V) Traffic Shapping :-

→ Another method of conjusion control is to ~~shade~~ shape the traffic before it enter the netwoll.

→ Traffic shapping controls the rate at which packets are sent (not just howmany) used in ATM & integrated service network

→ At connection setup time, the sender & ~~recei~~ carrier negosiate a traffic pattern (shape)

→ The two traffic shapping algorithm

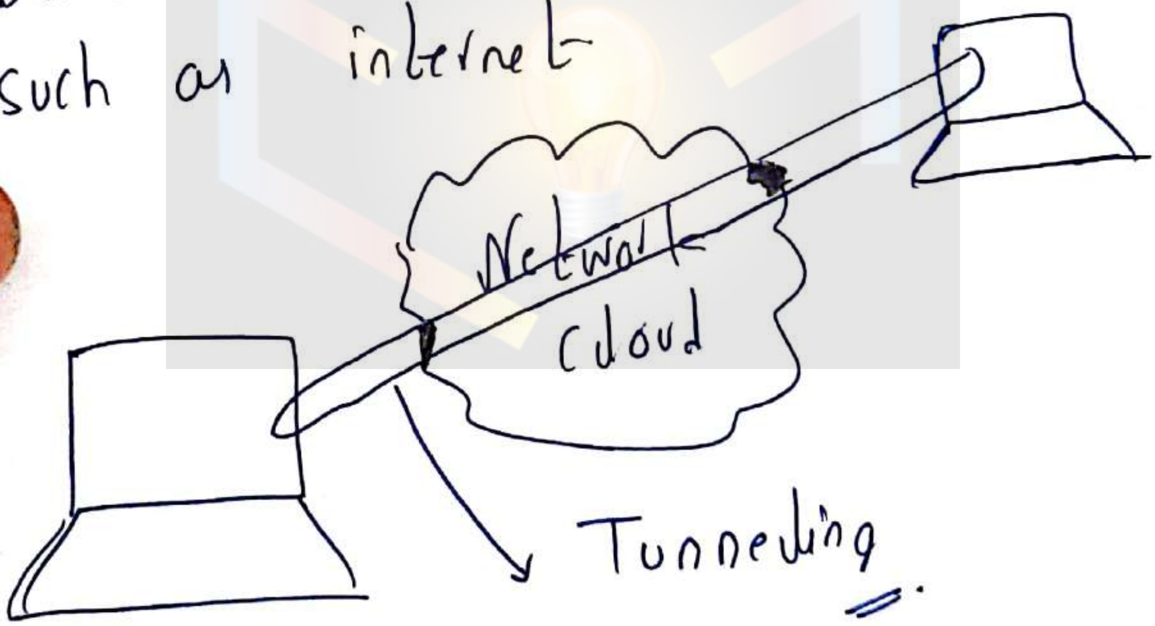
i) leaky bucket
ii) token bucket

10) Tunneling

→ Tunneling is a protocol that allows for the secure movement of data from one network to another.

→ Data packets follow Point to Point tunneling Protocol (PPTP)'s

→ Tunneling involves allowing private network communication to be sent across a public network such as internet



9)

→ Network layer Design Issues:

- → Store & Forward packet switching
- → Services provided to transport layer
- → Implementation of connection - less service.
- → Implementation of connection oriented service.
- → comparision of virtual - circuit and datagram network

9)

III) Load shedding :-

→ When buffer becomes full routers simply discard packets

→ Which packet is choosen to be the victim depends on the application & on the error stragey used in the data link layer.

→) For a file transfer

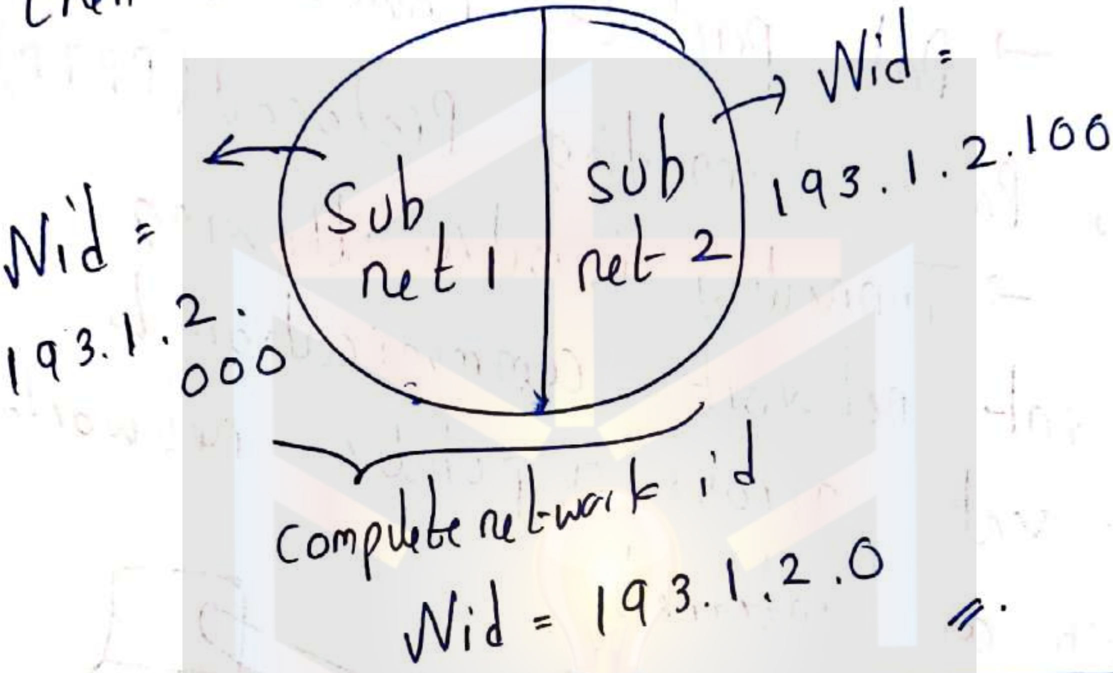
ex: cannot discard older packet since this will cause a gap in the received data

→ For real time voice or video it is probably better to throw away old data & keep new packets.

→ get the application to mark packets with discard priority.

7) Subnetting:

When a bigger network is divided into smaller networks in order to maintain security then that is known as subnetting



//.

×

5) a) Concatenated virtual circuit,
Connectionless internet circuit.

(in given Question bit 4 & 3)

Internetworking

Concatenated Virtual Circuits

Internetworking in a connection-oriented environment operates essentially as in the single network case:

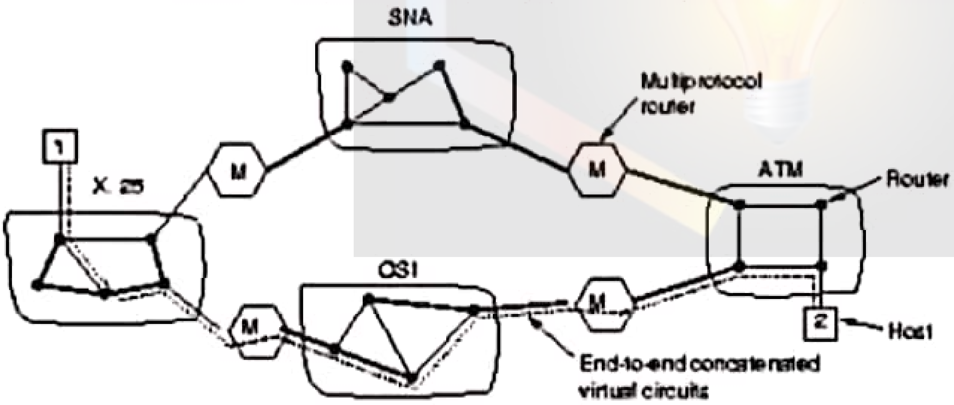
1. The sending host opens a virtual circuit as before, but now a circuit goes through router hops.

2. Any two neighboring routers at the internetworking level must be connected to a common network.

3. Regular router-based virtual circuits connect neighboring routers on the same physical network.

4. The end-to-end virtual circuit is a concatenation of individual virtual circuits through each of the networks along the path.

So each gateway/router maintains tables for each of the connections passing through it - what router to pass the packet on to, and an identifier for the virtual circuit.



Internetworking

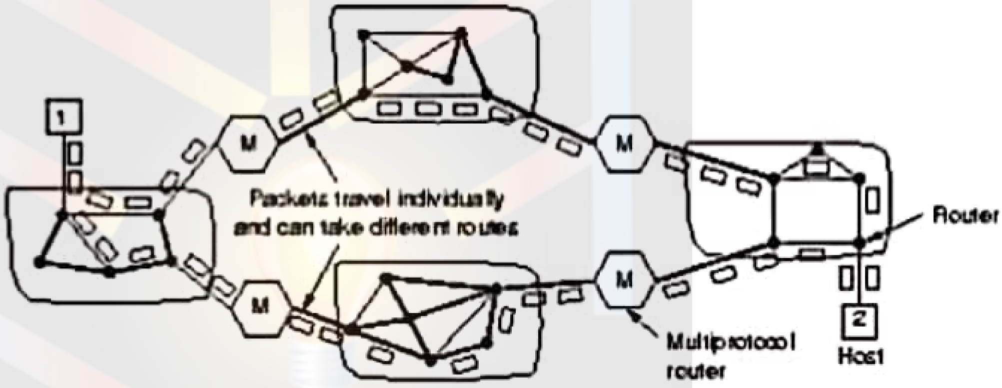
Connectionless Internetworking

Connectionless internets operate just as connectionless networks.

- A host sends a packet to a neighboring router, which forwards it the next router, and so forth.
- Just as with connectionless networks, routers make only a best-effort attempt at delivering the packet.

Datagrams

The Network layer puts datagrams on the subnet. See Figure 5.37



Issues that must be dealt with:

- Networks with different networks protocols are tough to translate between. This is rarely attempted. (See tunneling below.)
- Addressing - when adjacent networks have differing address schemes, the going gets tough. Again, problems are generally insurmountable.

1) 6 a) or b)
adaptive routing algorithm:

= i) Distance vector routing
↳ in CW.

ii) Link state routing
↳ same in CW it could be enough.

IV) Distance Vector routing :-

→ In distance vector routing the least cost root b/n any two nodes is the root with the min distance

→ In this protocol as the name says each node maintains a vector (table) of minimum distance to every node.

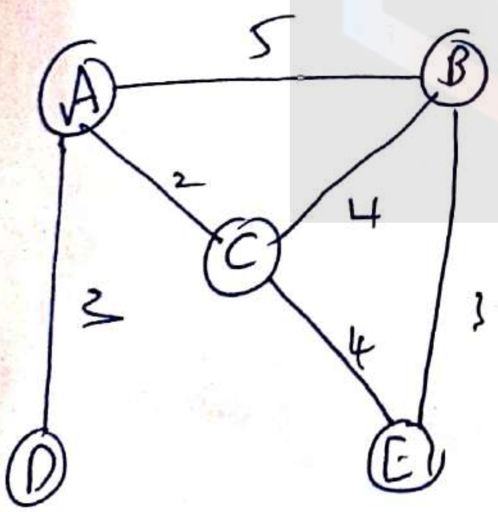
→ Mainly three things in this
- ✓ inizialization
- ✓ sharing
- ✓ updating

Inizialization

→ each node can know only the distance b/n itself & its immediate neighbours those directly connected to it.

→ each node will set a message to the immediate neighbour to find the distance b/n itself & their neighbours.

→ The distance for any entry that is not a neighbour is ∞ (unreachable).



A's table

To	cost	Next
A	0	–
B	5	–
C	2	–
D	3	–
E	∞	

C's table

To	cost	Next
A	2	–
B	4	–
C	0	–
D	∞	–
E	4	

B's table

A	5	–
B	0	–
C	4	–
D	∞	–
E	3	

D's table

A	3	–
B	∞	–
C	∞	–
D	0	–
E	∞	–

E's table

A	∞	–
B	3	–
C	4	–
D	∞	–
E	0	–

Sharing:-

→ The whole idea of distance vector routing is the sharing of info b/n neighbours

→ Although node A does not know about node E, node C, node B, node C does

→ node C shares its routing table with A

node

not
nod

ho
be
i
t

→ node A can also know how to reach node E.

→ On the other hand node C does not know how to reach node B, but node A does.

→ Node A shares with Node C how to reach to node B. It is nodes will be sharing it's routing table with it's imediate neighbours so that it can help to each other to reach the far nodes

Note: distance vector routing each node shares it's routing table with it's immediate neighbours periodically & their is any change?

Updating: When a node recives a two column table from a neighbour it needs to update it's routing table.

Updating takes 3 steps.

i) the receiving node needs to add the costs b/n itself & the sending node to each value in the 2nd column $\therefore$ $(x+y)$

distance + cost

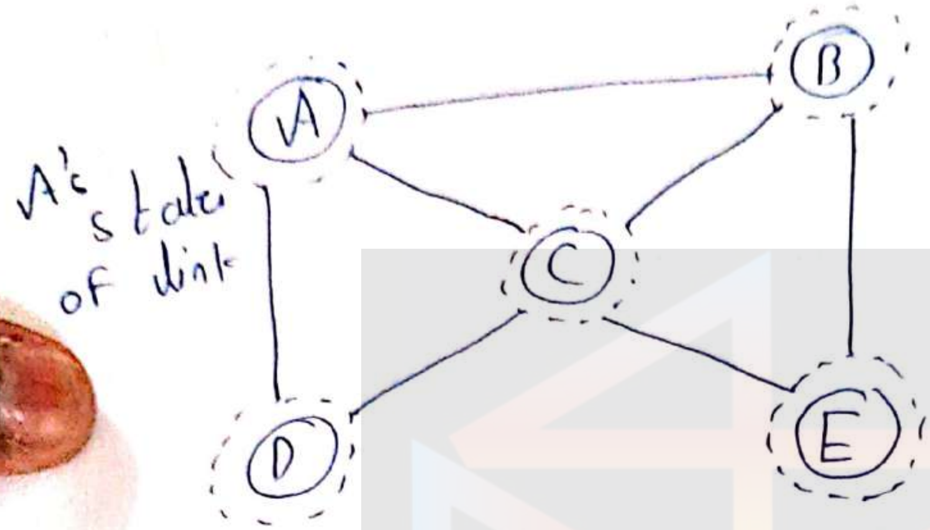
ii) IF the receiving node uses information From any row the sending node is the next node in the route

iii) The receiving node needs to compare each row of its old table with the corresponding row of modified version of received table.

<u>V Link state routing:</u>

Link state routing is based on the assumpsion that allthough the global knowledge about the topology is not clear, each node has a partial knowledge it knows the state (type, condition & cost) at links (status)

In otherwords whole topology can be combined From the patial knowledge of each node



Building routing tables:

→ Creation of the state of the link by each node called Link state packet (LSP)

→ Passing of the LSP to every other router called hope (Flooding)

→ Formation of shortest path in each other

→ Calculation of a routing table based on the shortest path tree

2) Congestion prevension policies

- Open loop (Prevent congestion before it happen)
  - Retransmission policy
  - window policy
  - Ack policy
  - Discarding policy
  - Admission policy
- ~~Closed loop (Remove congestion after it happens)~~

Open loop: Prevent congestion before it happens.

i) Retransmission: It is the policy in which retransmission of the packets are taken care. If the sender feels that a sent packet is lost or corrupted the packet needs to be retransmitted

ii) Window Policy: The type of window at the sender side may also affect the congestion It's better to use selective repeat window should be adopted as it sends the specific packet that may have been lost.

iii) Discarding Policy:

A good discarding policy adopted by the routers is that the router may prevent congestion & at the same time discard the corrupted packet.

iv) Acknowledgement Policy:

Since receiving acknowledgement also increase the change of congesion. Hence receiver should send Acknowledgment for N packets other than 1 packet

v) Admission Policy:

Any change in flow if it may cause congension we should not do it.