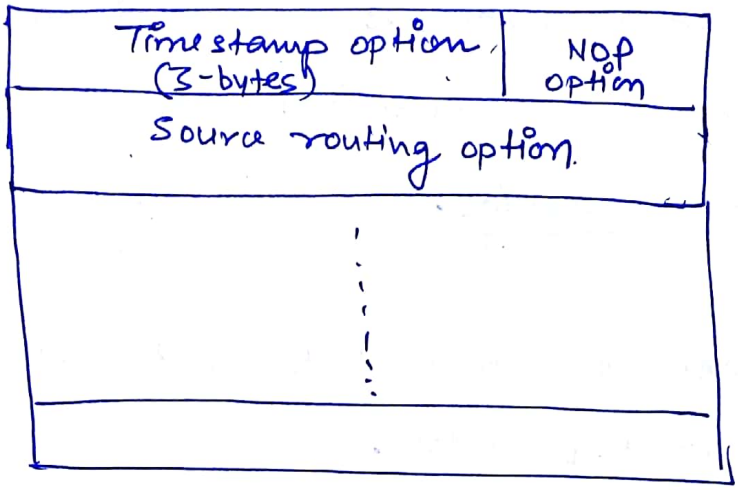
- Maximum 9 intermediate addresses can be used by source routing option.



↳ Timestamp option :-

- It is used for calculating the processing time of the router for the packet.





- NOP option is used to fill the gaps b/w options. It is (1-Byte option).

- EOP (end of option) is used as a separator b/w header and the data.

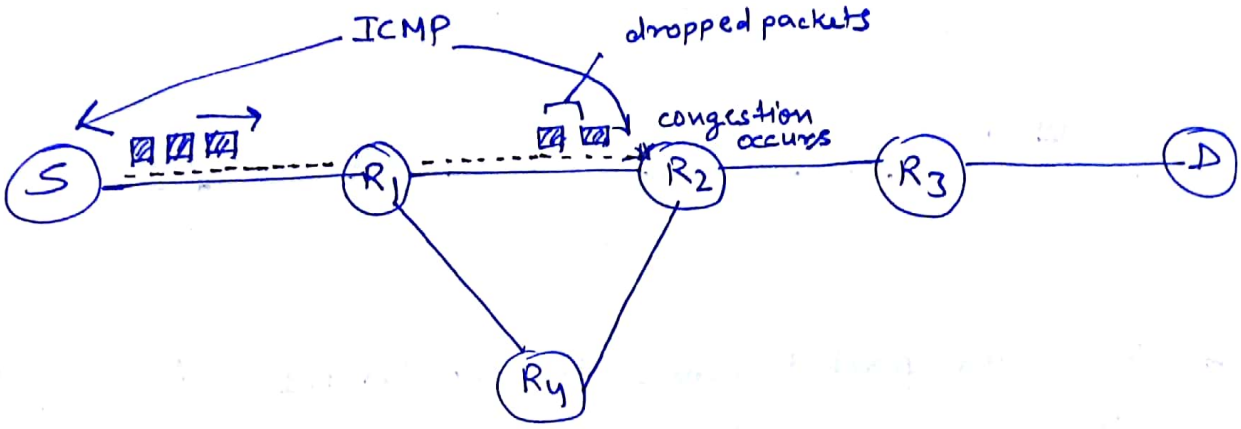
- Packets coming from a particular source can be identify by source IP address.

- Packet can be uniquely distinguished from a particular source with the help of source IP + identification number.

Internet Control Message Protocol (ICMP):-

↳ Reporting ~~massag~~ errors and management queries.

Source quench message :-



- if due to some problem let R_2 queue is completely filled due to more no. of packet coming in less time, then router buffer ~~is for~~ will fulled i.e router is congested. Then some packets are dropped.

- ICMP will came into existence, it take Source IP add from dropped Packets and informs to source by sending this message so that source can lower its transmission rate and hence congestion is resolved.

- If congested 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.

Parameter problem :-

- As data packet came to router R_1, it calculates its checksum and compare it with checksum inside IP header.

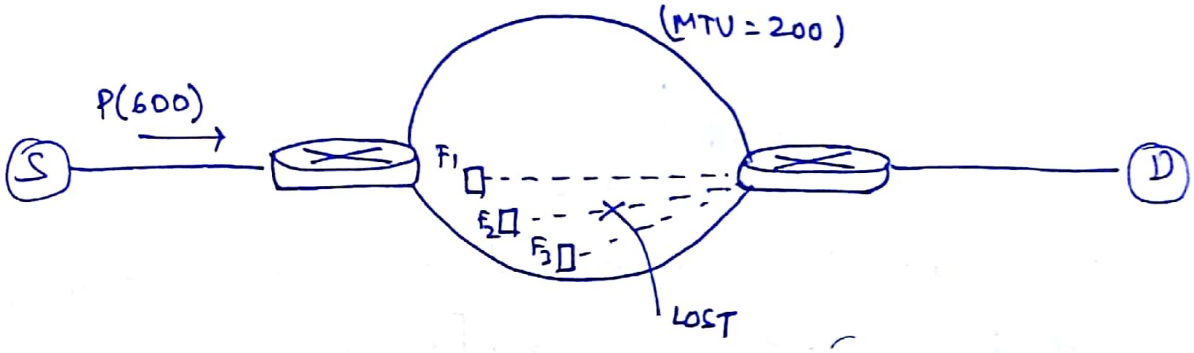
```
If ( checksum are same )
{
    packet accepted;
}
else
{
    packet rejected;
}
```

- When packet is dropped or rejected then ICMP sends msg "Parameter Problem" to source IP address.

- Reason for checksum mismatch can be due to noise modulation or by hacker.

* Checksum is calculated and updated in IP header at each router, as TTL value is changed at every node.

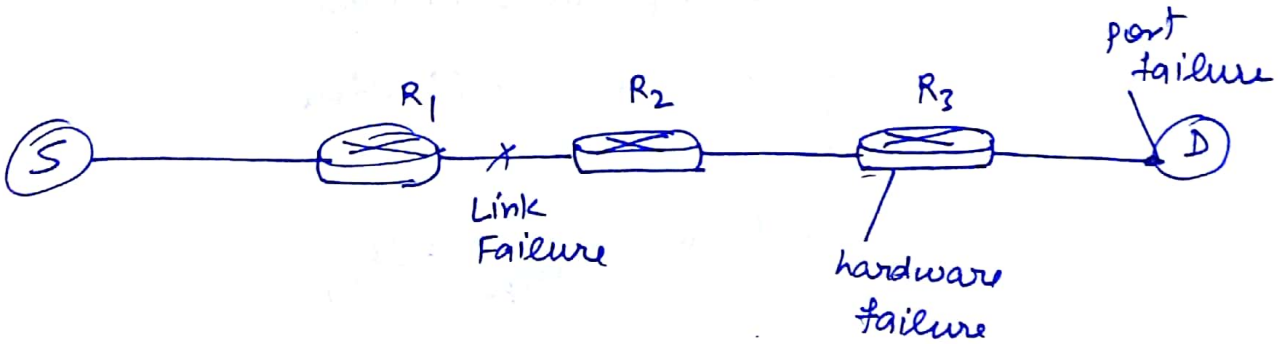
Time exceeded msg :-



- when some fragments are lost in a network then the holding fragments will be dropped.

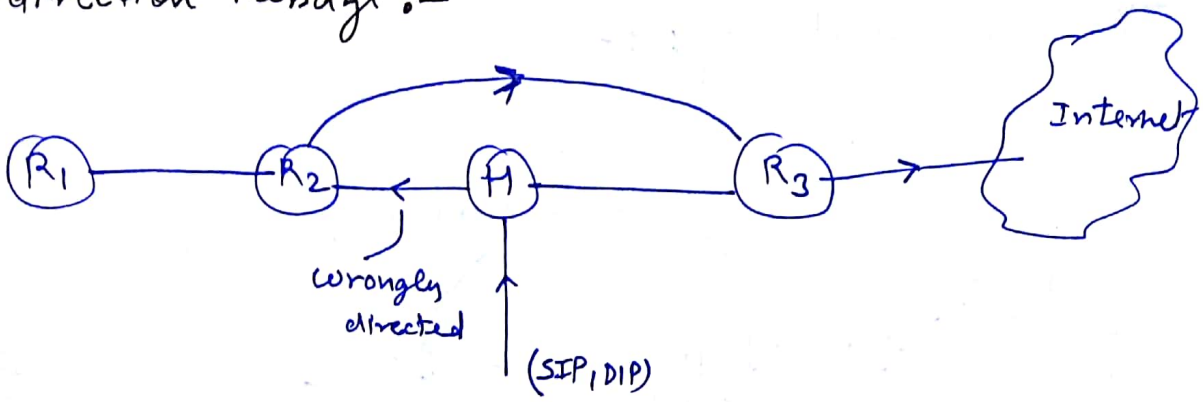
- Then ICMP will take the SIP from dropped packet & inform to source by sending "Time exceeded msg".

Destination unreachable :-



- ICMP error messages are transmitted not only by mediating routers, also by the host.

Redirection Message :-



- whenever a packet is forwarded in wrong direction, later it is redirected in correct direction then ICMP ~~decode~~ will send redirection msg to update it with correct entries.

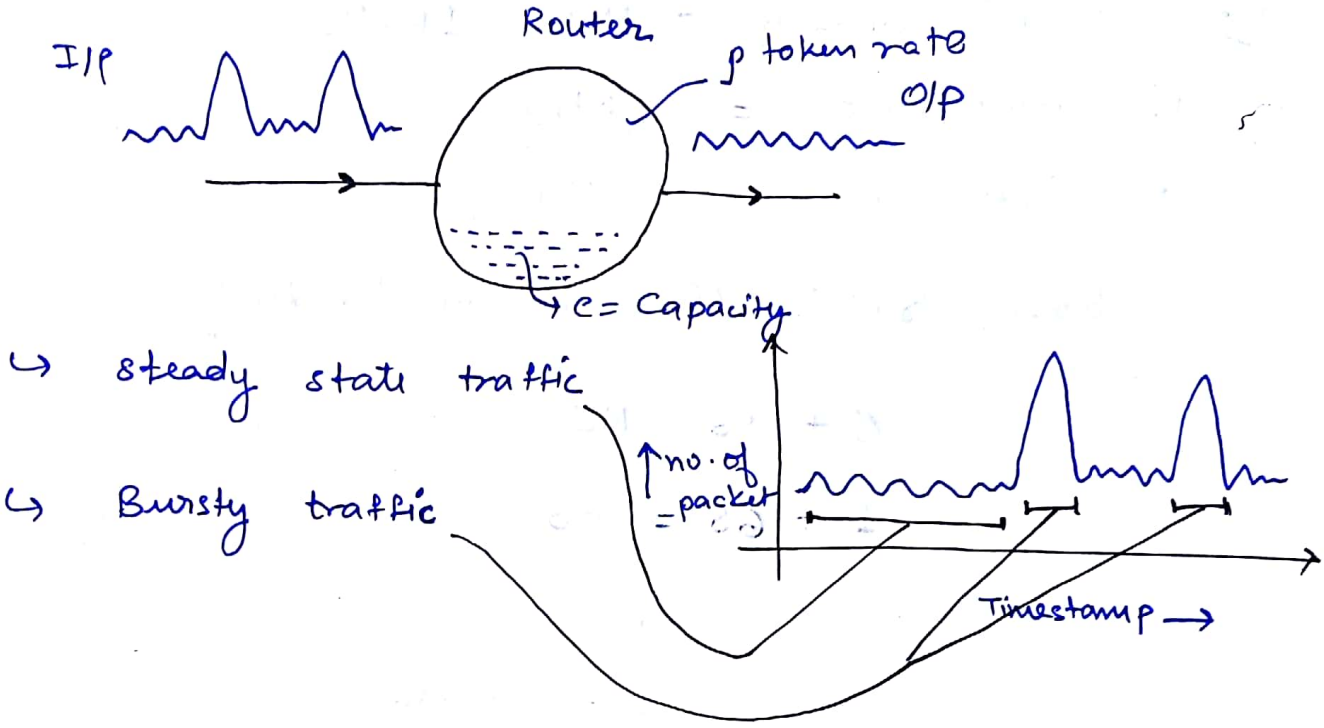
ICMP$_{v4}$ —helps→ IP$_{v4}$

- neighbour solicitation
- router solicitation

ICMP$_{v6}$ —helps→ IP$_{v6}$

- Whenever PROTOCOL field number is 1 then it is treated as the ICMP packet.

Traffic Shaping :-



- When the input traffic is in a steady state or bursty state, but the output rate remains constant state, then router achieved traffic shaping.

- If initial capacity is less then more tokens are generated, so more amount of data is forwarded, but total data is always constant.

$$C + S\rho = MS$$

- If initial capacity is more then less token's are generated so less amount of data is forwarded but total amount of data is same.

Q: Initial capacity = 1 Mbits

M Output rate = 8 Mbps

ρ Token rate = 6 Mbps

Bursty traffic time it can handle?

$$C + \rho S = MS$$

$$1 + 6S = 8S$$

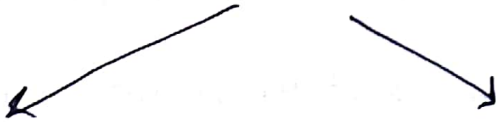
$$2S = 1$$

$$S = 1/2 = 0.5 \text{ sec}$$

Load Shedding :-

- It is a way of loosing packets, when packets can't be handled by router.
- Application like FTP, preference is given to old packets.
- Application like Multi-media preference is given to new packets.

Routing algorithm :-



Static algorithm

- don't consider load on network

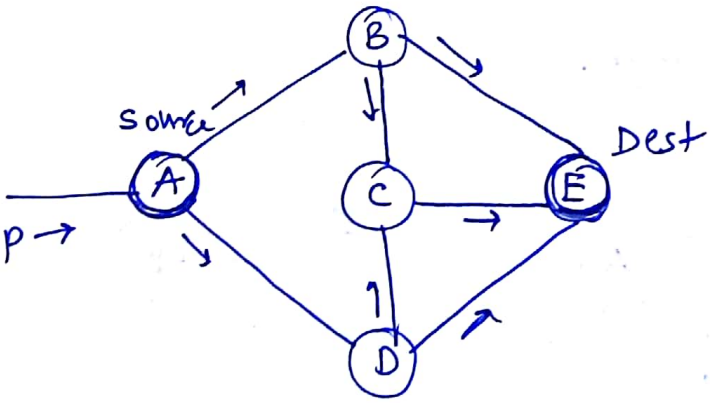
eg - flooding

Dynamic algorithm

- consider Load on network (adaptive algo)

eg - distance vector routing, link state routing, path vector routing.

Flooding algorithm :-



ABE → 2hops
ABCE → 3hops
ABCDE → 4hops

ADE → 2hops
ADCE → 3hops
ADCBE → 4hops

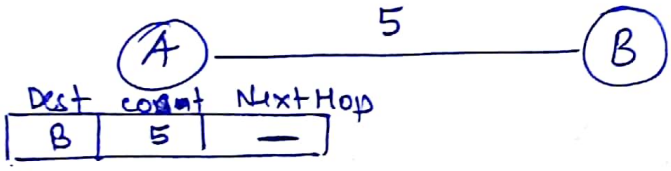
- whenever a packet comes to router, it will divert in all direction except point of origin.

- It is used to find out unknown destination i.e logical address will be known but Physical location of the system is not known.

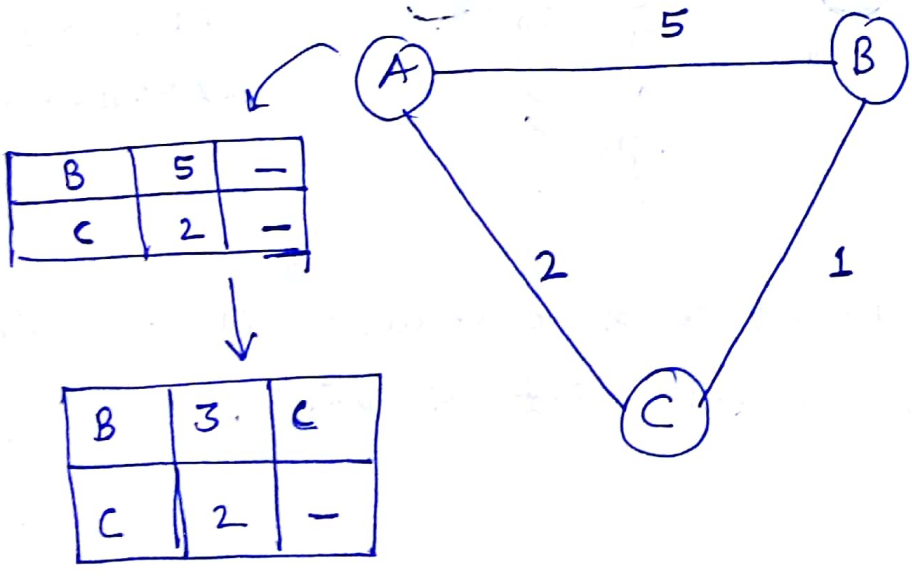
- Flooding creates redundant packet which may lead to congestion.

Distance vector routing :-

- Initially the routing table of a router is empty.



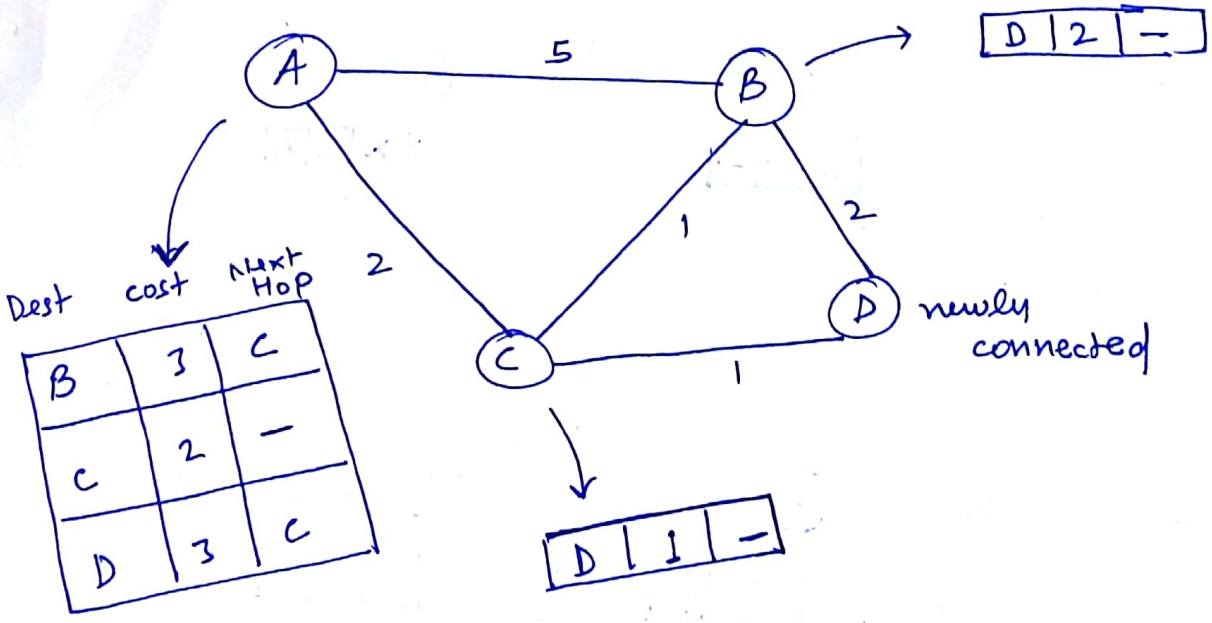
- Every router will be knowing the information of directly connected routers without applying any routing algo.



- whenever packet comes to router the neighbouring routers will give there vector tables and those table will be considered if the distance is less than exisiting distance.

- In this routing every router will get the ~~per~~ complete information of the network only with the help of neighbours.

- Once the router knows the complete information of the network. It is treated as converge or stable.

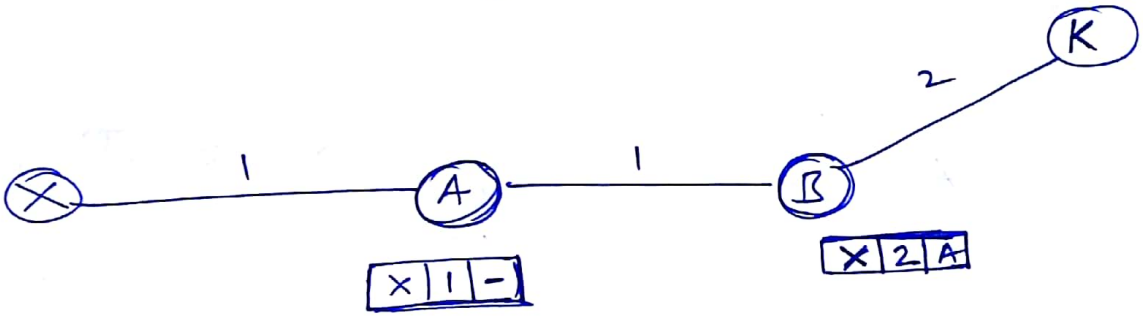


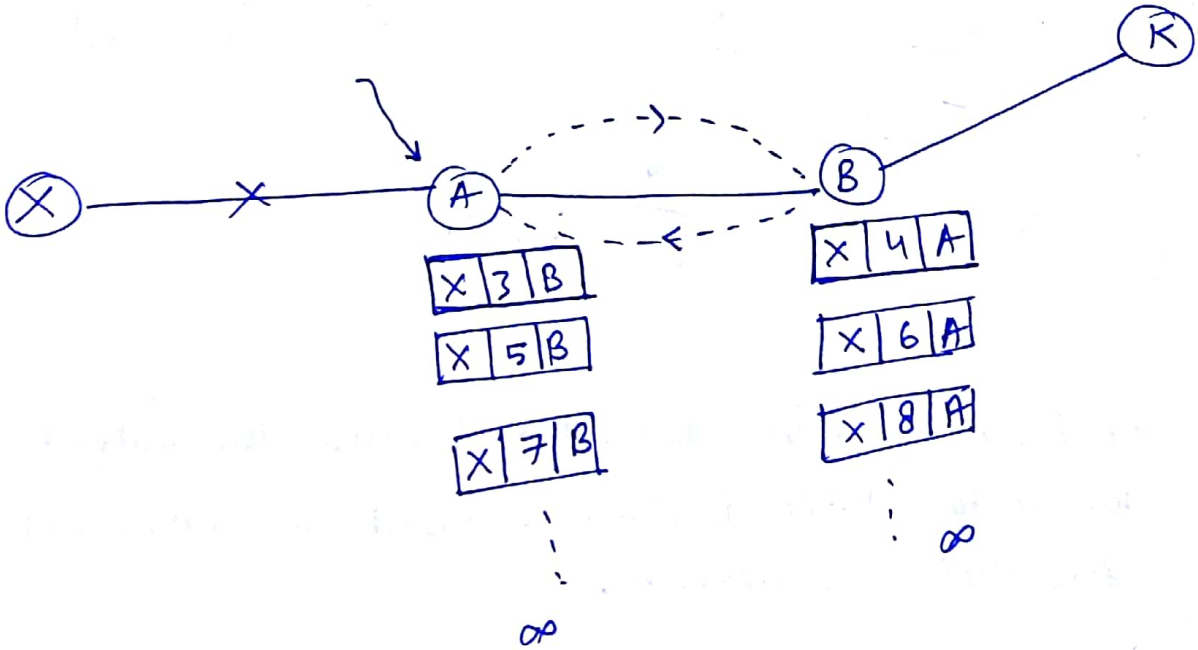
- It is a iterative algorithm because the output of the vector table is given as input for other routers for their calculation.

- It is also known as distributed algorithm, because the routing ~~algorithm~~ tables are updated one-by-one at every router.

- It is also known as the asynchronous algo, because the router knowing the information about a node with the help of neighbouring nodes at different time.

Count - to - infinity problem -

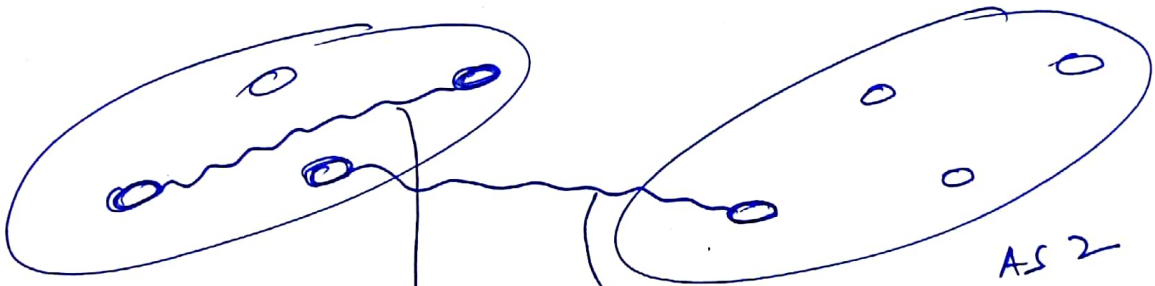




- Whenever links are broken there might be a chance that routing tables are filled with wrong values.

- These wrong values are given as input for other routers, than that router are also filled with wrong value. Finally the network will collapse.

- Data Packet will only rotate for finite amount of time ~~with~~ due to TTL value. So there is no real problem for Data Packets. The main problem is with the routing tables.



Autonomus system |

Intra - domain routing protocol

eg:- RIP, OSPF

RIP → routing into protocol

OSPF → open shortest path Forwarding

distance - vector routing ~~protocol~~ algo

Link-state routing algo

Inter domain Routing Protocol

eg:- BGP

Path vector routing algo