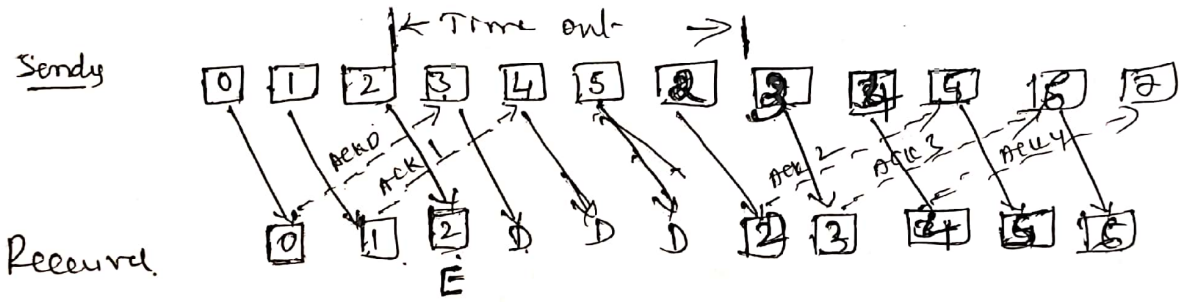
- If the Receiver window size is 1 the receiver simply discard all the subsequent frames. except the one it must give to network layer. i.e Receiver discards the frames that are currupted (or) out of order. and receiver does not send any ACK for such frame.

- For any frame that the sender does not receive any ACK, it understands that along with that frame all the following frames must have been discarded and retransmit all the following frames

- It leads to the retransmission of entire window of size N. hence it is called Go-Back-N protocol.



This method wastes lot of bandwidth if the error rate is HIGH, to avoid this we can use Selective Repeat

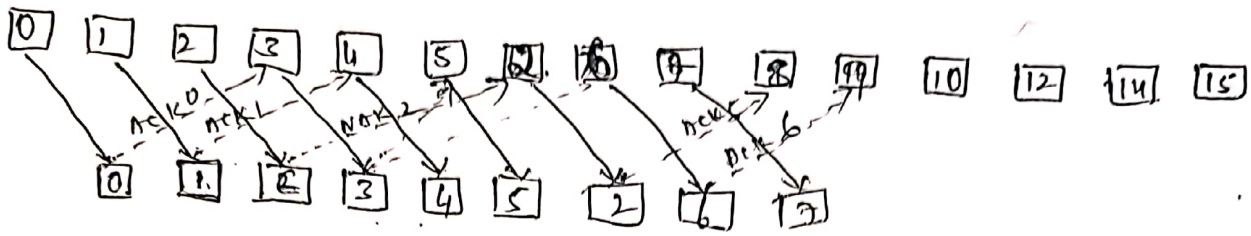
Selective Repeat sliding window protocol

- Only the erroneous (or) Lost frames are retransmitted and good frames are received even they are out of order.

- The Receiver must be able to buffer. some packets since the receiver must supply packets to higher layer in order

(*) Generally the sender's window size (W_s) = Receiver's Window

(*) If sender -ve ACK NAK for the frames received with error.



MAC (Medium Access Control) Sublayer.

* Sub layer of Datalink layer which decides how to allocate a single broadcast channel among competing devices. The channel connects each user to all other users

* There are two types of channel allocations.
  (*) static channel allocation
  (*) Dynamic Channel allocation.

Static allocation: (*) If there are N users the BW is divided into N equal sized portions, with each user being assigned one portion.

(*) When there is small & constant no. of users then this division is simple and efficient allocation mechanism.

(*) But when the number of Senders is large and varying then if there are more than N users

wants to communicate then some of them will be denied because of lack of bandwidth.

(2) Also some of users are allocated channel but users rarely transmit (or) receive then state sub channels are inefficiently used.

(3) Thus for static channel allocation method will not work well for bursty traffic.

Dynamic channel Allocation

Assumptions:

(1) Independent traffic: Each N independent stations (Computer) have program/users that generate traffic (frames) for transmission at a constant rate of λ and assumed that once a frame is generated the device is blocked until the frame is successfully transmitted.

(2) Single channel: All stations can transmit and receive on a single channel. And all devices are equally capable but may be with different priorities based on protocol.

(3) Observable Collisions: All stations can detect that a collision has occurred and collided frame must be retransmitted at a later.

(4) Continuous (or) slotted time.

Continuous means frame transmission may begin at-

at any time (instant), if the it is slotted time frame transmission must begin at start of a slot.

5. Carrier Sense & No Carrier Sense

With Carrier sense assumption the stations can sense channel before trying to use it
With ~~Carrier sense~~ No carrier sense assumption station can not sense channel before trying to use it will transmit.

Multiple Access protocol.

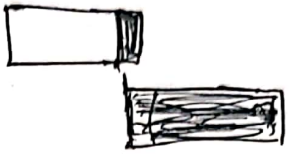
ALOHA: It is the work of Abramson for sharing a single channel among uncoordinated competing users.

* Two types of Aloha → pure Aloha
  → Slotted Aloha.

pure-ALOHA

* The users transmits the data whenever they have data to ~~sent~~ be sent.
* There may be chance for collision here for sender need some way to detect collision / frame has lost.
* The sender needs to wait for random ~~amt of~~ amount of time and retransmits again
* ~~When~~ ~~no~~ on a ~~system~~ ~~with~~ network with a shared common channel, if multiple users Competing to send data that leads to ~~confli~~ conflicts are known as Contention Systems

* In pure ALOHA even if the first bit of new frame overlaps with just last bit of the frame that has almost finished will leads to collision and needs to retransmit both frames



Collision.

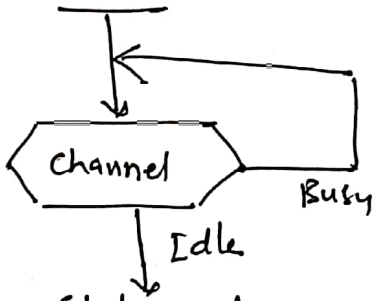
Slotted ALOHA

* In slotted ALOHA stations can not transmit continuously instead waits for its slot and at the begining of its slot can transmit
* slot is allocated for each frame
* In slotted ALOHA 37% of slots may be empty & 37% success and 26% collisions
* By increasing the number of attempts per packet may reduces the number of empties but increases the number of collisions exponentially.

Carrier sense Multiple Access protocols (CSMA)

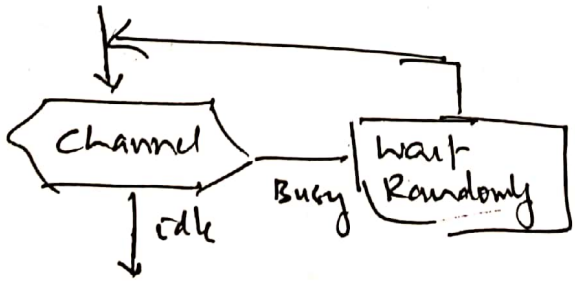
* protocols in which the stations listen (sense) for the channel (Carrier) and behave accordingly are called Carrier Sense protocols.
* Sense before transmit * listen before talks.
* ~~persistent and Non persistent CSMA are the two types~~
* Based on what the station will do after sensing the channel 3 methods have been devised.

1) 1- persistent : ⊛ Simple and straight-forward meth (with probabilit
⊛ station transmits frame immediately after the if the station finds channel is free
⊛ If station finds channel is busy, it continuously senses till the channel becomes idle.
⊛ Highest chance of collisions because 2 or more stations may find the channel is idle and send their frames immediately



Station transmits immediately.

(2) Non-persistent : ⊛ The station which has the data to transmit, ~~senses~~ senses the channel if idle sends immediately, if busy waits a random amount of time and then senses the line again
⊛ It reduces the chance of collision as it is unlikely that 2 or more stations will wait ~~for~~ same amount of time and retry simultaniously.



Station can transmit

⊛ Disadvantage is it reduces the efficiency because the medium remains idle when there may be stations ready

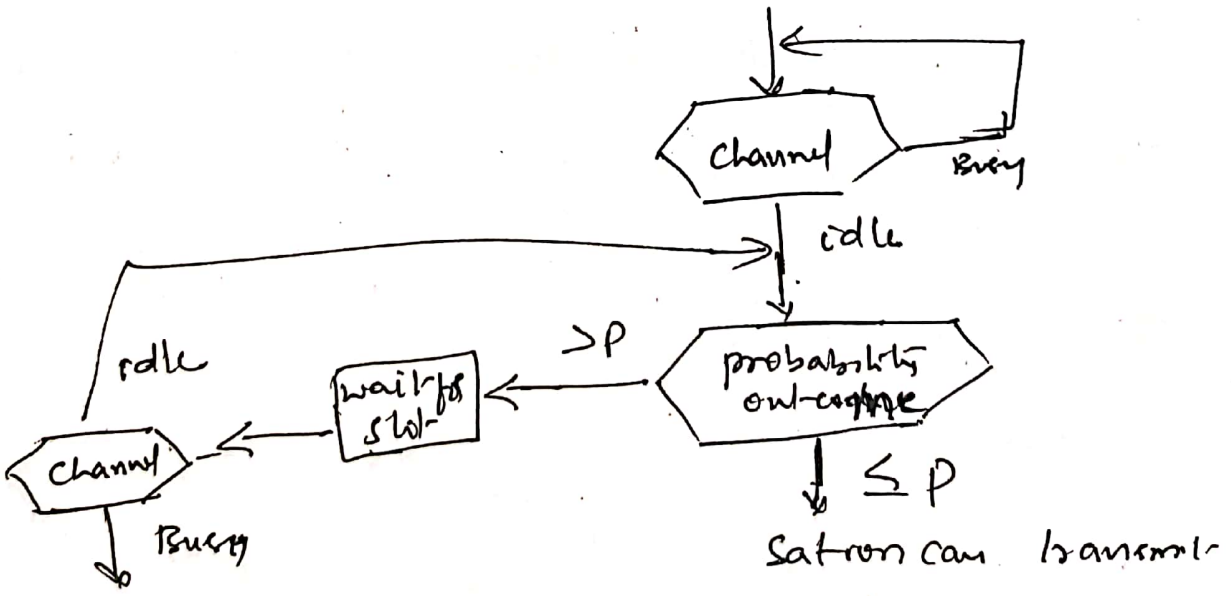
frames to send.

p-persistant : It Combines the advantage of both 1-persistant and Nonpersistant methods

⊕ Reduces chance of collision and improves efficiency

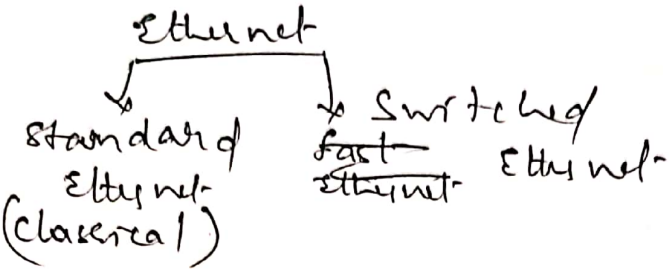
⊕ In this method after the station finds the line idle it follows

1. with probability p, the station sends the frame
2. with probability q = 1-p waits for the beginning of next time slot and checks the line again.
   a. if the line is idle it goes to step 1
   b. if the line is busy, it acts as collision is occured and uses the back of procedure.



Ethernet

* Wired LAN is ethernet, in 1985 IEEE started project called project 802 to set standards to enable interconnection among equipments.



classic / standard ethernet

* Thick ethernet
  1. uses Bus topology with an external transceiver.
  2. It also called 10base5 (10 → 10 Mbps, 5 → 500 m)
* The max length of Co-ax cable must not exceed 500m
  3. uses BNC connector
* Thin ethernet / 10base2
  1. uses bus topology, cable is thinner & flexible,
  2. Supports 10 Mbps and uses T-Connectors to connect systems.
* The max co-axial cable length must not exceed 200m beyond that repeaters are required

Switched Ethernet

(X) In Thick & Thin ethernet the problem was finding broken (or) loose connections in the network. This is solved in switched ethernet

(*) Band width is shared only b/n the stations and the switch.

(*) 10 Base-T network that supports 10 Mbps and uses twisted pair.

(*) 10 Base-F network that supports 10 Mbps and uses fiber optics.

Fast-Ethernet

(*) supports 100 Mbps (*) uses same 48-bit address

(*) uses same frame format

(*) 100 Base-Tx (*) 100 Base-Fx

Gigabit-Ethernet

(*) supports data rate of 1 Gbps

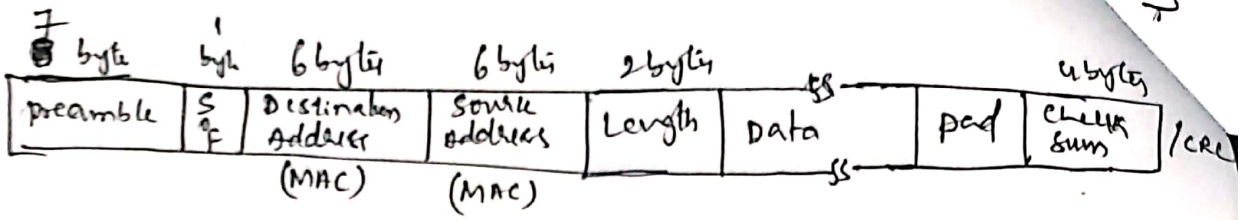
(*) uses same frame format

(*) 1000 Base-Sx (short wave fibre), 1000-Lx (long wave fibre

(*) 1000 Base-Cx (Copper STP) (*) 1000 Base-T (4-wire UTP)

~~Ethernet~~ Ethernet (802.3) frame format

Ethernet (802.3) frame format



preamble: 7 byte & alternating 1's and 0's used synchronize its input timing. it is 56 bits & alternating 10101010..... it produces a 10MHz square wave

SOF: Start of frame delimeter. 8 bits of 1 byte 10101011 which indicates the beginning of the frame and the last 2 bits 11 alerts the receiver that the next field is destination Address

Destination Address: 6 byte MAC (48 bits) address which is physical address of the Receiver. If all bits are 1 in DA then it will be broadcasted to all machine

Source Address: It Contains the 48 bit physical (MAC) address of the sender.

Length field: It specifies the number of bytes in the data field.

Data: This field carries data encapsulated from the upper layer protocols, its of minimum 46 bytes and maximum upto 1500 bytes

pad: If the data portion of frame is < 46 bytes, then this Pad field is used to fill out the frame to the minimum size.

Important: The minimum length of frame is to prevent the stations from completing the transmission of short frame.

for the first bit has even reached the far end of the cable, it means it helps for Collision detection.

CRC: is an error-detecting code used to detect errors.

Network layer

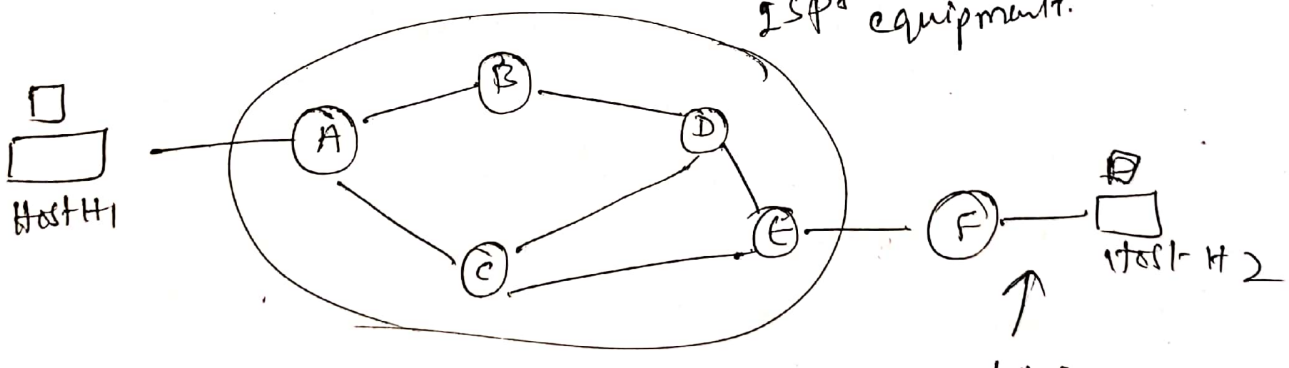
* ~~Routing~~ * providing service to the upper layer
  - Source to destination delivery of packets
  - Logical addressing

~~State~~ Network layer Design Issues.

~~The major Components~~

Store and forward packet switching.

The major components of Network are carrier equipment (routers connected by transmission line) and the customer equipments. (may be Host or a router).



Here A, B, C, D, E are ISP's equipments (routers)

F is customer equipment (routers) maintained by and operated by customer

Here a Host with packets to send transmits it to the nearest routers either on its own LAN (or) over a p-to-p link to ISP. i.e. $H_1 \rightarrow A$ (or) $H_2 \rightarrow F$

The packet is stored there until it has going and the check sum can be verified. Then it is forwarded to the next router along the path until it reaches the destination host.

Services provided to Transport layer

The network layer provides services to the transport layer at the network layer / transport layer interface and the services should be

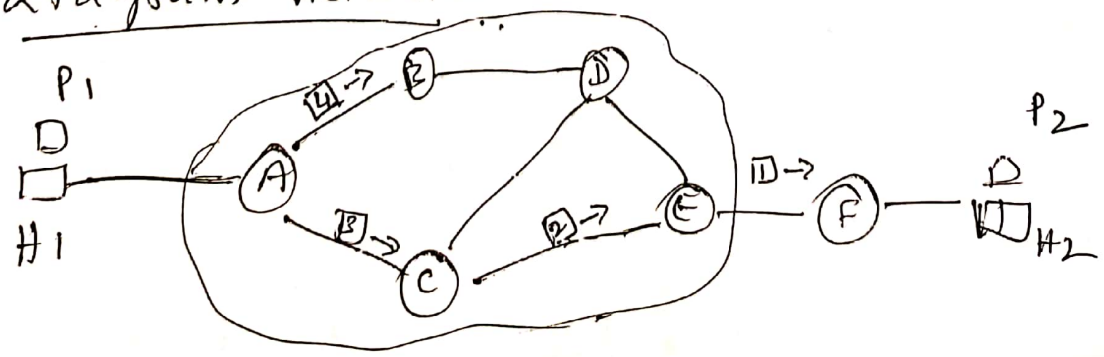
1. The services should be independent of router technology
2. The Transport layer should be shielded from the number, type and the topology of the routers present.
3. The network address should use uniform numbering plan, even across LANs and WANs

Implementation of Connectionless service

(*) packets are injected into the network and routed independently of each other.

(*) no advance set-up is needed and the packets are called Datagrams and network is called.

Datagram network



on host H_1

Suppose if Process P_1 has message for process P_2 on host H_2 then Transport layer of H_1 prepends a transport header to front of message and handovers the result to N/W layer

(*) Network layer breaks the longer message into 4 packets 1, 2, 3 and 4 and send each of them to router A

(*) From now the data packet are routed based on the routing table entry and table entry contains Destination & outgoing line.

∴ Router A table

Initially	
A	–
B	B
C	C
D	B
E	C
F	C

Later	
A	–
B	B
C	C
D	B
E	B
F	B

Router C table

A	A
B	A
C	–
D	D
E	E
F	E

Router E table

A	C
B	D
C	C
D	D
E	–
F	F

According to the table entry at each router packet 1, 2 & 3 may be sent via router C, But in the later time due to some reason like traffic jams etc packet 4 to the same destination may be routed via Router B

(*) The algorithm that manages the tables and makes the routing decisions is called the Routing Algorithm

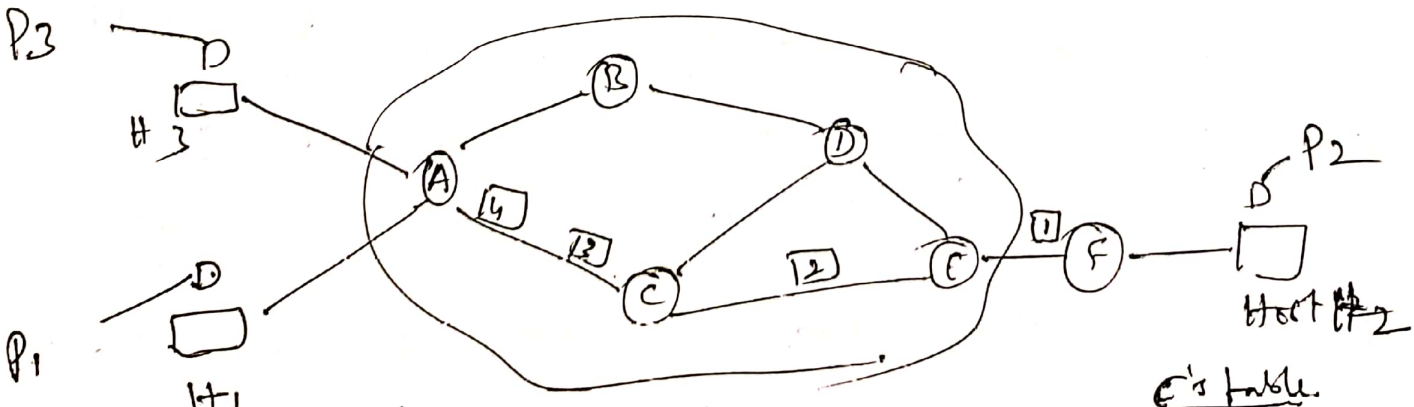
(*) IP (Internet protocol) is the basis for the entire Internet. Each packet carries a destination IP address that routers use to individually forward each packet. (IPv4 & IPv6)

Connection Oriented Service Implementation

(*) path is established before any data packet is sent. This connection is called (Virtual circuit) VC and the network is called Virtual-Circuit-network

(*) When the connection is established, a route from Source machine to Destination machine will be established and stored in the routers table and all packets are forwarded in the same route.

(*) Each packet carries the Virtual circuit number (VC No) telling which Virtual circuit it belongs to.



From Diagram

Host H_1 has established Connection with Host H_2 with ID-1 and also H_3 established Connection with Host H_1 with ID-2 (from the out table of A) but has ID-1 from H_3 to A ∴ it can be differentialid as $\begin{Bmatrix} H_1 - 1 \\ H_3 - 1 \end{Bmatrix}$

(*) From out table routes A. packets from both the hosts H_1 & H_3 follow same paths to differentiate them the VC-ID will be different. so A's table

in	
H_1	1
H_3	1

in

out	
C	1
C	2

out

coming from H_1 & H_3 are forwarded to C router C with ID-1 & ID-2 respectively.

C's table

in	
A	1
A	2

in

out	
E	1
E	2

out

coming from A forwarded to E on ID-1 if from host H_1

coming from A forwarded to E on ID-2 if from host H_3.

E's table

in	
C	1
C	2

in

out	
F	1
F	2

out

coming from C forwarded to F on VC ID-1 if from H_1

—"— C forwarded to F on VC-ID-2 if from H_3

Routing Algorithms : Sudo /etc/init.d/dnsmasq restart (to restart dnsmasq)

(*) The routing algorithms are the part of network layer. s/w responsible for deciding on which o/p line an incoming packet should be transmitted.

(*) The properties that are desirable in a routing algorithm are - Correctness, Simplicity, Stability, and optimality

There are two major groups of Routing Algorithms.

(1) Non-adaptive Algorithm. The routing algorithms that do not change decisions based on the current traffic and topology.

(a) The route from node I to node J is computed in advance, offline and downloaded to the routers when the N/w is booted

(b) It is also called ~~reclotable~~ static Routing

(2) ~~Adap~~ Adaptive routing Algorithm: The routing algorithms that changes their routing decisions ~~to~~ based on the current traffic and topology.

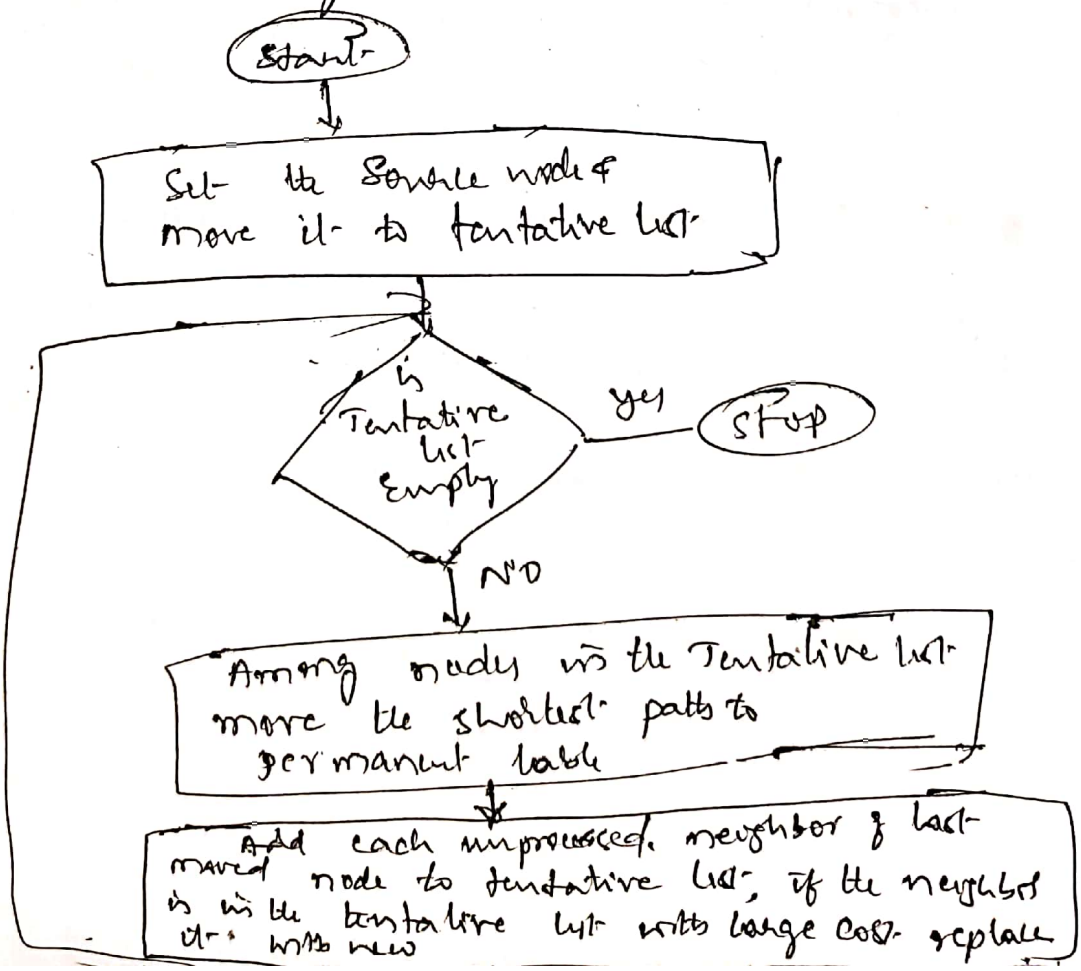
(a) Adaptive Algorithms differs from each other in ~~the~~ the way they get the informations (i.e locally, adjacent routers (or) from all routers), when they change the route and what metric is used for optimization. (e.g distance, no. of hops to be crossed (or) estimated transit time)

Optimality principle: It gives the general statement about the optimal route without regard to network topology (or) traffic

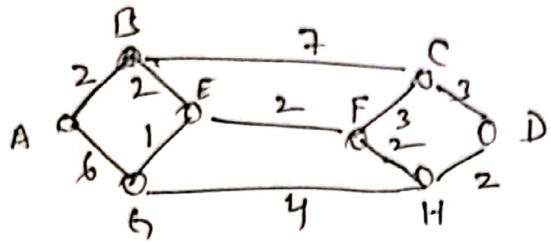
Optimality principle states that; if the router RJ is on optimal path from router RI to Router RK then the optimal paths from RJ to RK also falls along the same route.

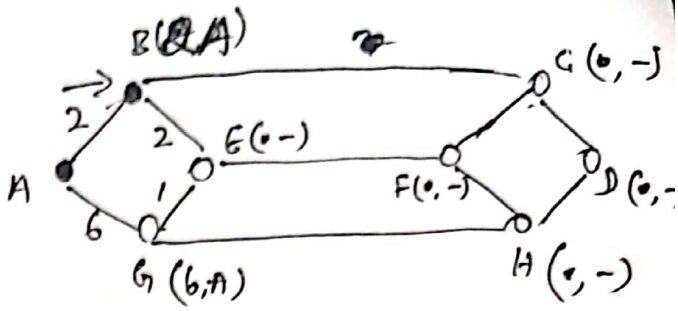
Shortest path Routing (Dijkstra's Algorithm)

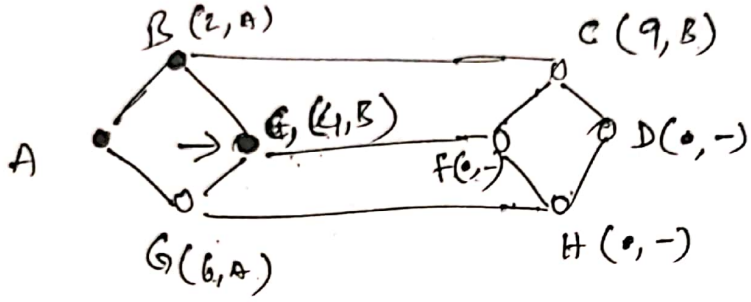
* This algorithm finds shortest path between a given pair of routers.
* The metric for paths may be distance or number of hops. But this algorithm considers the distance
* Each node is labled with its distance from the source node along the best paths.
* permanent lable : It represents the shortest possible paths from source to the node and will never change after.
* Tentative node : It represents the path from source to the node which may not be shortest and once the shortest path is found the Tentative lable will be changed to permanent lable

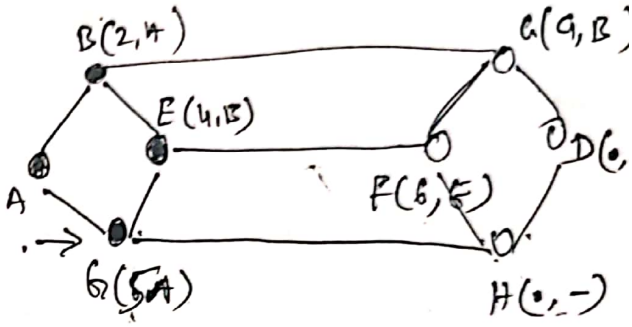


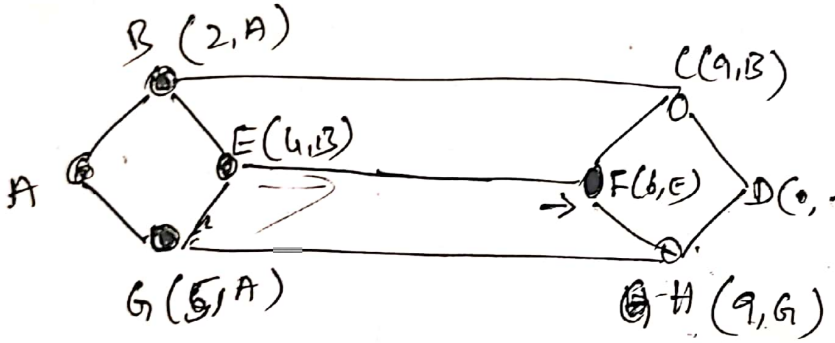
(4) The node with shortest path will become the part of permanent list and it will become an Active node

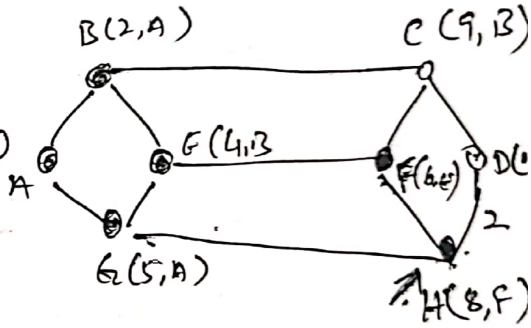












a.

- D (10, F) So the shortest path is

A $\xrightarrow{2}$ B $\xrightarrow{2}$ E $\xrightarrow{2}$ F $\xrightarrow{2}$ H $\xrightarrow{2}$ D

The cost is 10.

~~Add~~ Dis-advantage : It makes decisions based on local knowledge and not with complete knowledge of the entire topology.

~~Flooding~~

Flooding

(*) Takes the routing decisions based on local knowledge

(*) In flooding every incoming packet is sent out on every outgoing line except on incoming port.

(*) Flooding generally packet number & duplicate packet i.e. to avoid duplicates header in each packet contains hop counter which is decremented at each hop and is discarded when the counter reaches zero. Generally the count is initialized to the length of the path from source to destination. If the sender does not know the length of the path. then count is initialized to the worst case i.e the full diameter of the network.

(*) The disadvantages of flooding is the routers duplicates the packets even which they have received before.

(*) So to reduce the duplicates still further the better method is to make the routers to keep tracks packets which have been flooded by router to avoid sending them out for 2nd time. one way to achive this is to have the source router to put a sequence number.

(7) Not practical for sending most packets but flooding ensures that the packet is delivered to every node in the network i.e useful for broad casting information but wastful for single destinations

(8) Some algorithms wireless networks make use of the concepts of flooding.

(9) Flooding is robust, it will find path even if one exists to get a packet to its destination

(10) With flooding Router need to know only the neighbors.

(11) flooding always chooses the shortest paths.

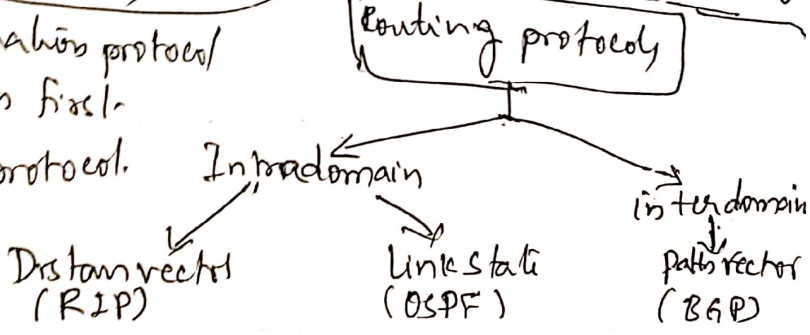
Distance vector Routing

(12) Dynamic routing algorithms also called as Bellman-Ford algorithm

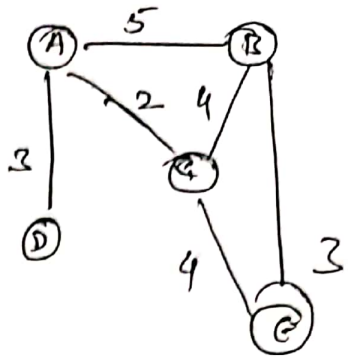
(13) Each Router maintains a table (vector) of minimum distances to every node.

(14) Each entry in the table contains
- (a) preferred outgoing line for the required destination
- (b) Estimate of time/distance to that destination (metric may be number of hops / time delay in msec)

RIP: Routing information protocol
OSPF: Open shortest path first.
BGP: Border Gateway protocol.



Consider a ~~graph~~ network graph.



① Initialization

② Initially each node can know only the distance between itself and its intermediate neighbours connected directly..

③ Each node can send message to ~~nbr~~ the immediate neighbours and find distance

A's table

To	Cost	next
A	0	—
B	5	—
C	2	—
D	3	—
E	∞	

B's table

To	Cost	next
A	5	—
B	0	—
C	4	—
D	∞	
E	3	—

C's table

To	Cost	next
A	2	—
B	4	—
C	0	—
D	∞	—
E	4	—

D's table

To	Cost	next
A	3	—
B	∞	
C	∞	
D	∞	—
E	∞	

E's table

To	Cost	next
A	∞	
B	3	—
C	4	—
D	∞	—
E	0	

④ Sharing : Distance vector routing estimates/finds paths by sharing information. In the above example node-A don't know how to reach node-E but node-C knows. So if node-C shares its routing table with A node A can also know how reach node-E using node-C also node-A knows how reach D so by sharing they can improve their routing tables

Scanned by CamScanner

Each router can share first 2 columns of its table with its neighbor.

Updating

Each node on receiving 2 columns from neighbors updates their table in 3 steps.

1. Receiver node adds the cost b/n itself and the sending node
2. The receiving node needs to add the name of the sending to each row as the third (3rd) column. If the receiving node uses information from any row
3. The receiving node compares each row of its old table with the corresponding row of the modified version.

   (a) If the next-node entry is different, the receiving node chooses the row with smaller cost; if same the old one is kept.

   (b) If the next-node entry is same the receiving node chooses the new row

Example for updation

Received from C

To	Cost	next
A	2	C
B	4	C
C	0	C
D	∞	C
E	4	C

A's old.

To	Cost	next
A	0	A
B	5	C
C	2	C
D	3	E
E	∞	E

A's modified table

To	Cost
A	4
B	6
C	2
D	3
E	∞

C→A + A→C : 2 + 2 = 4

C→B + A→C : 4 + 2 = 6

C→C + A→C : 0 + 2 ⇒ 2

C→D + A→D : ∞ + 3 ⇒ 3

C→E + A→E : 4 + ∞

C → A + A → C
2 2 · = 4

C → B + A → C
4 · 2 = 6

C → C + A → C
0 2 = 2

C → D + A → C
0 2 = 2

C → E + A → C
4 2 = 6

So the modified table of A is

T1	Cost
A	4
B	6
C	2
D	

Link State Routing:

In distance vector routing if any router goes down it leads to count to infinity problem as the node which is not adjacent will not know about the status of the node which is inactive. To solve this problem Link state routing can be used.

* LSR will have the complete picture of the network i.e each router builds the complete topology of the entire network.

(*) Every router contains identical information about the network and each router is able to calculate its own best path independently.

(*) Link state is also known as shortest path first

(*) Link state algorithm is stated in 5 steps

1) Discover and learn about the neighbors

When each router is booted, every one will send HELLO pack to its neighbors and the other end replies with its identity

2) Setting the Link Cost

Each router estimates the cost to each of its neighbours. The common method is to send ECHO packet and measure the round trip time & divide it by two to get the delay.

Ex: 1 Gbps Ethernet may have cost of 1 and 100 Mbps may have cost of 10

3) Building link state packet (LSP)

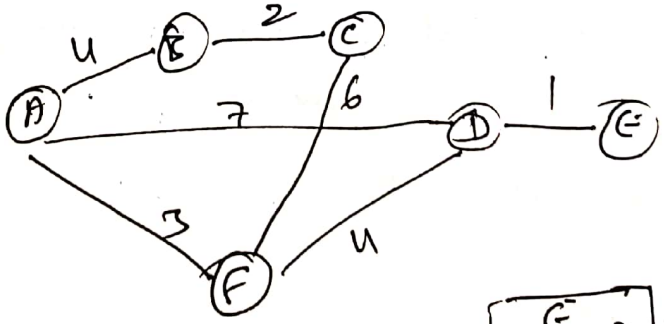
After collecting the information routes build LSP. LSP starts with identity of sender,

Sequence number: which is used along with sender to keep track of LSP and check against the list of packets already seen. If it is new it is forwarded, if duplicate discarded.

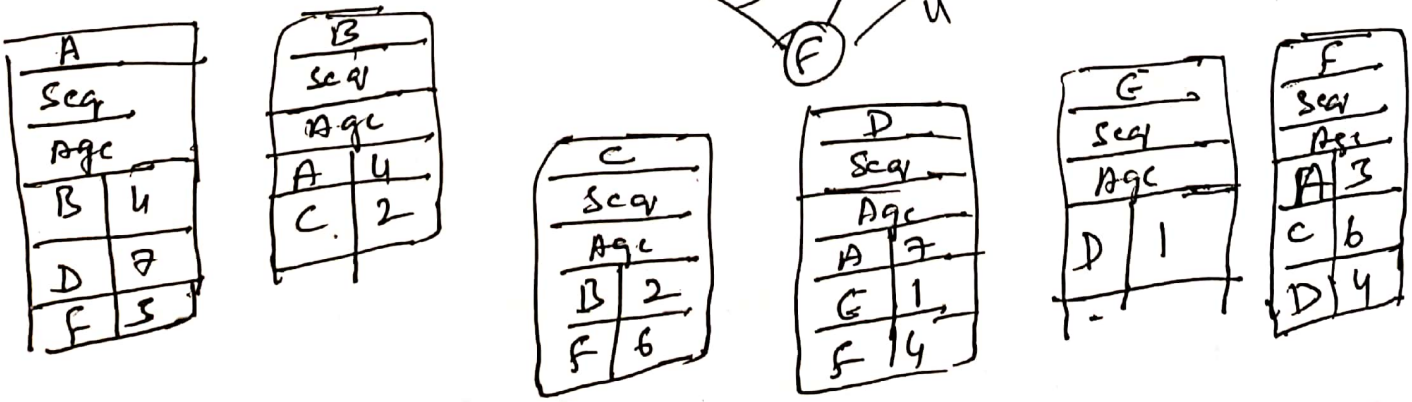
Age: This field is decremented by each router during the initial flooding to make sure that no packet can get lost and live for indefinite period of time. (i.e when Age = 0 the packet is discarded.

List of neighbors: LSP contains of a node contains its neighbors and their distance.

Consider the graph



LSP



4) Distribution: Uses flooding to distribute the packets. To control the overflow and duplicate using Sequence no, it is incremented for each new packet delivered. and the router keeps only the LSP with highest sequence number & drops LSP with lower Seq no.

5) Compute Shortest paths

After gathering all the LSP a router can Construct entire - Subnet graph and can algorithms like Dijkstra's algorithm can be run locally to Construct Shortest paths to all possible destinations

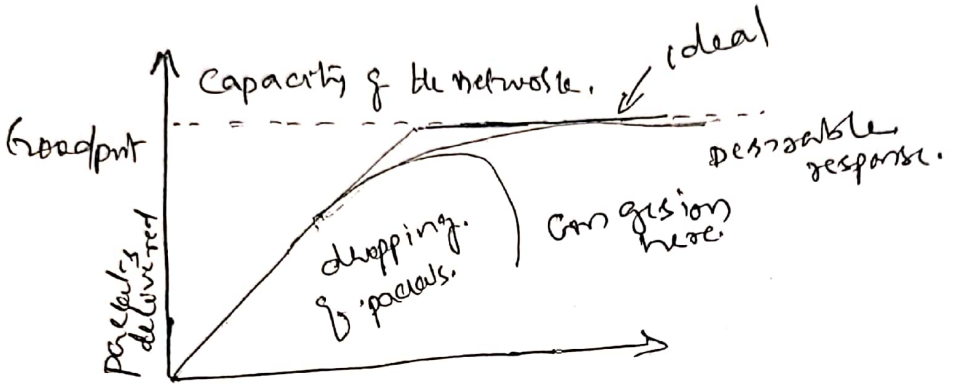
Problems in Link State Routing

(x) The memory required to store the data is proportional to K*n for n routers each with 'K' neighbours

(x) Time required to Compute is more

Congestion: Too many packets present in the network causes packet delay and packet loss that degrades the performance. This situation is called Congestion.

The responsibility of handling congestion is shared among network and Transport layer.



Reasons for Congestion:

- Sudden arrival of packets on a particular o/p line from multiple i/p source.
- Insufficient memory in a router to hold packets
- Slow processor can also cause congestion
- Low bandwidth channel can also cause congestion.

Congestion Control: ensures that the subnet is able to carry the offered traffic and not overloaded.

Flow control: Ensures fast sender does not overload ~~packets~~ receiver.

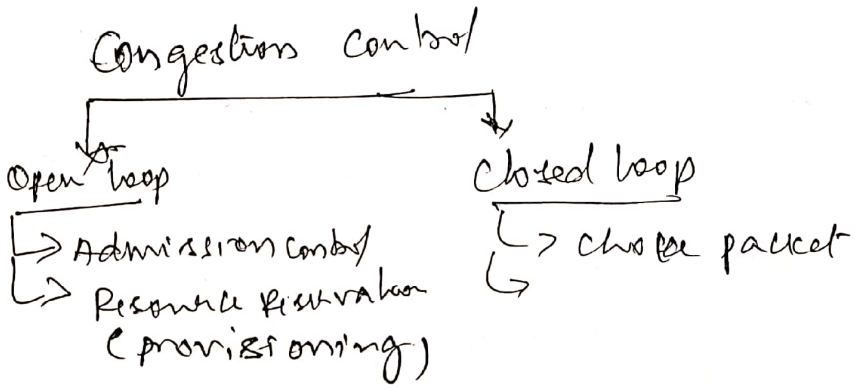
(*) Congestion control required when the buffers at the switches (7) overflows

(*) Congestion involves all hosts, lines, routers & it is global issue

(*) Flow control is needed when the buffers at receiver overflows i.e when Receiver is slow in processing

(*) Flow is b/w Sender & receiver, it is local issue or can be done on end-to-end basis.

Approaches to Congestion control



Open loop Congestion Control : policies are designed and applied to prevent Congestion before it happens rather than dealing with it after it has occured.

(*) Admission Control : In this method the ~~load~~ load is decreased to avoid Congestion. In virtual network new connections ~~are~~ can be refused if they would leads to congestion. i.e if the congestion is suppose to happen then the network can eliminate the Sources responsible for the problem to throttle their traffic (or) slow down the traffic itself.

problems are : * How to identify the onset of Congestion

(2) and how to inform source that needs to slow down

So router can monitor the average load and Queueing delay or packet loss. Rising number in packet loss indicates growing congestion

Traffic policing: process of monitoring and ~~The network may~~ enforcing the traffic flow of packets during connection period. The most implementation of traffic policing is done through

~~(1)~~ Leaky Bucket algorithm:

In this each router will have buffer to hold the incoming packets, so that no matter at what rate the packet arrives at the i/p line of router, the router pass to its outgoing line at fixed rate:

If there is no overflow at the buffer. then the traffic is within the agreed norms all packet will be transported.

If buffer spillover. it may lead to congestion and additional packets will be lost