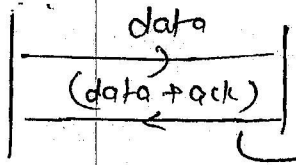


Half duplex

Piggybacking

Dated 15/06/2014

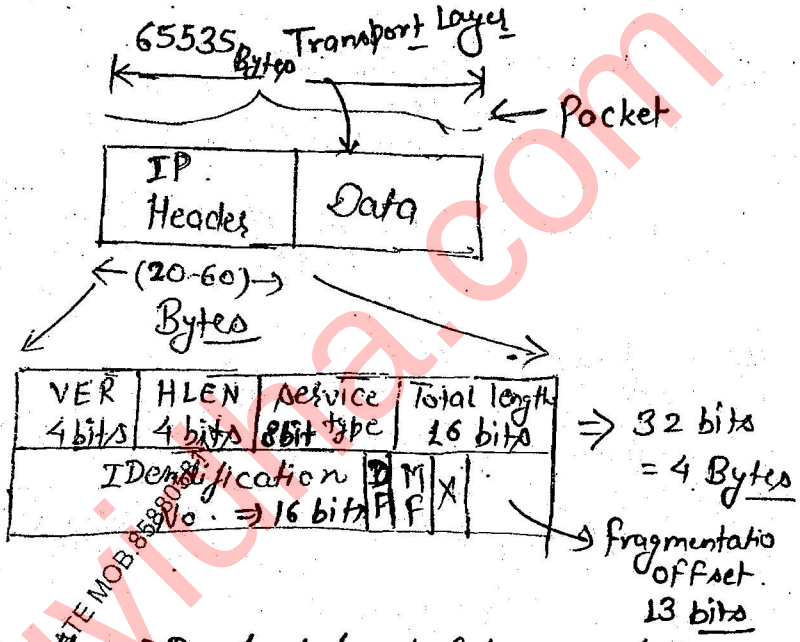
Network Layer :-

IP Protocol :-

'version' :-

0100 ⇒ IPv4

0110 ⇒ IPv6



* The starting 4 bits of the IP packet decides whether the packet is IPv4 or IPv6.
* other than these two possibilities, If the packet come to the routes the packet will be discarded.

0000
0001
0010
0011 } X (Don't cares)

0100 ⇒ 4 rows * 4 bytes = 16 Bytes X

0101 ⇒ 5 rows * 4 = 20 Bytes

0110 ⇒ 6 rows

:

1111 ⇒ 15 rows ⇒ 15 * 4 Bytes = 60 Bytes.

(20-60) Bytes ← Range

(1) HLEN = 1010

Size of Header = 10 * 4 Bytes = 40 Bytes ← Header Size

★ HLEN (Header LAN) indicates the size of the header that is available in the packet.

★ Service type is going to indicate the type of service that is provided to the packet by the Router.

① Total Length bits :

= 0000000111111111

⇒ Size of the packet :- 511 Bytes ↙ Size of packet

② HLEN = 1001

Size of Header = 9 * 4 = 36 Bytes

Header + Data = packet

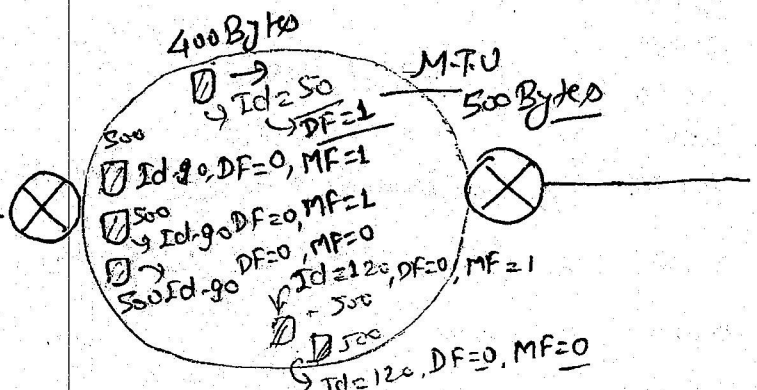
36 + 512

36 + x = 511

x = 475 Bytes ↙ Data Size

★ If Both Total Length and Header Length is given, we can calculate, size of the data.

★ Identification No :- (16 bits)



Note :-

★ fragments belonging to same packet will be given same Id. No. so that the destination Router can eaily Combine the fragments belonging to same D...

DF :- Do not fragment or

If DF = 1 → Packet

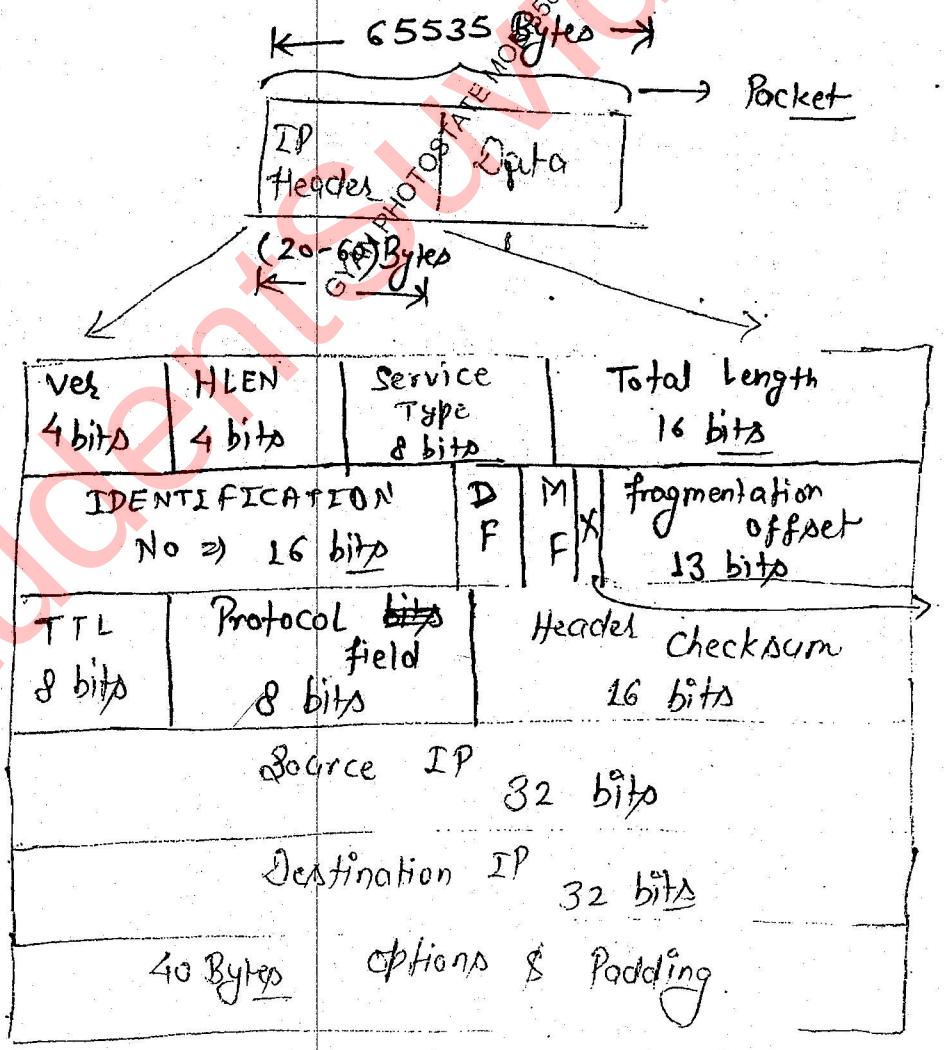
If DF = 0 → fragment

★ 'DF bit' indicates, whether the content is packet or fragment.

★ All Intermediate fragment, starting from '1', 'MF' value is 1. specially for the last fragment MF value is '0'.

★ for the packet MF value always be 'zero' (0)

★ 'Fragment OFFset' indicates the size of the fragment and also the position of fragment in the packet.

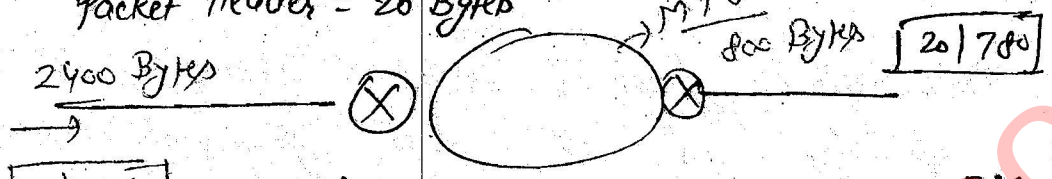


U.J value

20 | 976		20 | 976		20 | 776		20 | 56
offset							Padding bits
122 x 8	1 offset	0 - 121		122 - 243		244 - 365	366 - 372
976	21					121	
976 x 3						364	
2928							
2980 - 2928							
52							

(0, 122, 244, 366)

(4) Packet Header = 20 Bytes



20 | 2380

$\frac{2380}{780} = 3.05 \simeq 4$ fragments

97 × 8 = 776

$\frac{780}{8} = 97$

	1st fragment	2nd fragment	3rd frag.	4th fragment
Id	50	50	50	50
DF	0	0	0	0
MF	1	1	1	0
fragment values	20 | 97	20 | 97	20 | 97	
	20 | 776	20 | 776	20 | 776	20 | 56
fragment offset	(0-96)	(97-191)	(192-287)	(288-294)
	(0, 97, 192, 288)			

52 + 4 → Padding bits

Que :- Given fragments are 0, 60, 120, 180 (LL)
IP- Header is 20 Bytes.
All fragments are of equal size then calculate the packet size :-

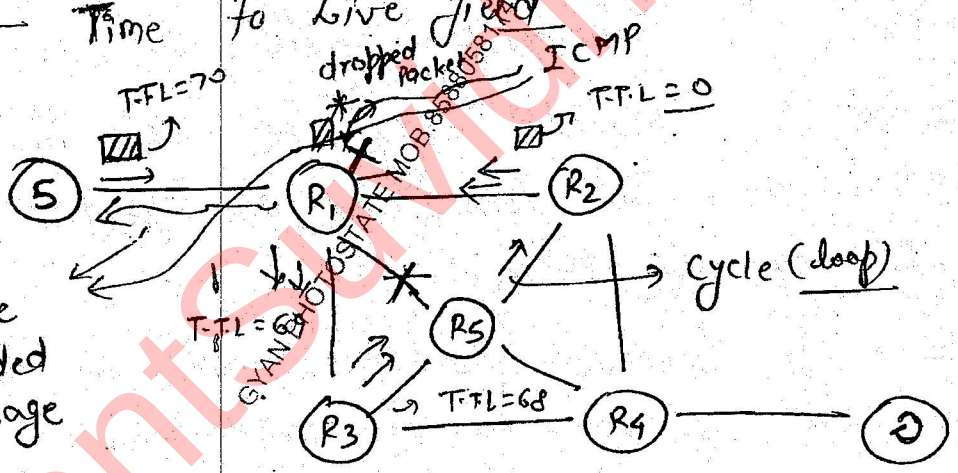
0-59, 60-119, 120-179, 180-239

60×8 = 480

[20|480] [20|480] [20|480] [20|480]

480×4 = 1920 ⇒ [20|1920] ⇒ Packet size = 1940 Bytes
Packet

★ TTL :- Time to Live field



★ The purpose of T.T.L is to identify, If any loop will exist for the packet or not.
★ whenever the packet is forwarded by a router, the T.T.L value is decremented.
★ whenever the link is broken, there is a chance, that packet might be forwarded in the wrong path.
★ whenever the packet is in a loop, at one point of time, T.T.L. value will become 'zero' then the Next Router will drop the packet.

★ ICMP will [illegible] packet and inform to source by sending "time-exceeded message".

★ "Protocol field" :- is going to indicate the type of application of which, the packet belongs.

★ "IP Protocol is a connection-less, unreliable, Best effort delievery protocol."

★ IP doesn't provide any error control.

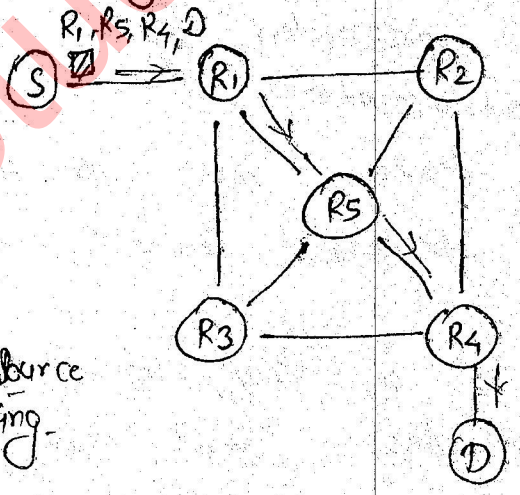
★ Header checksum is only provided for the Header because for the data, it is already provided in Transport Layer by TCP protocol

★ checksum is provided only for the Header, so that processing time is less and the packet is forwarded fastly by the Routers.

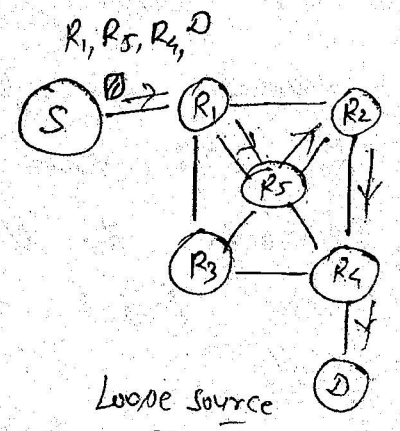
★ Checksum is provided for the header, so that the data will go to correct destination.

★ Options & padding :-

★(i) Source Routing option :-



Strict source Routing.

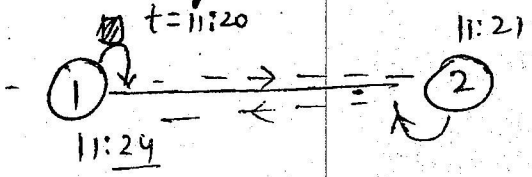


Loose Source Routing.

* "The packet strictly following the path, that is specified by the source. It is known as 'Strict Source Routing'.

* Along with the path that is specified by the source, If some other paths are visited by the packet, It is known as 'Loose Source Routing.'

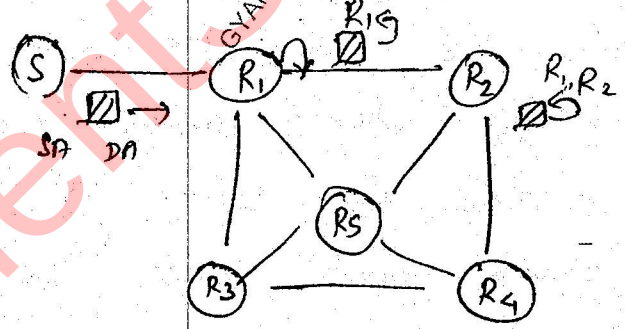
*(ii) time-stamp option :- (3 Bytes)



→ 11:24 - 11:20 = 0.04 → R.T.T.

* time stamp option is used for calculating Round trip time (R.T.T) between two end systems.

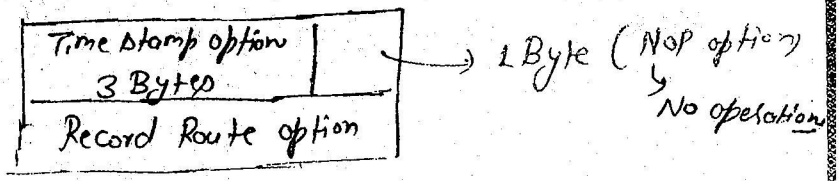
*(iii) Record-Root option :-



* whenever Record-Root option is used, then the packet will record the ~~root~~ route of different routers, once it reaches to destination.

*(iv) NOP option :- (1 Byte)

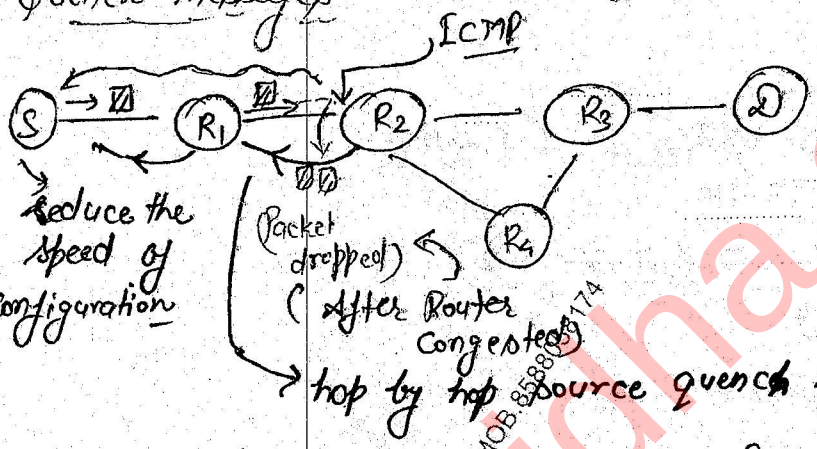
* NoP option is used to fill the gaps between the options.



End of option is used as the seperator between data and Header.

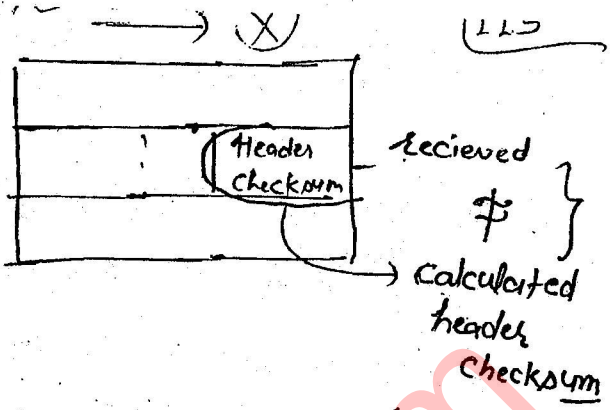
* ICMP (Internet control message protocol) :-
  - ↳ reporting errors and management queries

(i) Source Quench messages :-



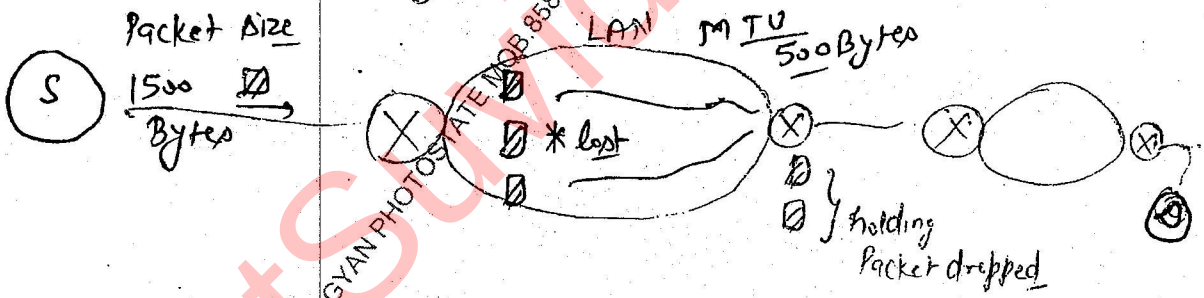
* When more number of packets coming in less time the router will be full in no time. then the router is congested., some packets will be dropped.
* ICMP will take the source IP and inform to source by sending 'source quench message.' then source will reduce the speed of transmission then the congested 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 reduce the speed of transmission.

(ii) Parameter Problem :-



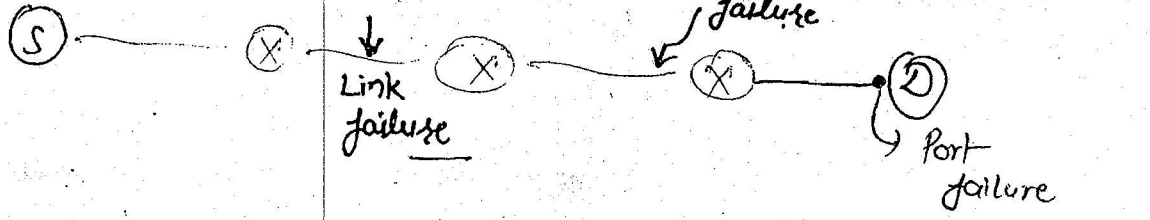
* once the data is transmitted, header bits are modified by the noise then the calculated Header checksum will not be equal to recieved header-checksum then the packet is dropped.
* ICMP will take the Source-IP and inform to Source by pending 'Parameter Problem' message.

(iii) Time Exceeded Message :-



* when some fragments are lost the Network then the holding fragments will be dropped by the router.
* ICMP will take the Source IP from the dropped fragment and informs to Source by sending, Time exceeded message.

(iv) Destination unReachable :-



$500 + 100 = (100 + 500)$

$100 + 500 = (500 + 100)$

(1) output rate = 8 Mbps

token rate = 6 Mbps

Initial capacity = 1 M bits

Burpty traffic time = ?

$C + Ss = MS$

$10^6 \text{ bits/sec} + 6 \times 10^6 \times S \text{ sec} = 8 \times 10^6 * (S \text{ sec})$

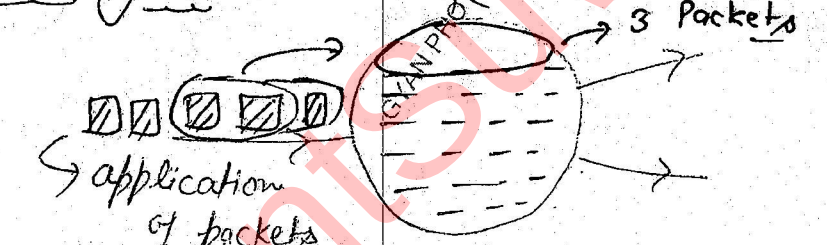
Steady state
or
S = Burst traffic time

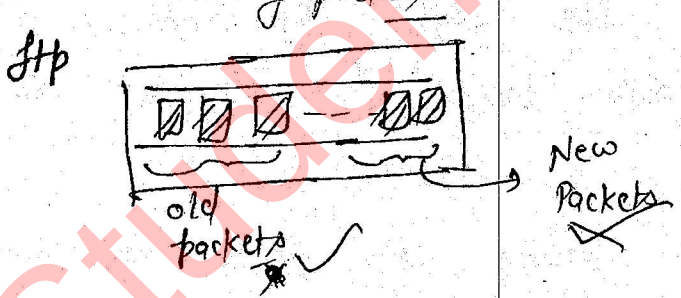
$10^6(1 + 6S) = 8 \times 10^6 S$

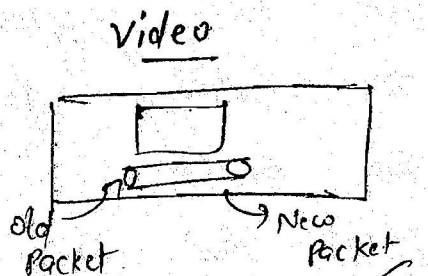
$1 = 2S$

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

Load Shedding :-





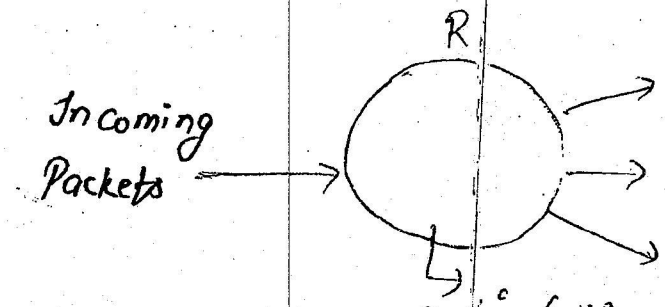


* Load shedding is a way of dropping packets when the packets can not be handled by router.
* Applications like FTP presence is given to old packets.

given to new packets.

This concept is also called milk & wine concept.
↳ New ↳ old

⇒ Routing Algorithms :-



→

(i) Static Algorithms :- does not consider the load on network ("Non-adaptive algo")

Ex:- flooding algo.

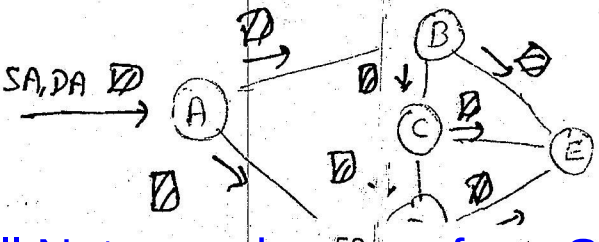
(ii) Dynamic Algorithms :- consider the load on network (Adaptive Algorithms)

Ex:- i) Distance vector Routing algo.
ii) Link state routing algo.
iii) Path vector Routing.

Flooding :-

Flooding is defined as "whenever a packet comes to router, it is diverted in all directions except the point of origin."

* flooding creates redundant packets.



ii) Calculate No of possible paths from A to B using flooding algorithm, using hop as a metric.

ABE ⇒ 2 hops
ABCE ⇒ 3 hops
ABCDE ⇒ 4 hops
ADE ⇒ 2 hops
ADCE ⇒ 3 hops.
ADCBE ⇒ 4 hops

* Drawback of 'flooding' is it creates redundant packets which may lead to Congestion of the Router..

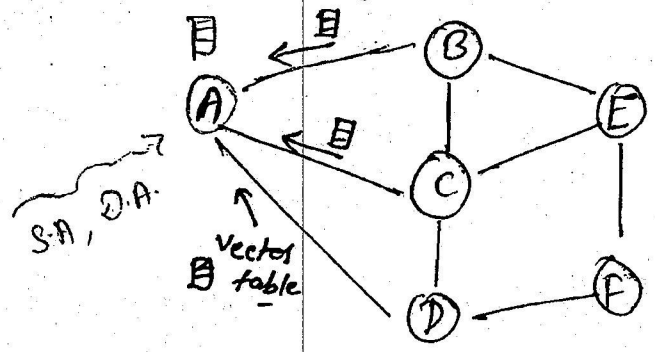
* Advantage of flooding is It creates redundant packets, to find the unknown destination.. (logical address will be known but physical address can't be known, so to identify that flooding is used.)

* Dynamic Algorithms :-

* The path of a packet will change when New links are added or the existed links are broken, for the same destination.

* The Routing table of the routers should be updated then only path can be changed.

:- Distance Vector Routing Algorithm :-



★ "Whenever a packet comes to router, the neighbouring routers will give their vector tables then a new vector table is calculated for that node to forward the data."

★ It is also known as 'Iterative algorithm' because the output of the vector table is given as input for other routers for their calculations.

★ It is also known as distributive algorithm because the routing tables are calculated for every node wherever the packet comes.

★ It is also known as "Asynchronous algorithm" because Routers are giving their vector tables at different instance of time. (possibly with a time difference).

Qu:- vector ~~delay~~ table of B = (A B C D E F
7, 0, 4, 3, 1, 2)

vector table of C = (2, 3, 0, 5, 4, 3)

vector table of E = (3, 4, 5, 0, 5, 6)

measured delay (metric) of A to B, C, D are 4, 2, 3

vector table of ...

:- vector table of A via B = (A B C D E F
11, 4, 8, 7, 5, 6)

AA = AB + BA
= 4 + 7 = 11

AB = AB + BB
= 4 + 0 = 4

AC = AB + BC
= 4 + 4 = 8

AD = AB + BD
= 4 + 3 = 7

AE = AB + BE
= 4 + 1 = 5

AF = AB + BF
= 4 + 2 = 6

:- vector table of A via C := A to C delay = 2

A B C D E F
(4 5 2 7 6 5)

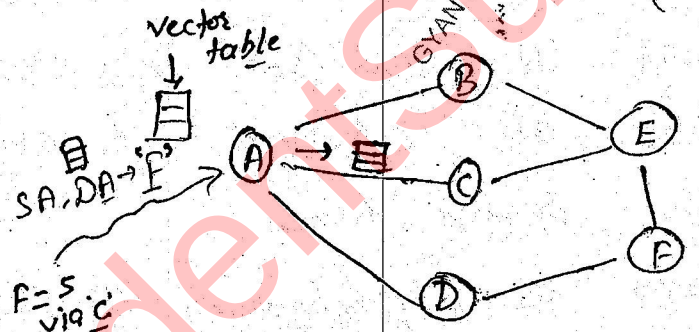
AA = AC + CA
= 2 + 2 = 4

:- vector table of A via D :-

A to D delay = 3
(6, 7, 8, 3, 8, 9)

:- final vector table of A

A B C D E F
(0, 4, 2, 3, 5, 5)
self
= (_, B, C, D, B, C)
via values



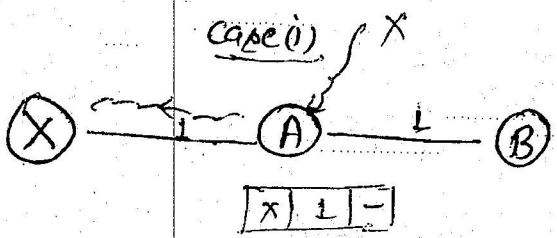
Note :- ★ Distance vector routing will work fine, whenever there are no breakages of the link.

★ whenever the link is broken, the packets will be routed in wrong direction, then there is a chance of forming a loop for the packet in the Network, this problem is known as "Count to infinity problem".

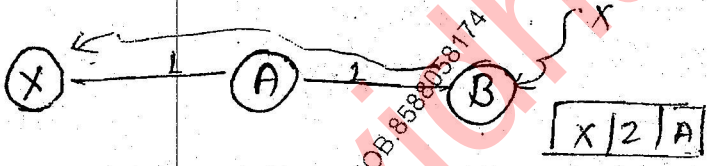
⇒ Count to infinity problem :-

* Every Router initially, the Routing table is empty.
* Without applying any routing algo. every routers will be knowing the information of directly connected routers.

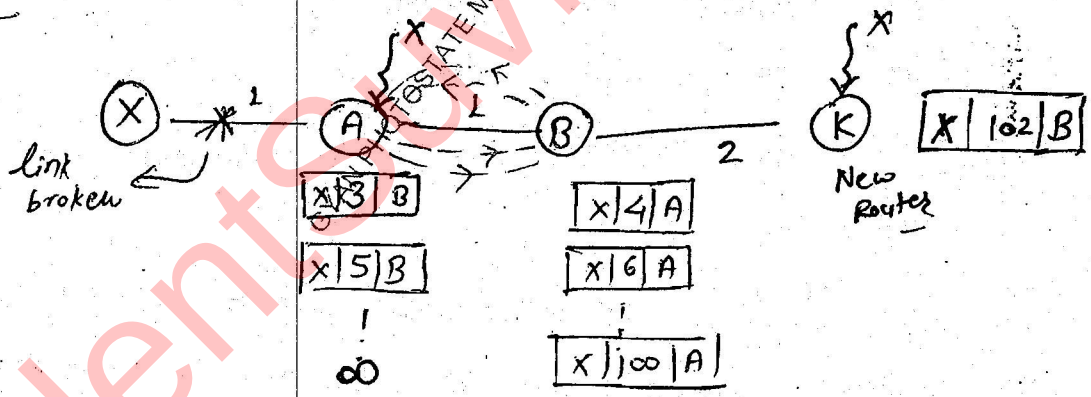
Case-(i) :-



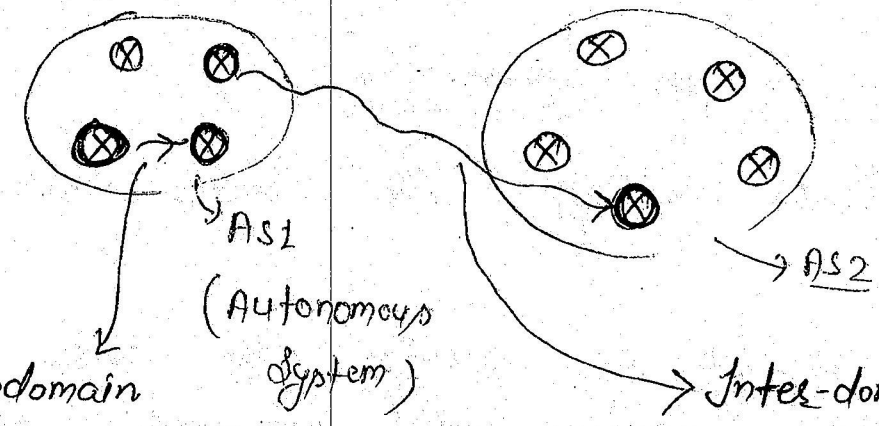
Case-(ii) :-



Case-(iii) :-



* The Drawback of distance vector is count infinity problem i.e. the packet will rotate continuously unnecessarily consuming the resources.
* This problem is not a infinite problem i.e. the packet will rotate in a finite time until T.T.L = 0.



Intradomain routing protocol

Ex: RIP, OSPF

(Routing Information Protocol)

(open socket Path forwarding)

Distance vector routing algorithm

Link State Routing algorithm

Inter-domain routing Protocol

Ex:- BGP

(Border gateway Protocol)

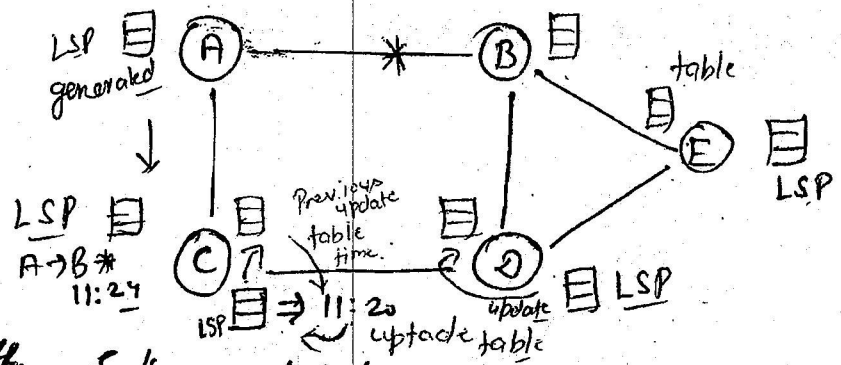
Path vector routing algorithm.

★ If the Packets are routed from a Router, in one autonomous System to a router in the same autonomous System is known as intradomain routing protocol.

★ If the Packets are routed from Router, in one autonomous System to a router in another autonomous System, It is known as inter-domain routing protocal.

:- "Link State Routing Algorithm" :-

★ In distance vector, algorithm is applied on 'data packets' whereas in 'Link state routing', the algorithm is applied on 'control packet' based on that data packets are transmitted.



★ The Entire operation of Link State algorithm is based on LSP Packet.

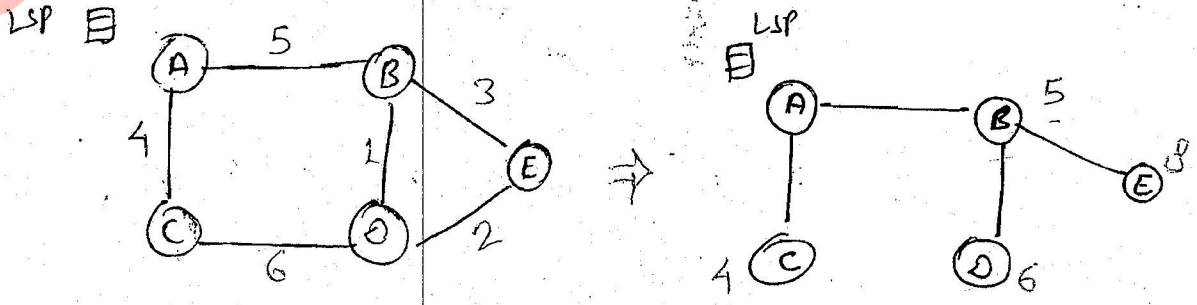
★ LSP packet contains the number of routers, number of links, links up & down, LAN Networks that are connected.

★ The LSP packet is given to all routers with the help of 'flooding algorithm.' so whenever the link is broken it will knowing immidietly to all routers with the help of LSP.

★ LSP packet should be generated periodically with the latest information of the Network.

★ Before applying flooding, graph will be converted into tree using shortest path tree algorithm.

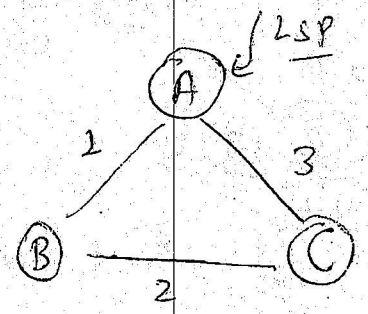
★ Shortest path tree algorithm :-



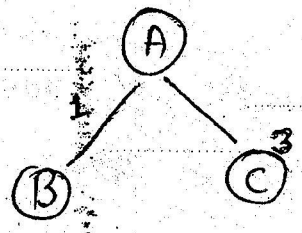
* Router with Lowest Router_id will going to have priority to generate LSP.

Que 2:-

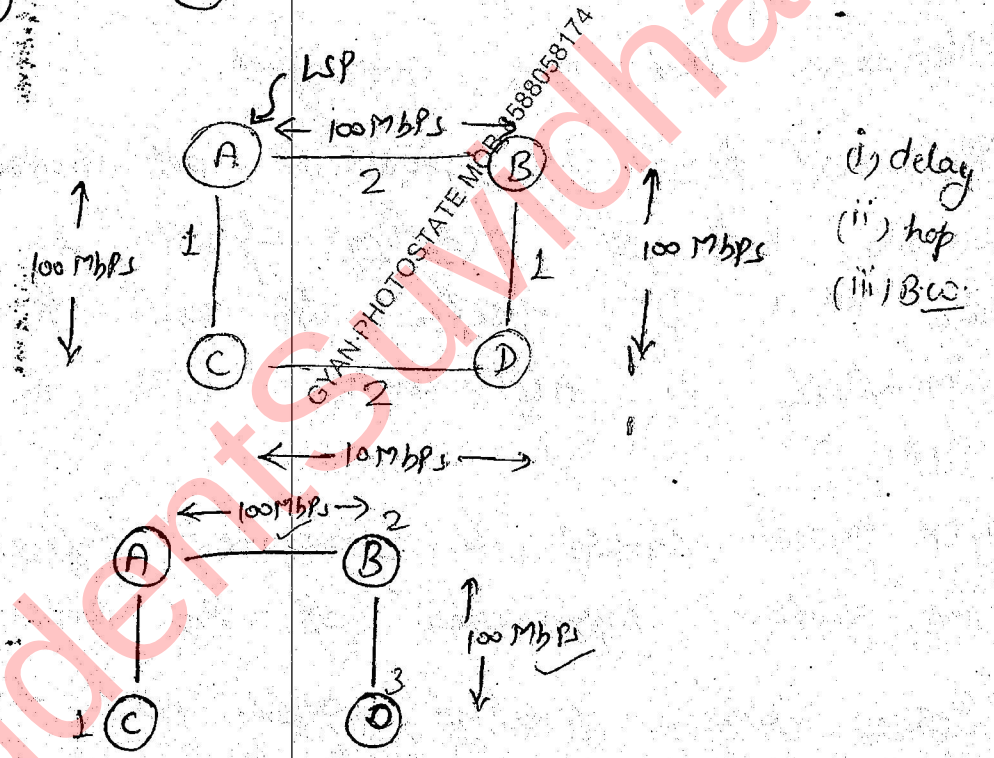
Shortest Path Algo :-



(i) Delay
(ii) Hop



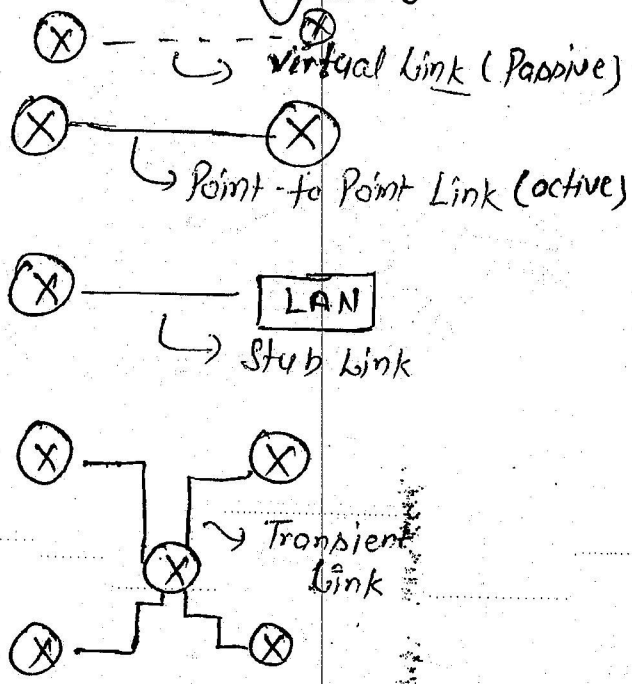
Que 3:-

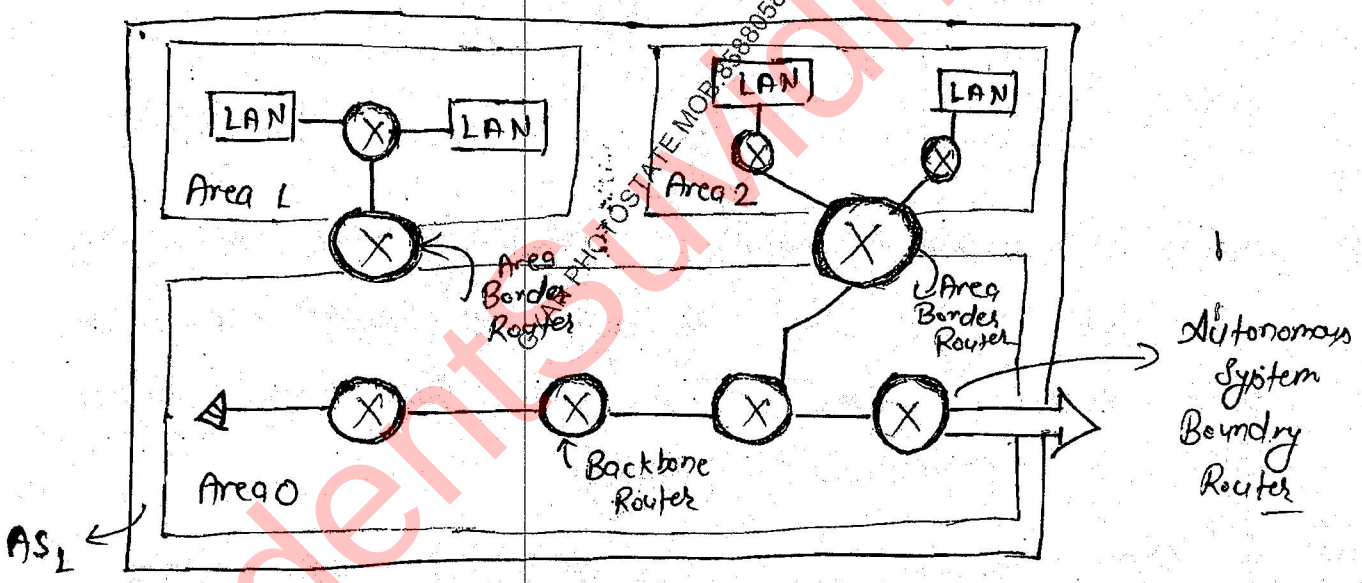


(i) delay
(ii) hop
(iii) Bw.

* Cost & complexity is high in Link state compared to distance vector routing algorithm.

Intra-domain routing

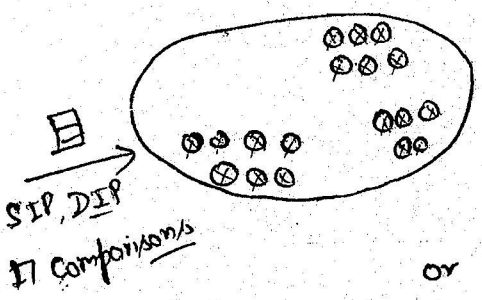




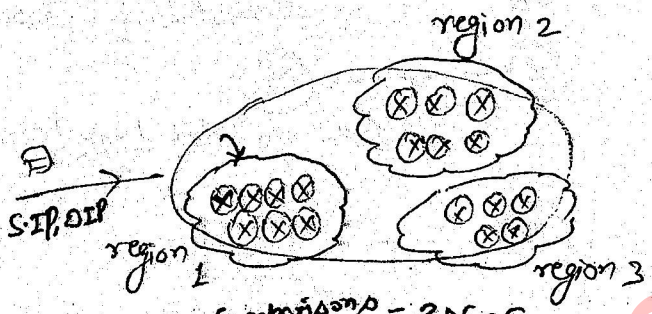
- Area Border Router is used for connecting Area 0 with other Areas.
- Autonomous System Boundry Router is used for connecting different autonomous systems.
- whenever the link is broken, the data is diverted via virtual link to support fault tolerence.
- Out of all areas Area 0 is known as Backbone Area

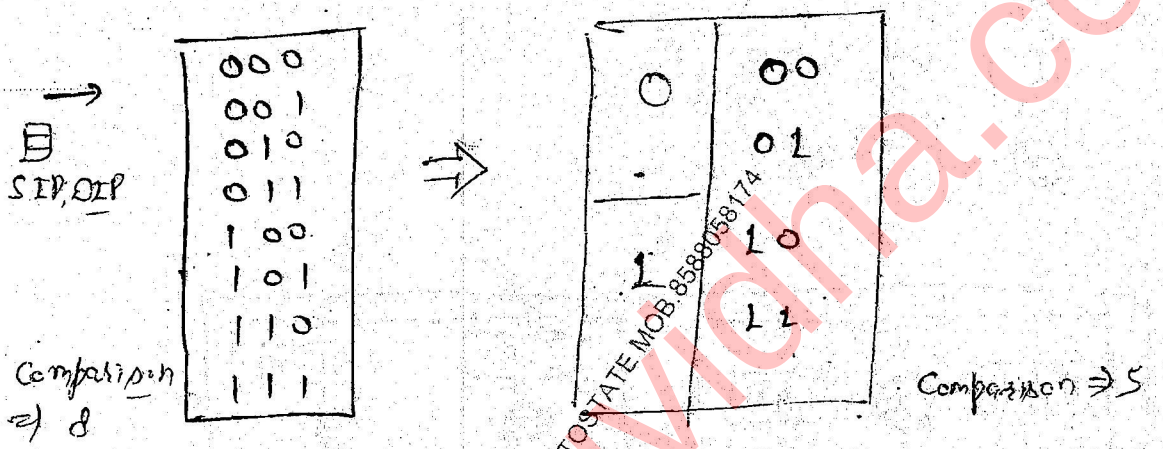
* Area Border Routers internally used hierarchical routing.

* Heirarchical Routing :-



or

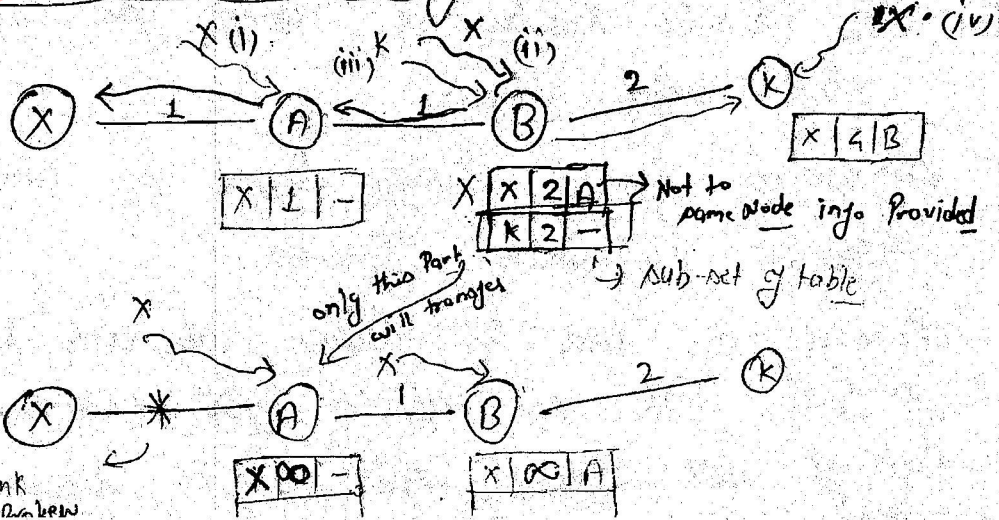




* Using heirarchical routing, physically the table size will not change but logically it will reduce so that searching time will be less and packet will be forwarded fastly.

* Special case :- Distance vector Routing with Split - Horizon

Case-(i) :-



★ There is no count to infinity problem in distance vector with split horizon.

★ whenever a packet comes to a router the neighbouring Router will give only sub-set of the table so that the routes will update with current information.

★ In distance vector routing whenever a link is broken, it will take O(n) {Big O(n)} time to reach the information to every node, so it is a slow convergence algorithm.

★ Link State Routing algorithm is a fast convergence algorithm because whenever the link is broken it will take O(1) time to reach the information in the Network.

Que: An upper layer packet is split into 10 frames, each of which has an 80% chance of arriving undamaged. If No error control is done by Data link protocol. How many times must the message be send on average to get the entire message through.

P → 10 frames → = = ! = → P = 0.8 → 10 frames

Probability of frame reaching safely = 0.8

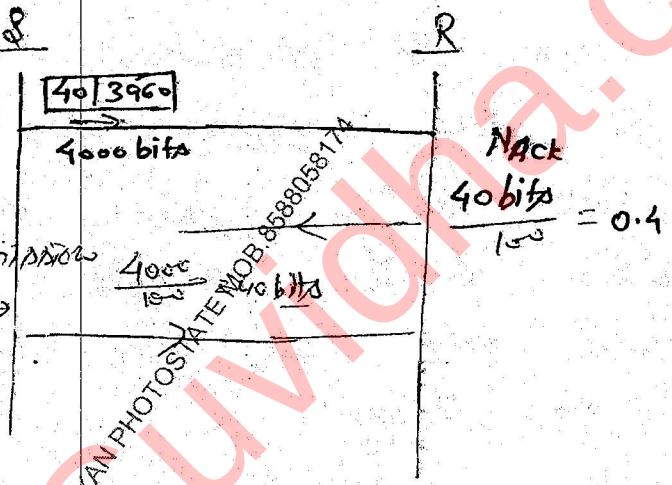
Probability of message reaching safely = 0.8 * 0.8 * 0.8 * 0.8 (10 frames) = $(0.8)^{10}$

mean no of transmissions of a message (data) = $\frac{1}{P} = \frac{1}{(0.8)^{10}} = 9.3$

Q) Calculate the fraction of bandwidth that is wasted on overhead (Headers & retransmissions) with data frames consisting of 40 bit Headers 3960 data-bits. acknowledgment frames never occur. NAck frames are 40 bits, the error rate for the data frames is 1% error rate of Nack is negligible.

:-

Note:- Negative (Nack) ack is applied during error detection policies.



fraction overhead (header + Retransmission)

out of 100 frame

⇒ 1 frame is modified

⇒ 1 Nack = 1 retransmission

so out of 1 frame ⇒ Nack / 400

↳ out of 1 frame → 4000 / 100 = 40

⇒ Total overhead for one frame

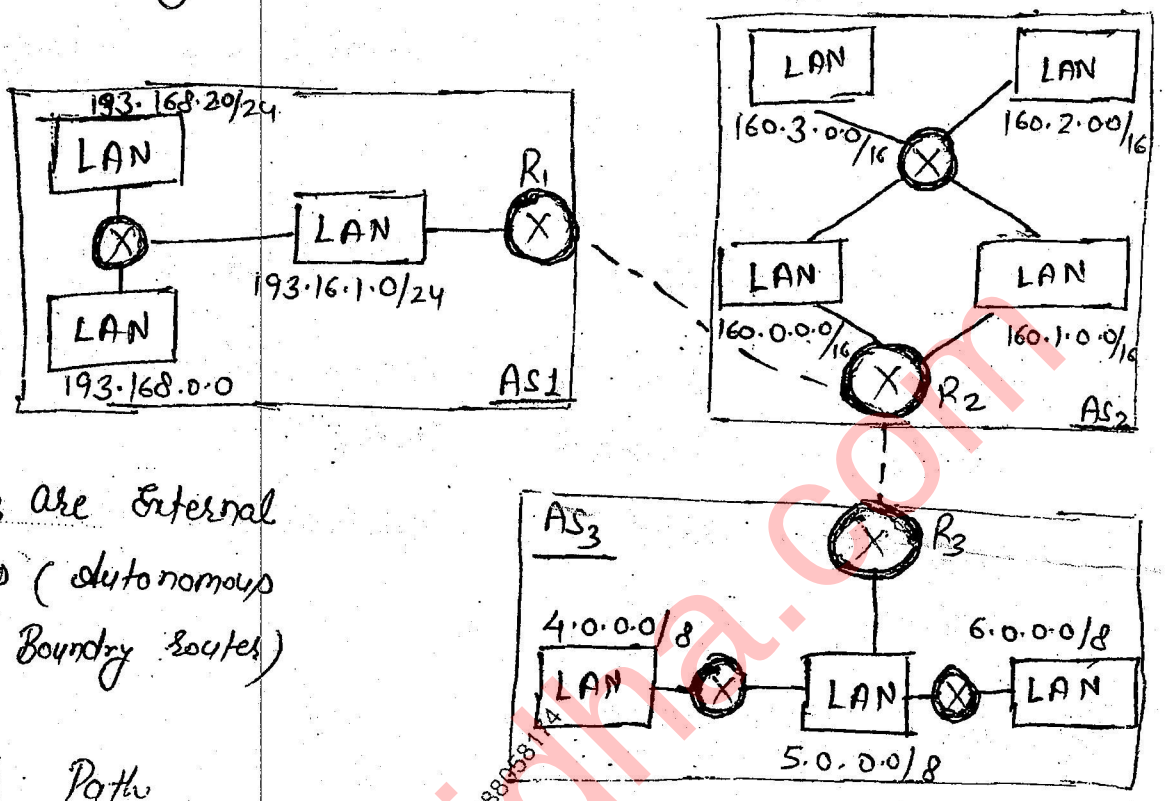
= 40 + 0.4 + 40

= 80.4

fraction of overhead i.e. wasted = 80.4 / (3960 + 80.4) * 100%

= 1.98 ≈ 2% of Bandwidth

Path vector routing (Protocol).



R_1, R_2, R_3 are External Routers (Autonomous System Boundry Routers)

Network	Path
193.168.0.0/24	AS_1
193.168.1.0/24	AS_1
193.168.2.0/24	AS_1
160.0.0.0/16	$AS_1 \rightarrow AS_2$
160.10.0/16	$AS_1 \rightarrow AS_2$
160.2.0.0/16	$AS_1 \rightarrow AS_2$
160.3.0.0/16	$AS_1 \rightarrow AS_2$
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	$AS_1 \rightarrow AS_2 \rightarrow AS_3$

Network	Path
193.168.0.0/22	AS_1
160.0.00/14	$AS_1 \rightarrow AS_2$
4.0.0.0/8	$AS_1 \rightarrow AS_2 \rightarrow AS_3$

193.168.0.0/24

0.0 ⇒ 00000000.00000000

! Supernet bits

000000 00 . 11111111 } 2^8

193.168.1.0/24

1.0 ⇒ 00000001 . 00000000

00000001 . 11111111 } 2^8

193.168.2.0/24

2.0 ⇒ 00000010 . 00000000

00000010 . 11111111 } 2^8

$2^{10} \leq 4 \times 2^8$ ↪ 3

↪ $2^{32-10} = 22$ mask

14th Vector Routing

BGP (Border gateway Protocol)

IBGP (Internal BGP)

EBGP (External BGP)

* IPGP is used for communication between external routes and internal routes.
* EPGP is used for communication between two external routers.

⇒ RARP, BOOTP, DHCP :-