UNIT- III

Network Layer

Delivery of data pkt from S to D accross multiple hops & link. It is lowest layer i.e. concerned with end-to-end transmission.

Duties of N/w Layer

Internetworking, Addressing, Routing, Packetizing, Fragmentation

* Network Layer Design Issues:

1) Store and Forward packet Switching:

→ The host sends the pkt. to the nearest router.
→ The pkt is stored in the router until it has fully arrived and its checksum is verified for error detection.
→ Once, this is done, the pkt is forwarded to next router.
→ Since, each router needs to store the entire pkt before it can forward it to the next hop, the mechanism is called store-and-forward switching.

2) Services provided to Transport Layer:

Through the n/w/transport layer interface, the n/w layer transfer it's services to the transfer layer.

The objectives of N/w layer while providing these services are :-

- Offering services must not depend on router technology.
- The transport layer (TL) needs to be protected from the type, number and topology of the available routes.
- The n/w addresses for the TL should use uniform numbering pattern also at LAN and WAN connections.

Based on the connections there are 2 types of services provided :

Connectionless : The routing and insertion of pkt into subnet is done individually. No added setup is required.

Connection-Oriented : Subnet must offer reliable service and all the pkts must be transmitted over a single route.

3) Implementation of Connectionless Service :

→ pkt termed as "datagrams" and corresponding subnet as "datagram subnet".

→ Each pkt is transmitted independently, each pkt contains its routing info.

→ No prior setup of routes are needed before transmitting a msg.

→ Each datagram belong to the msg follows its own individual route from the S to D.

→ Eg. Internet Protocol or IP.

4) Implementation of Connection Oriented Service:

→ First we establishes a connection, use it and then release it.

→ the data pkts are delivered to the R in the same order in which they have been sent by the S.

It can be done in either two ways:-

- Circuit Switched Connection: A dedicated physical path or a circuit is established b/w the communicating nodes and then data stream is transferred.
- Virtual Circuit Switched Connection: The data stream is transferred over a pkt switched n/w, in such a way that it seems to the user that there is a dedicated path from the S to R.
A virtual path is established here, while other connections may also be using the same path.

* Differences b/w virtual circuit & Datagram N/w:

Virtual circuits are comp. n/w that provide connection oriented services and Datagrams provide connectionless services.

Eg. Internet is based on Datagram n/w. ATM (Asynchronous Transfer Mode) and frame delay are virtual circuit n/ws. and they use connectn at n/w layer

Virtual Circuit	Datagram Network
1) Virtual circuits are connection-oriented, which means that there is a reservation of resources like buffers, BW etc. ~~for the time during~~ which it is used for data transfer session.	It is a connectionless service. There is no need for reservation of resources as there is no dedicated path for a connection session.
2) It uses a fixed path for a particular session, after which it breaks the connection and another path has to be set up for the next session.	It is a true pkt switched n/w. There is no fixed path for transmitting data.
3) All the pkts follows the same path, hence, a global header is required only for the first pkt. of connection and other pkt will not require it.	Every pkt is free to choose any path. Hence all pkts must be associated with a header containing info. about the source and the upper layer data.
4) pkts reach in order to the destination as data follows the same path.	Data pkt reach the destination in random order; which means they need not reach in order in which they were sent out.

5)	They are highly reliable	They are not reliable.
6)	Implementation is costly as each time a new connection has to be set up with reservation of resources and extra info. handling at routers.	It is always easy & cost efficient to implementation. There is no need of reserving resources and making a dedicated path each time an app. has to communicate.

* **Routing Algorithms**

It is a part of n/w & layer s/w. N/w layer must determine the best route through which pkts can be transmitted from S to D. The Routing protocol provide this job. Best path means "least cost path" from S to D.

Properties of Routing algo:

1) Correctness & simplicity
2) Robustness
3) Stability
4) Fairness & optimality
5) Efficiency.

Types of Routing Algo:

- Adaptive Routing Algo
  - Centralized algo
  - Isolation algo
  - Distributed algo
- Non adaptive Routing Algo
  - Flooding
  - Random walks

1) Adaptive Routing Algo:

→ known as dynamic routing algo.

→ algo makes the routing decision based on topology & n/w traffic.

→ Main parameters are hop count, distance and estimated transit time.

Types:

i) **Centralized algo:** It is known as global Routing algo. as it computes the least cost path b/w S to D. by using complete & global knowledge about the n/w.

This algo. takes the connectivity b/w the nodes and link cost as i/p and this info. is obtained before actually performing any calculation.

'Link State algo' is referred to a centralized algo since it is aware of the cost of each link in the n/w.

ii) **Isolation algo:** obtains the routing info. by using local info. rather than gathering info. from other nodes.

iii) **Distributed algo:** it is known as decentralized algo as it computes the least-cost path b/w S and D in an iterative & distributive manner.

No node has the knowledge about the cost of all the n/w links. In the beginning, a node contains the info. only about its own directly attached links and through an iterative process of calculation computes the least-cost path to the destination.

A distance vector algo is a decentralized algo as it never knows the complete path from S to D, instead it knows the direction through which the pkt is to be forwarding along with the least cost path.

2) Non-Adaptive Algo:

→ Known as Static routing algo.
→ When booting up the n/w, the routing info. stores to the routers.
→ It does not take the routing decision based on n/w topology or n/w traffic.

Types:

1) Flooding: Every incoming pkt is sent to all the outgoing links except the one from it has been reached. Disadvantage is node may contain several copies of a particular pkt.

ii) Random Walks? A pkt sent by the nodes to one of its neighbours randomly. Advantage is, It uses the alternative routes very efficiently.

Difference blw Adaptive & Non-Adaptive Routing algo?

Adaptive	Non-Adaptive
1) It constructs the routing table based on the n/w conditions.	It construct the static table to determine which node to send the pkt.
2) It is used by dynamic routing.	Used by static routing.
3) Routing decisions are made based on topology & n/w traffic.	Routing decision are the static tables.
4) Complex.	Simple.

* Shortest Path Routing Algo?

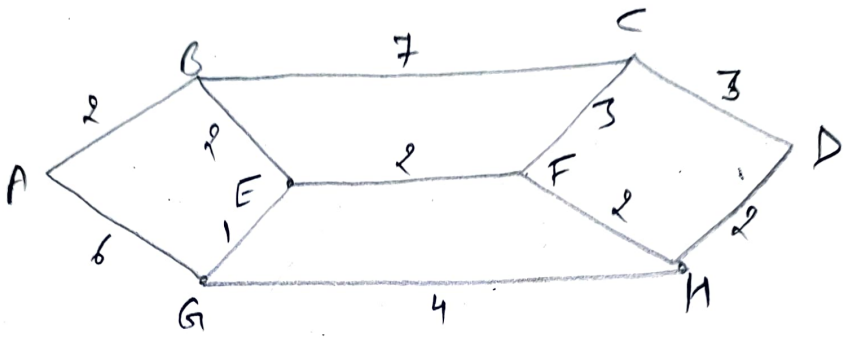
Dijkstra's algo or shortest path algo. is an algo for finding the shortest paths blw nodes in a graph. eg. road n/w.

In Dijkstra algo, each node is labelled with its distance from the source node along the best ~~path~~ known path.

Initially No paths are known, so all nodes are labelled with infinity. As the algo proceed, and paths are found, the label may change respectively better paths. A label may be either tentative or permanent.

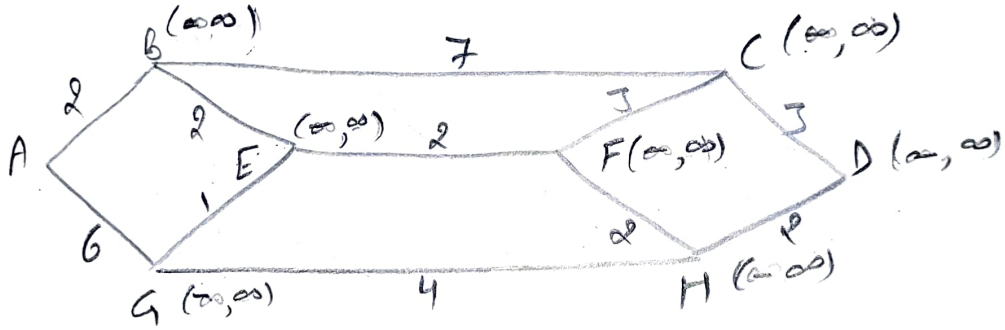
When it is discovered that a label represent the shortest possible path from the source to that node, it is made permanent and never change thereafter.

3.

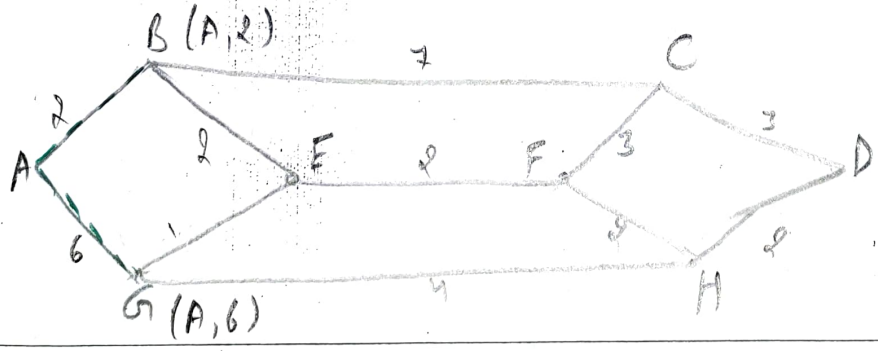


A → D

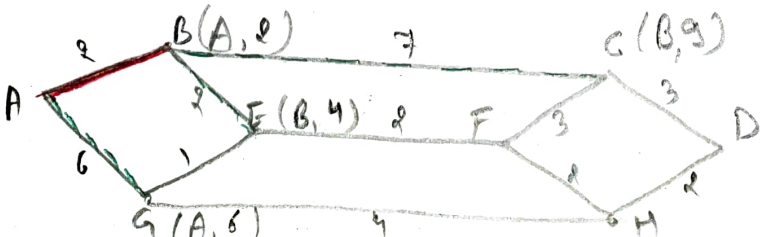
Step 1



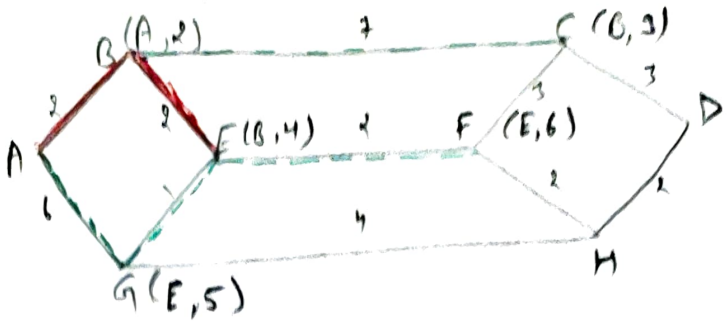
Step 2



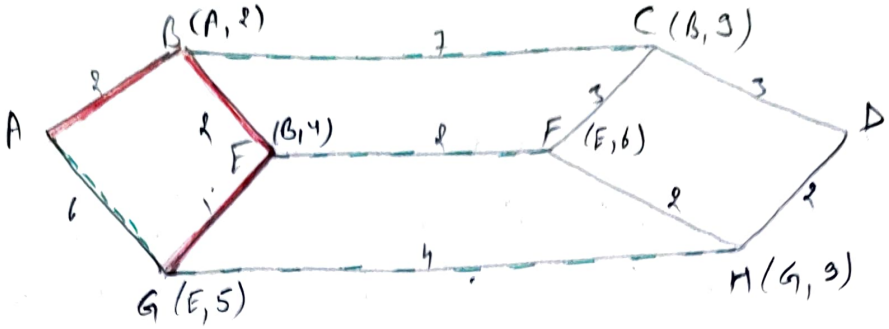
Step 3



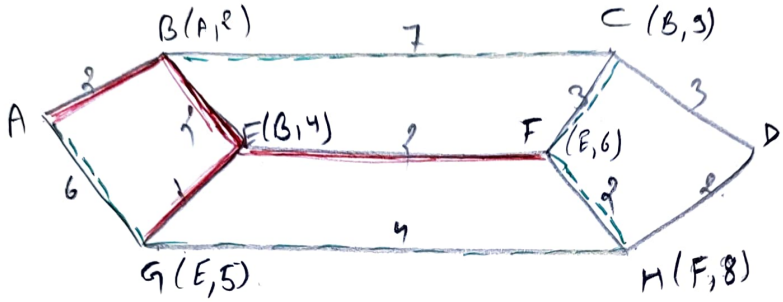
Step 4



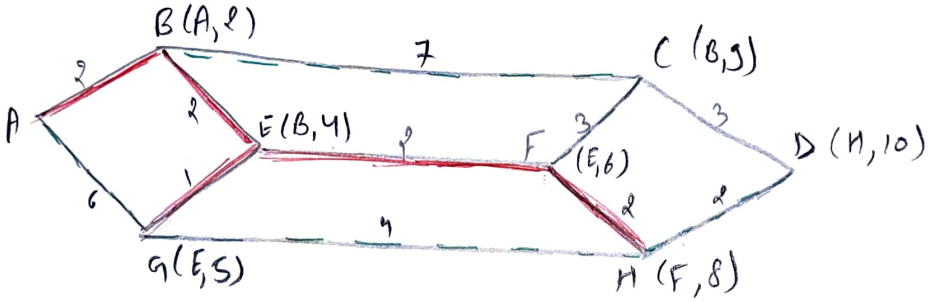
Step 5



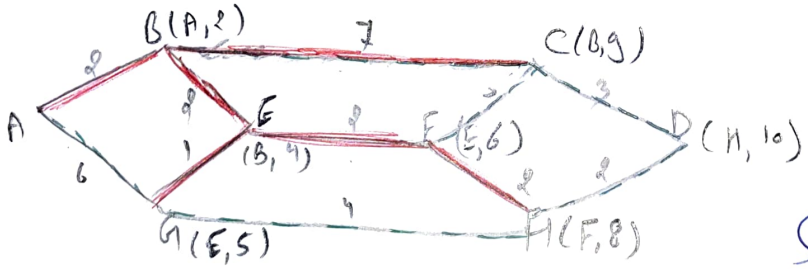
Step 6



Step 7

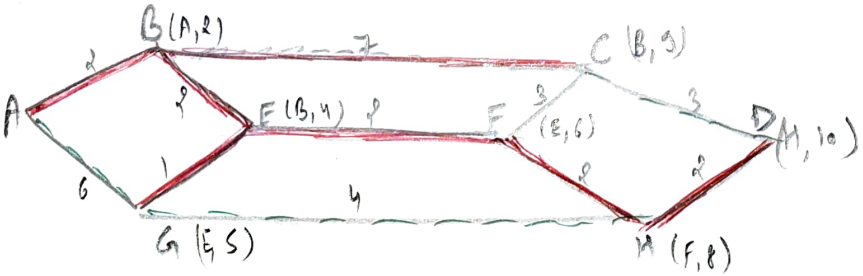


Step 8

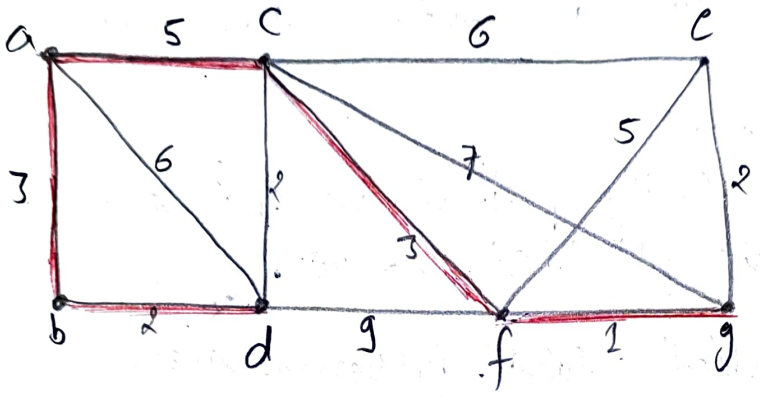


Step 10

Step 9



Dijkstra Algo Example:



V	a	b	c	d	e	f	g
a	0_a	3_a	5_a	6_a	∞_a	∞_a	∞_a
b	0_a	3_a	5_a	5_b	∞_b	∞_b	∞_b
c	0_a	3_a	5_a	5_b	11_c	8_c	12_c
d	0_a	3_a	5_a	5_b	11_c	8_c	12_c
f	0_a	3_a	5_a	5_b	11_c	8_c	9_f

* Distance Vector Routing Algo :

→ A Distance vector routing protocol in data n/w determines the best route for data pkts based on distance.

→ Measure the distance by the no. of routers a pkt has to pass, one router counts as one hop.

→ It is iterative, distributed & asynchronous.

→ It is dynamic algo.

→ Each router maintains a distance table known as vector.

→ Distance-vector routing protocols use the Bellman-Ford algo to calculate the best route.

→ It is also called Ford-Fulkerson algo.

→ Let $d_x(y)$ be the least cost path from node x to node y. The least cost are related by Bellman Ford equation:

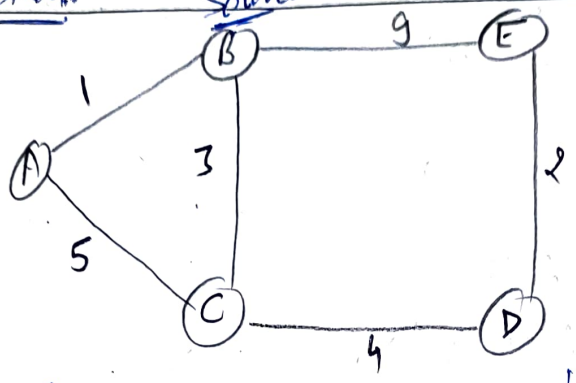
$$d_x(y) = \min_v \{C(x,v) + d_v(y)\}$$

x : Source node , y = destination node

v : Intermediate node

Direct Method: Source

Eg



Make Routing table for hop 'B' (Source).

Destination	Cost	Next hop
A	1	A
C	3	C
E	9	E
D	7	C

from S to D, we calculate Cost & no. of intermediate nodes should be min.

Step1 B to A

$B \rightarrow A : 1$ ✓

$B \rightarrow C \rightarrow A : 8$

$B \rightarrow E \rightarrow D \rightarrow C \rightarrow A : 20$

Step 2 **B to C**

$B \to C : 3$ ✓

$B \to E \to D \to C : 15$

$B \to A \to C : 6$

Step 3 **B to E**

$B \to E : 9$ ✓✓ no intermediate node

$B \to C \to D \to E : 9$ ✓ two intermediate node

$B \to A \to C \to D \to E : 12$

Step 4 **B to D**

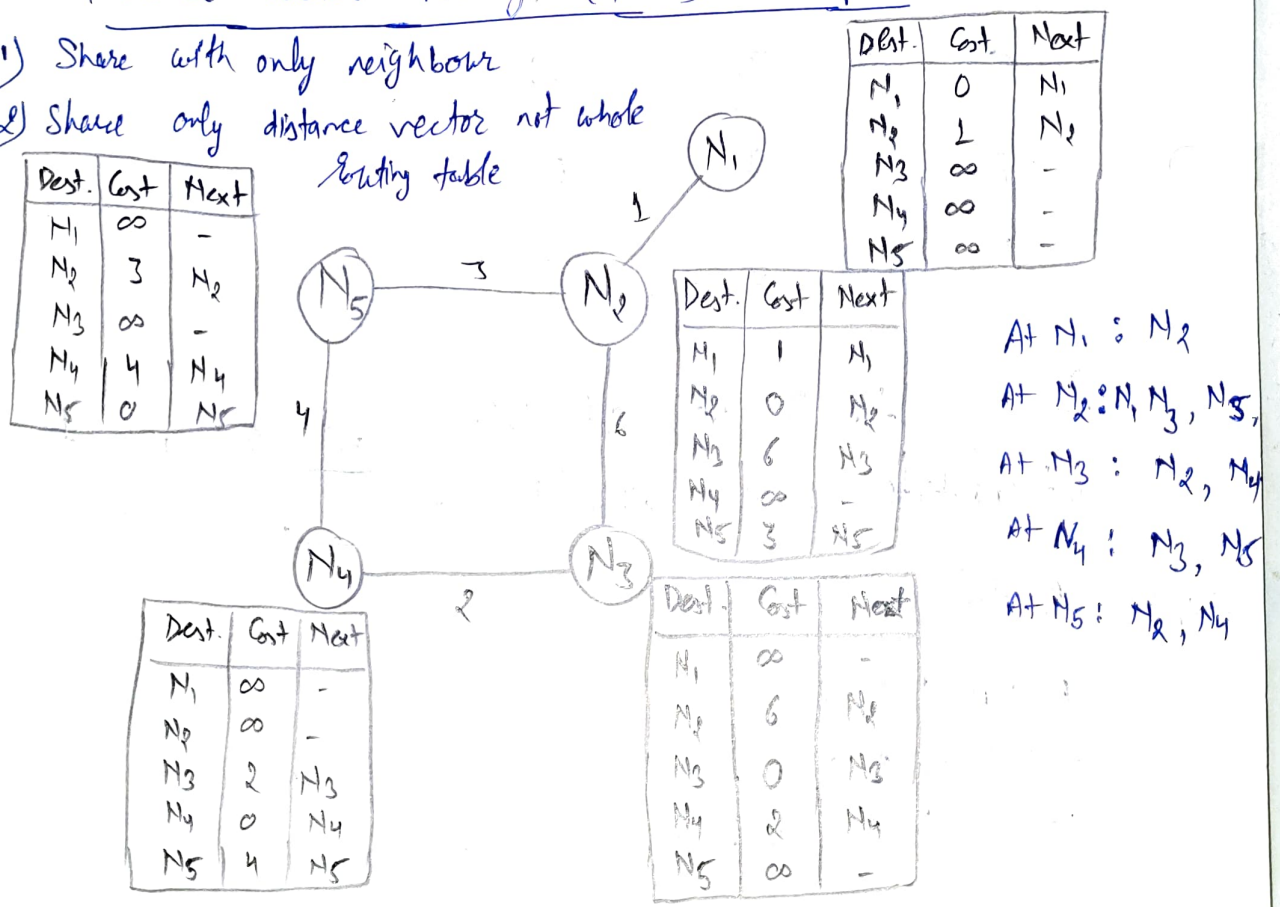
$B \to E \to D : 11$

$B \to C \to D : 7$ ✓

$B \to A \to C \to D : 10$

Q. Distance Vector Routing (DVR) Example? (Another method)

1) Share with only neighbour
2) Share only distance vector not whole routing table



Dest.	Cost	Next
N_1	∞	-
N_2	3	N_2
N_3	∞	-
N_4	4	N_4
N_5	0	N_5

Dest.	Cost	Next
N_1	0	N_1
N_2	1	N_2
N_3	∞	-
N_4	∞	-
N_5	∞	-

Dest.	Cost	Next
N_1	1	N_1
N_2	0	N_2
N_3	6	N_3
N_4	∞	-
N_5	3	N_5

Dest.	Cost	Next
N_1	∞	-
N_2	∞	-
N_3	2	N_3
N_4	0	N_4
N_5	4	N_5

Dest.	Cost	Next
N_1	∞	-
N_2	6	N_2
N_3	0	N_3
N_4	2	N_4
N_5	∞	-

At N_1 : N_2

At N_2 : N_1, N_3, N_5

At N_3 : N_2, N_4

At N_4 : N_3, N_5

At N_5 : N_2, N_4

POORNIMA
COLLEGE OF ENGINEERING
DETAILED LECTURE NOTES

i) At N_1, distance vector of N_2 $\begin{bmatrix}1\\0\\6\\\infty\\3\end{bmatrix}$

New Routing table of N_1

Dest.	Cost	Next
N_1	0	N_1
N_2	1	N_2
N_3	7	N_2, N_3
N_4	∞	–
N_5	4	N_3

$N_1 \to N_2$: $N_1 \to N_2$ and $N_2 \to N_2$
$1 + 0 = 1$

$N_1 \to N_3$: $N_1 \to N_2$ and $N_2 \to N_3$
$1 + 6 = 7$

$N_1 \to N_4$: $N_1 \to N_2$ and $N_2 \to N_4$
$1 + \infty = \infty$

$N_1 \to N_5$: $N_1 \to N_2$ and $N_2 \to N_5$
$1 + 3 = 4$

ii) At N_5, DVR of N_2 $\begin{bmatrix}1\\0\\6\\\infty\\3\end{bmatrix}$ and N_4 $\begin{bmatrix}\infty\\\infty\\2\\0\\4\end{bmatrix}$

New Routing Table of N_5

Dest.	Cost	Next
N_1	4	N_2
N_2	3	N_2
N_3	6	N_4
N_4	4	N_4
N_5	0	N_5

$N_5 \to N_1$: $N_5 \to N_2$ and $N_2 \to N_1$
$3 + 1 = 4$

$N_5 \to N_4$ and $N_4 \to N_1$
$4 + \infty = \infty$

$N_5 \to N_2$: $N_5 \to N_2$ and $N_2 \to N_2$
$3 + 0 = 3$

$N_5 \to N_4$ and $N_4 \to N_2$
$4 + \infty = \infty$

$N_5 \to N_3$: $N_5 \to N_2$ and $N_2 \to N_3$
$3 + 6 = 9$

$N_5 \to N_4$ and $N_4 \to N_3$
$4 + 2 = 6$

$N_5 \to N_4$: $N_5 \to N_2$ and $N_2 \to N_4$
$3 + \infty = \infty$

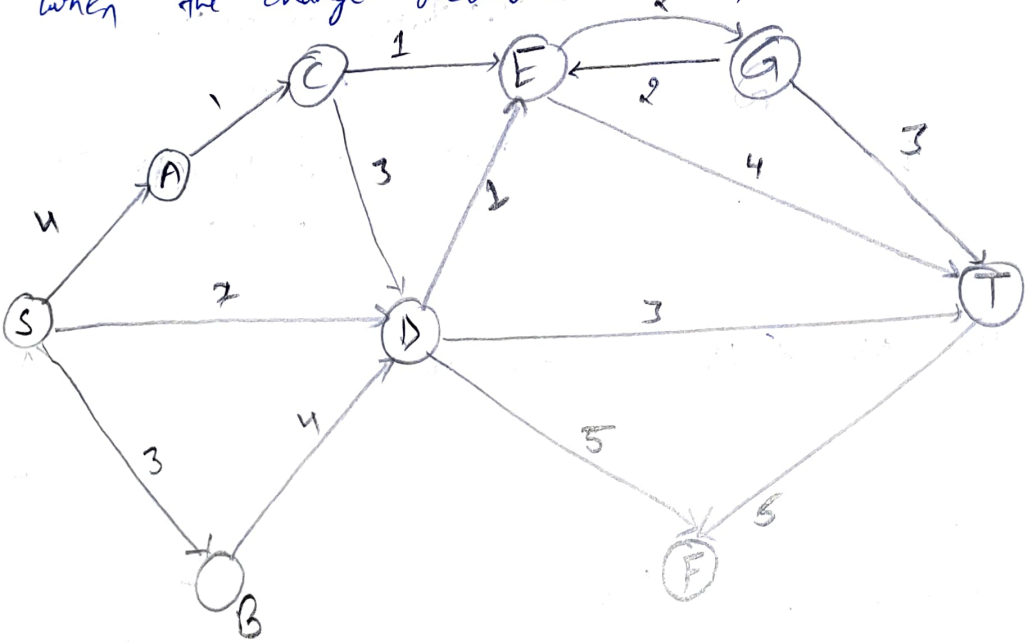
$N_5 \to N_4$ and $N_4 \to N_4$
$4 + 0 = 4$

* Link State Routing Algo:

It is a technique in which each router shares the knowledge of its neighbour with every other router in the internetwork.

Keys:

- **Knowledge about the neighborhood:** Instead of sending its routing table, a router sends the info. about its neighborhood only. A router broadcast its identities and cost of the directly attacked links to other routers.
- **Flooding:** Each router sends the info. to every other router on the internetwork except its neighbors. This process is known as flooding. Every router that receives the pkt sends the copies to all its neighbors. Finally, each & every router receives a copy of same info.
- **Info. Sharing:** A router sends the info. to every other router only when the change occurs in the info.



Source node

	S	A	B	C	D	E	F	G	T
	0	∞	∞	∞	∞	∞	∞	∞	∞
S-0		4	3		7				
B-3 No updates		4			7				
A-4				5	7				
C-5					7	6			
E-6					7			8	10
D-7							12	8	10
G-8	No updates						12		10
T-10	No updates							12	
F-12									

S - B - A - C - E - D - G - T - F

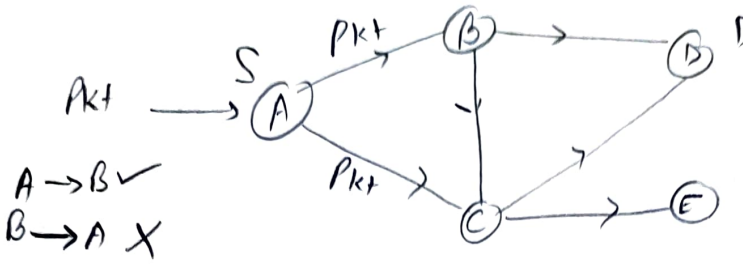
= 0 + 3 + 4 + 5 + 6 + 7 + 8 + 10 + 12

= 55

* Flooding Routing Algo:

→ It is a static routing algo.

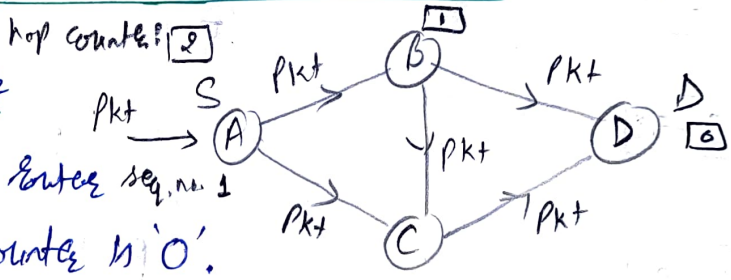
→ Every incoming pkt is sent on all outgoing lines except the line on which it has arrived



Disadvantage

Vast no. of ~~pkts~~ ~~are~~ duplicate pkts are generated.

How to Stop & eliminate duplicate pkts:



1) Using a hop Counter

↳ decrement in each router seq. no. 1

↳ discard pkt if Counter is '0'.

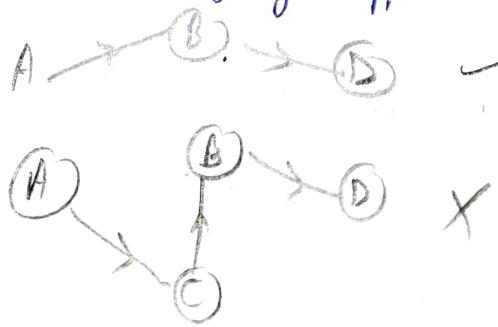
2) Sequence No. in pkt

↳ avoid sending the same pkt second time

↳ keep in each router per source a lists of pkts directly seen.

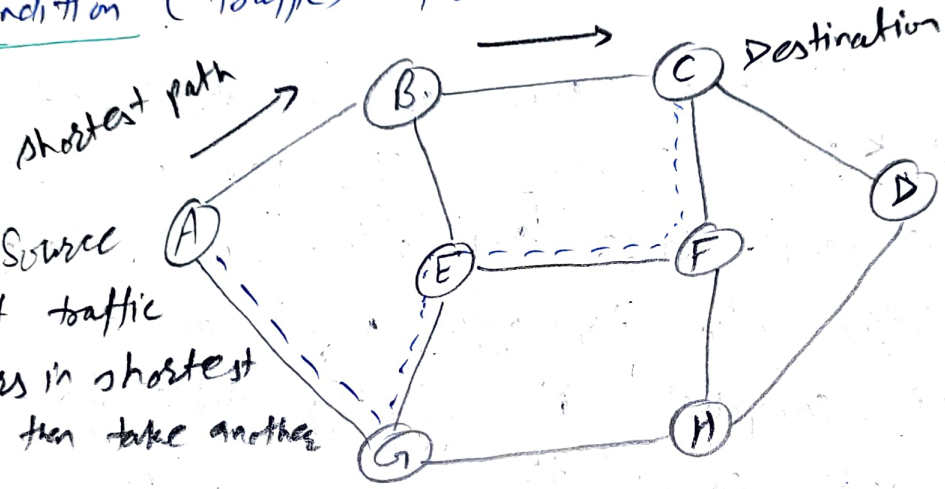
3) Selective flooding:

↳ use only those lines that are going approximately in right direction.



* Flow based Routing Algo:

This a Static algo whic uses topology and load Condition (traffic) for deciding a route.



But if traffic occurs in shortest path then take another path

To Use the technique of flow based Routing the follow info should be known in advance:

1) Subnet topology (diff. direction)
2) Traffic matrix (less traffic, more traffic)
3) Line capacity matrix. (BW should be known).

✳ Unicast Routing – Link State Routing:

Unicast means transmission from a single sender to a single receiver. It is a pt.-to-pt. comm^n b/w sender and receiver. There are various unicast protocols such as TCP, HTTP etc.

There are three major protocols for unicast routing:
1) Distance vector Routing (DVR)
2) Link state Routing (LSR)
3) Path-vector Routing.

Link State Routing: DVR use a distributed algo to compute their routing tables, LSR uses link-state routers to exchange msg. that allow each router to learn the entire n/w topology. Based on this topology, each router is compute its routing table by using a shorest path computation.

Features:

- **Link State packet:** a small pkt that contains routing info.
- **Link State database:** a collection info. gathered from link state pkt.
- **Shorest path first algo. (Dijkstra algo):** a calculatn performed on the DB results into shorest path
- **Routing table:** a list of known paths & interfaces.

Open shortest path first (OSPF) Routing Protocol:

- OSPF is a unicast routing protocol developed by working group of the Internet Engg. Task force. (IETF)
- It is a intradomain routing protocol.
- It is an open source protocol.
- It is similar to Routing Information Protocol (RIP).
- OSPF is a classless routing protocol, which means that in its updates, it includes the subnet of each route and enabling variable length subnet masks. With variable length subnet masks, an IP n/w can be broken into many subnets of various sizes. This provides n/w administrators with extra network-configuration flexibility. These updates are multicasts at specific addresses (224.0.0.5 and 224.0.0.6)
- OSPF is implemented as a prog. in the n/w layer using the services provided by the internet Protocol.
- IP datagram that carries the msg. from OSPF ~~state~~ sets the value of protocol field to 89.
- OSPF is based on SPF algo., which sometimes reffered as a Dijkstra algo.

- OSPF has two versions: version 1 and version 2. version 2 is mostly used.

OSPF Messages: OSPF is a very complex protocol. It uses five diff. types of msg. The

1) Hello message (Type 1): It is used by the routers to introduce itself to the other routers.

2) Database Description message (Type 2): It is normally send in response to the Hello msg.

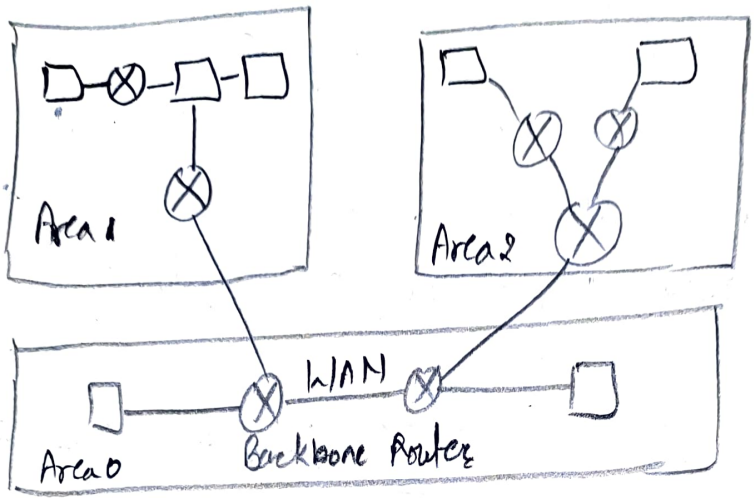
3) Link-state request message (Type 3): It is used by the routers that need info. about specific Link-State pkt.

4) Link-state update message (Type 4): It is main OSPF msg. for building Link-state database.

5) Link-state acknowledgement message (Type 5): It is used to create reliability in the OSPF protocol.

~~Comparison b/w Distance Vector Algo & Link State Routing Algo:~~

OSPF Areas:



- OSPF divides the autonomous sys. into areas where the area is a collection of n/w, host and routers. ~~Like~~ ~~intrane~~
- Routers that exist inside the area flood the area with routing info.
- In area, the special router also exist. They are present at the borders of an area, and are known as Area Border Routers. These router collect the info. about an area and share the info. with other areas.

All the areas inside an autonomous sys. are connected to the backbone routers. And these backbone routers are part of a primary area. This role of primary area is to provide comm^n b/w diff. areas.

How does OSPF work?

Step 1: "Become OSPF neighbors". The two connecting routers running OSPF on the same link creates a neighbors relationship.

Step 2: "Exchange database info!" After becoming the neighbors, the two routers exchange the LSDB info. with each other.

Step 3: "Choose the best route." Once the LSDB info. has been exchanged with each other, the router chooses the best route to be added to a routing table based on calculation of SPF.

Types of Links in OSPF: Connection b/w two routers

1) **Point-to-Point link:** It directly connects the two routers without any host or router in b/w.

2) **Transient link:** When several routers are attached in a nlw, they are known as transient links.

3) **Stub link:** It is a nlw that is connected to a single router. Data enters to the nlw through the single router and leaves the nlw through the same router.

4) **Virtual link:** If the link b/w two routers is broken, the administration creates the virtual path b/w

the routers, and path could be a long one also.

OSPF Message Format:

Version (8)	Type (8)	Message (16)
Source IP address		
Area Identification		
Check sum	Authentication type	
Authentication (32)		

- Version: 8 bit that specifies OSPF protocol version.
- Type: 8 bit that defines OSPF packet.
- Message: 16 bit field defines the total length of msg, including the header.
- Source IP address: Define the add. from which the packets are sent. It is a sending routing IP add.
- Area Identification: define area within which the routing take place.

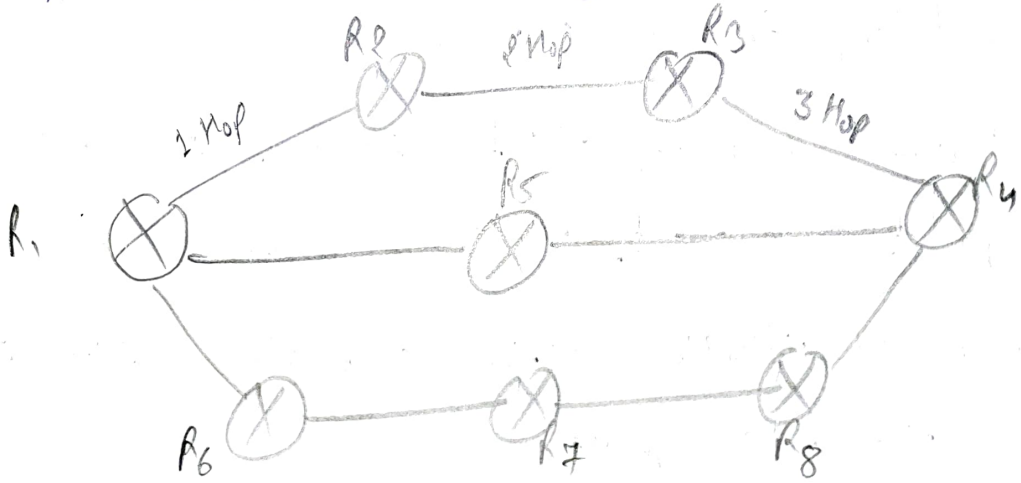
- Checksum: used for error correction and error detection.
- Authentication type: 0 and 1. 0 means for none that specifies no auth. is available. and 1 means for pwd that specifies the password-based authentication.
- Authentication: 32 bit field. contains the actual value of the authentication data.

* RIP Protocol:

- Stands for Routing Information Protocol.
- It is an intra-domain routing protocol used within an autonomous system. eg. web browsing within an institutional area.
- The main focus of RIP is to know the structure of the pkt, how many fields it contains, and how these fields determine the routing table.

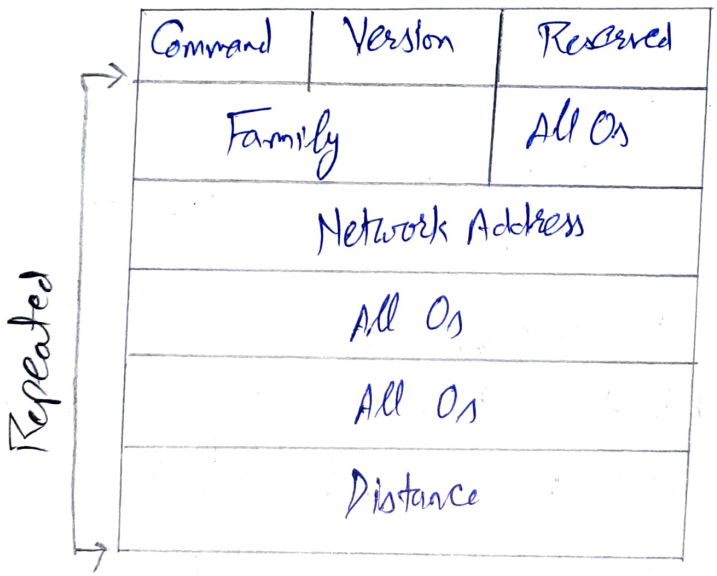
How is hop count determined?

When the router sends the pkt to the n/w segment, then it is counted as a single hop.



When the router 1 forward the pkt to the router 2 then it will count as 1 hop count. Similarly router 2, 3..... In the same way, RIP can support max. upto 15 hops, which means that the 16 router can be configured in a RIP.

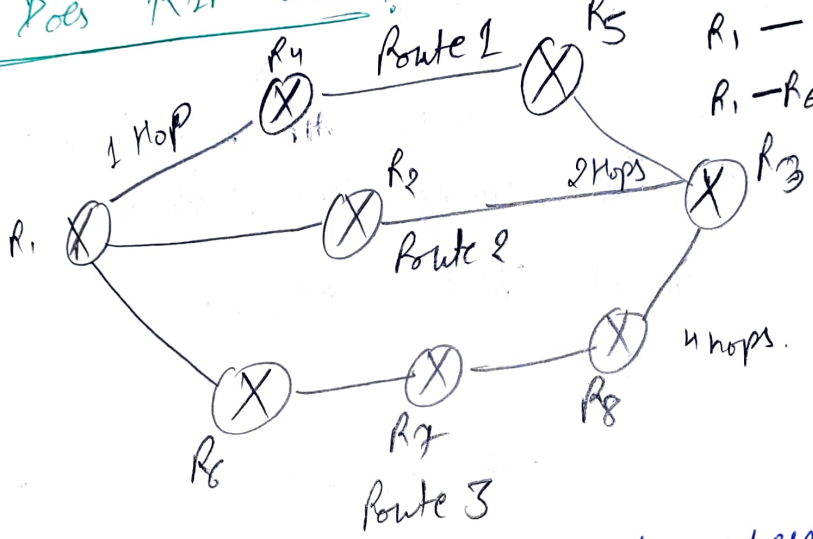
RIP Message Format: the msg. format is used to share info. among diff. routers.



- Command: 8 bit field used for request or reply. The value of the req. is 1 and value of reply is 2.
- Version: Which version we are using. Suppose we are using the protocol of version 1, then put 1 in this field.

- **Reserved:** It filled with zeros.
- **Family:** 16 bit field. used TCP/IP family so put 2 value in this field.
- **Network Address:** 14 bytes field. if use IPV4 version, then use 4 bytes and other 10 bytes are all 0s.
- **Distance:** it specifies hop count, i.e. no. of hops used to reach the destination.

How Does RIP work?



Hops

$R_1 - R_4 - R_5 - R_3$ - 3

$R_1 - R_2 - R_3$ = 2

$R_1 - R_6 - R_7 - R_8 - R_3$ -

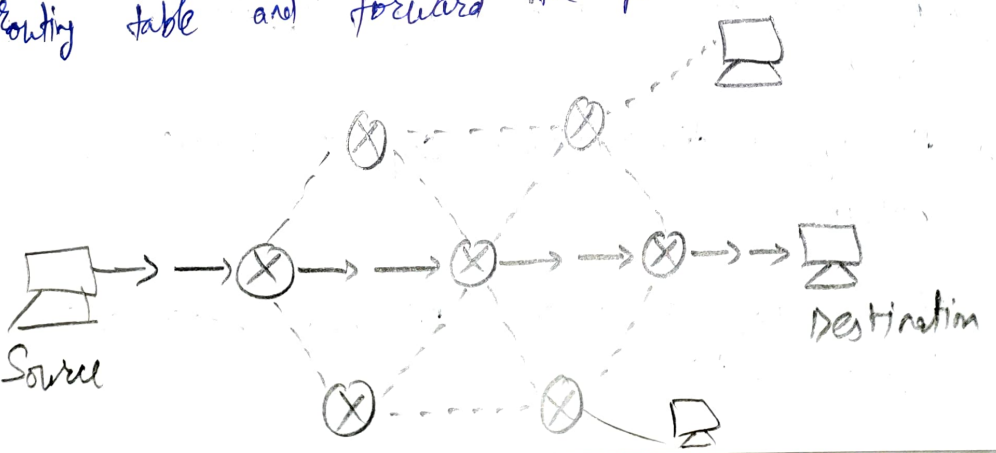
If there are 8 routers in a n/w where router 1 wants to send the data to router 3. If the n/w is configured with RIP, it will choose the route which has the least no. of hops. So RIP choose Route 2 bcoz it has only two hops.

* Comparison b/w Distance vector Routing Algo and Link State Routing Algo:

	DVR	LSR
1)	It uses a distance calculation plus an outgoing n/w interface (a vector) to choose the best path to a destination n/w.	It track the status and connection type of each link and produces a calculated metric based on these and other factors, including some set by the n/w administrator.
2)	Each Router maintains Routing table indexed by and containing one entry for each Router in the subnet.	It is the advanced version of DVR.
3)	Algo took too large to converge	Algo is faster.
4)	It support dis-contiguous subnets	Support contiguous subnets.
5)	It uses hop count & Composite metric	It uses metric cost.

) Bkl is less	wide Bkl is available.
) Routers measure delay directly with special ECHO pkts.	All delay measures and distributed to every router.
) It doesn't take line Bkl into account when choosing the routes.	It does.
) less scalable such as RIP supports 16 hops and EIGRP has max. of 100 hops.	very much scalable; support infinite hops.
) less money required.	more money required.

* Unicast Routing: Most of the traffic on the internets and Intranets known as unicast data or unicast traffic is sent with specified destination. Routing unicast data over the internet is called unicast routing. It is the simplest form of Routing bcoz the destination is already known. Hence the router just look up the routing table and forward the pkt to next hop.

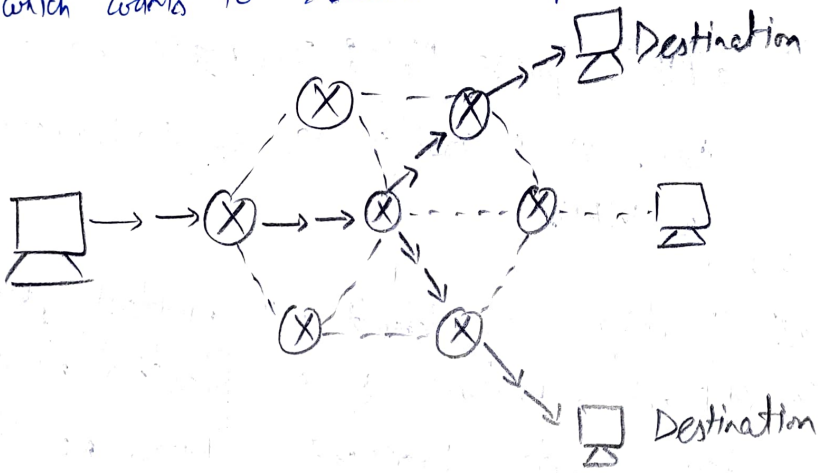


Unicast Routing Protocols

1) Distance Vector Routing Protocol
   ↳ Eg. RIP

2) Link State Routing Protocol
   ↳ Eg. OSPF

* **Multicast Routing:** The data is sent to only nodes which wants to receive the packets.



- The router must know that there are nodes, which wants to receive multicast pkts then only it should forward.
- It works on spanning tree protocol to avoid looping.
- It also uses reverse path forwarding technique, to detect & discard duplicates and loops.

Multicast Routing Protocols:

Unicast routing protocols use graphs while multicast routing protocols use tree i.e. spanning tree to avoid loops. The optimal tree is called shortest path spanning tree.

- DVMRP: Distance Vector Multicast Routing Protocol
- MOSPF: Multicast Open Shortest Path First
- CBT: Core Based Tree.
- PIM: Protocol Independent Multicast
  - PIM Dense Mode: This mode uses source based trees. It is used in dense environment such as LAN.
  - PIM Sparse Mode: This mode use shared tree. It is used in sparse environment such as WAN.

Broad Cast Routing: By default, the broadcast pkts are not routed and forwarded by the routers on any n/w. Routers create broadcast domains. Broadcast msg. is destined to all n/w devices. In this pkts are sent to all nodes even if they do not want it.

POORNIMA

POORNIMA
COLLEGE OF ENGINEERING

DETAILED LECTURE NOTES

Broadcast Routing can be done in two ways (algo):

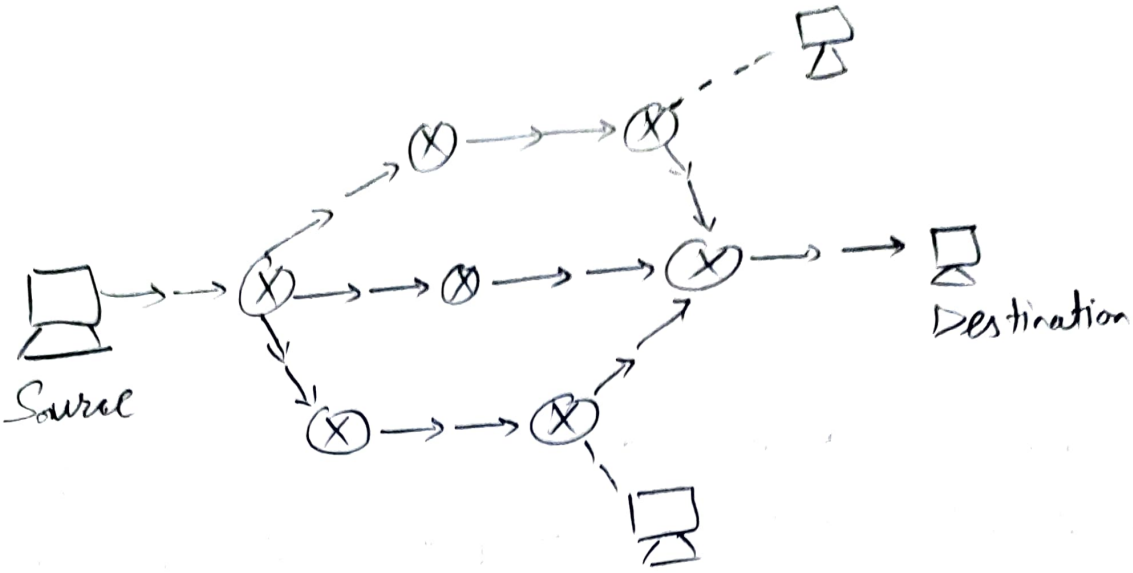
- A Router creates a data pkt and then sends it to each host one by one. In this case, the Router creates multiple copies of single data pkt with diff. destination addresses. All pkts are sent as unicast but beoz they are sent to all, it simulates as if Router is broadcasting.

  This method consumes lots of BW and Router must destination addl. of each node.

- When router receives a pkt i.e. to be broadcasted, it simply floods those pkts out of all interfaces. All routers are configured in same way.

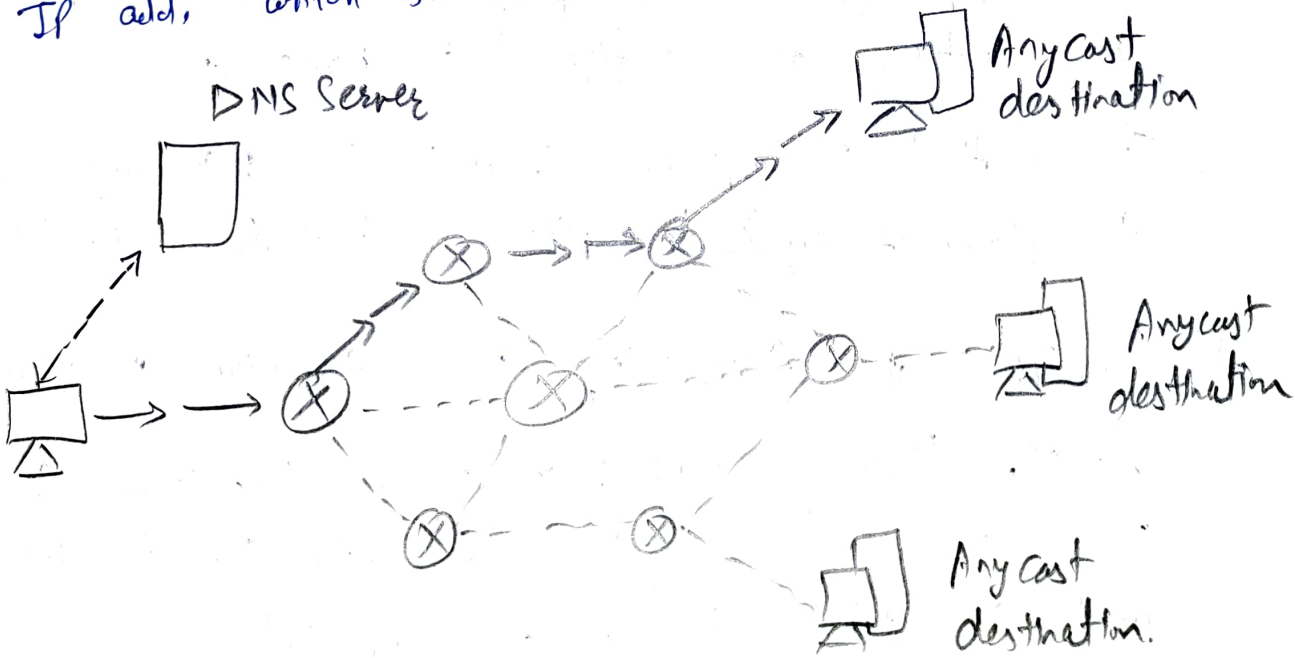
  This method is easy on Router's CPU but may cause the prob. of duplicate pkts received from preo routers.

Reverse path forwarding is a technique, in which Router knows in advance about its predecessor from where it should receive broadcast. This technique is used to detect & discard duplicates.



* Anycast Routing? multiple hosts can have same logical addr. When a pkt destined to this logical addr. is received, it is sent to the host which is nearest in routing topology.

Anycast Routing is done with help of DNS Server. Whenever an Anycast pkt is received it is enquired with DNS to where to send it. DNS provides the IP addr. which is nearest IP configured on it.



* Border Gateway Protocol (BGP):

It is an interdomain routing protocol, and it uses the the path-vector routing. It is a gateway protocol that is used to exchange routing info. among the autonomous sys. on the internet.

BGP Packet Format:

Marker (32)	
Length (16)	Type (8)

1) Marker : 32 bit field which is used for the authentication purpose.

2) Length : 16 bit field that defines the total length of msg, including the header.

3) Type : 8 bit field that defines the type of packet.

Types of packets: four types of pkt in BGP.

1) Open : When the router wants to create a neighbourhood relation with another router, it sends the open pkt.

2) Update: This is used in either of two cases:

i) It can be used to withdraw the destination, which has been advertised previously

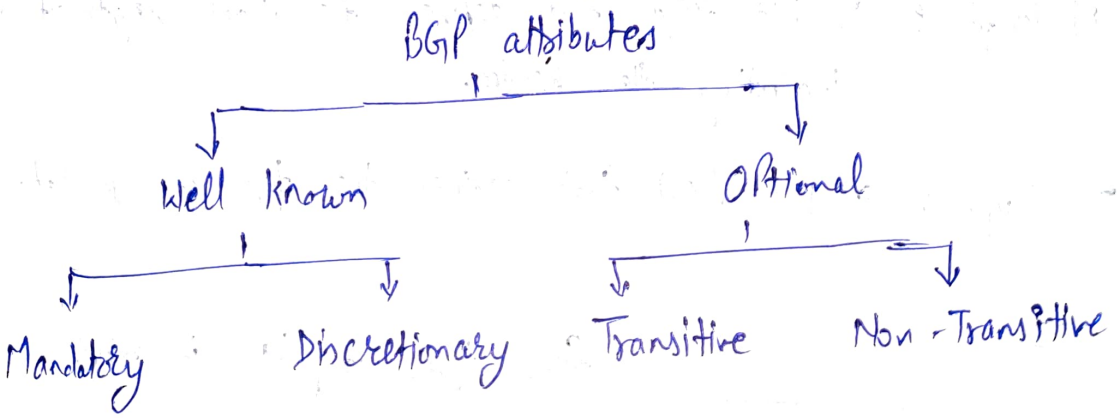
ii) It can also be used to announce the route to the new destination.

3) Keep alive: The keep alive pkt is exchanged regularly to tell other routers whether they are alive or not.

Eg. These are two routers R_1 & R_2. The R_1 sends the keep alive pkt to R_2 while R_2 sends the keep alive pkt to R_1 so that R_1 can get to know that R_2 is alive and R_2 can get to know that R_1 is alive.

4) Notification: The notification pkt is sent when the router detects the error condition or close the connection.

Path attributes: BGP chooses the best route based on attribute of the path.



POORNIMA

POORNIMA
COLLEGE OF ENGINEERING
DETAILED LECTURE NOTES

1) Well-known attribute: It recognized by every BGP router.

↳ well-known mandatory: When BGP is going to advertise any network, but it also advertises extra info, and that info. with path attributes info. The info. includes AS path info., Origin info., next-hop info..

Here, mandatory means it has to be present in all BGP routing updates.

↳ Well-known discretionary: It recognized by all the BGP routers and passed on to other BGP routers, but it is not mandatory to be present in an update.

2) Optional attribute: Not necessarily to be recognized by every BGP router.

↳ Optional Transitive: BGP may or may not recognize this attribute, but it is passed on to the other BGP neighbors. It marked as a partial.

↳ Optional Non-Transitive: If BGP cannot recognize the attribute, it ignores the update and does not advertise to another BGP Router.

BGP sessions: BGP means communication b/w the autonomous system.

1) Internal BGP Session: It exchange the info. b/w the routers inside an autonomous sys.

2) External BGP Session: Nodes or routers of diff. autonomous sys. communicate with each other.

Functionality of BGP:

1) The first fun^n consist of initial peer acquisition and authentication. Both the peers established a TCP connection and perform msg. exchange that guarantees both sides have agreed to communicate.

2) The second fun^n mainly focus on sending of +ve or -ve reach-ability info.

3) The third fun^n verifies that the peers and the n/w connection b/w them are functioning correctly!

* IPV4:

→ Connectionless Protocol used for pkt-switched n/w. eg. Ethernet.

→ It operates on a best effort delivery model, in which neither delivery is guaranteed, nor proper sequencing or avoidance of duplicate delivery is assured.

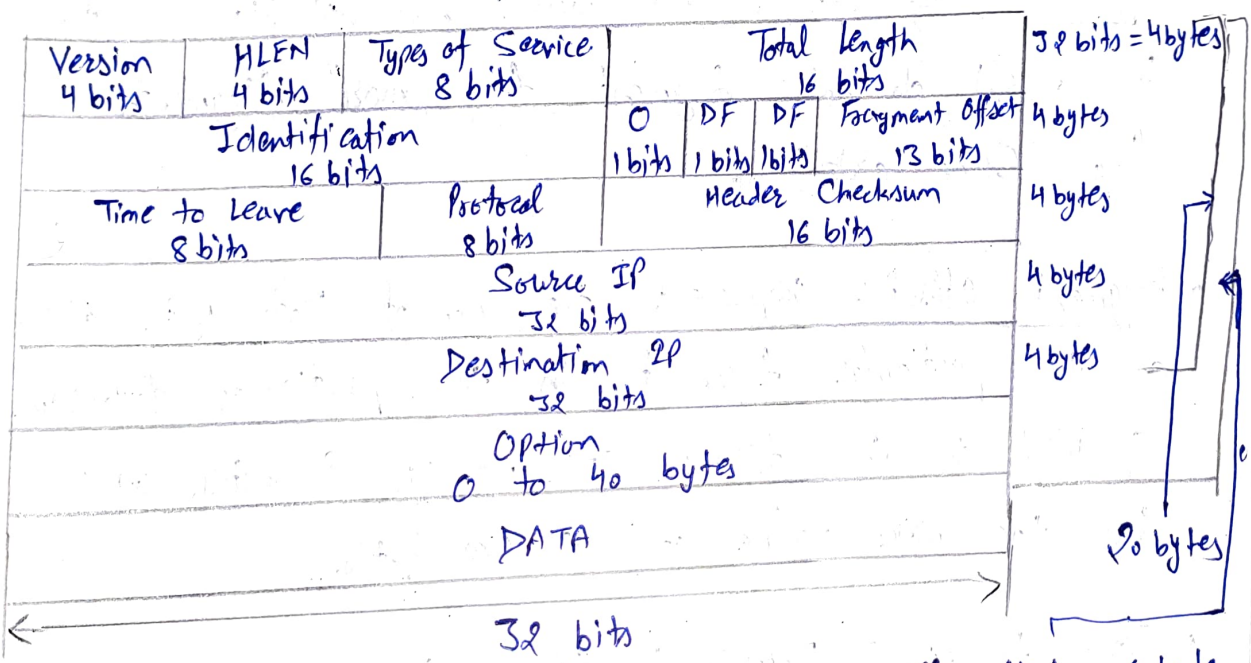
→ It provides a logical connection b/w n/w devices by

providing identification for each device.

→ IPv4 uses 32-bit (4 byte) addressing, which gives 2^{32} addresses.

→ IPv4 addresses are written in dot-decimal notation, which comprises of four octets of addr. expressed individually in decimal and separated by periods, for instance 192.168.1.5.

IPv4 Datagram Header:



Max. Header = 60 bytes
Min. Header = 20 Byte

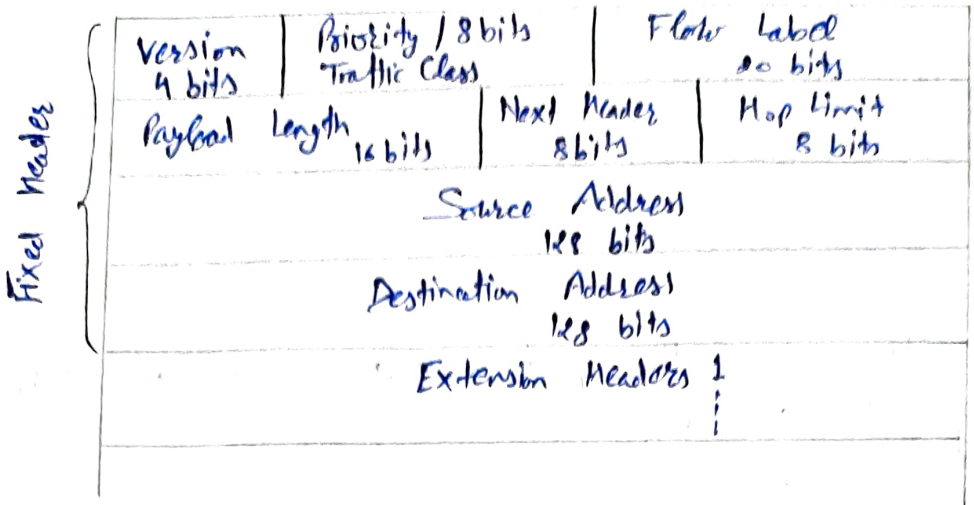
- Version: Version of the IP protocol (4 bits), which is 4 for IPv4.
- HLEN: IP Header length (4 bits), which is the no. of 32 bit words in the Header. The min value for this field is 5 and max. is 15.
- Type of Service: Low Delay, High Throughput, Reliability is (8 bits).
- Total Length: Length of header + Data (16 bits), which has a min. value 20 bytes and max. is 65,535 bytes.
- Identification: Unique pkt Id for identifying the group of fragments of a single IP datagram (16 bits)
- Flags: 3 flags of 1 bit each: reserved bit (must be zero), do not fragment flag, more fragments flag (same order)
- Fragment Offset: Represents the no. of Data Bytes ahead of the particular fragment in the particular datagram. Specified in the terms of no. of 8 bytes, which has the max. value of 65,528 bytes.
- Time to Live: Datagram's lifetime (8 bits), It prevents the datagram to loop through the n/w by restricting the no. of Hops taken by a pkt before delivering to the Destination.

- Protocol: Name of the protocol to which the data is to be passed (8 bits).
- Header Checksum: 16 bits header checksum for checking errors in the datagram header.
- Source IP address: 32 bits IP address of the Sender.
- Destination IP address: 32 bits IP address of the recei
- Option: Optional info. such as source route, record route. Used by the n/w administrator to check whet a path is working or not.

* IPV6:

⇒ IPV6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of comple and efficiency.

IPV6 Header Format



- **Version (4 bits):** It contains bit sequence 0110.
- **Traffic Class (8 bits):** It is similar to service Field in IPV4 packet. It helps routers to handle the traffic based on Priority of the pkt: If congestion (blockage, limitation) occurs on router than pkts with least priority will be discarded.
- **Flow Label (20 bits):** Flow Label field is used by source to label the pkts belonging to the same flow in order to request special handling by intermediate IPV6 routers, such as non-default quality of service or real time service.

Intermediate router can use source addr., destination addr. and flow label of the pkts. B/w a S and D multiple flows may exist because many processes might be running at the same time.

Routers or Host that do not support the functionality of

flow label field and for default router handling, flow label field is set to 0. While setting up the flow label, source is also supposed to specify the life time of flow.

- **Payload Length (16 bits):** It is a 16 bit (unsigned integer) field, indicates the total size of payload which tells routers about info. of pkt a particular pkt contain in its payload.

  Payload length field include extension header (if any) and upper layer pkt. If payload length is greater than 65,535 bytes, then payload length field will be set to 0.

- **Next Header (8 bits):** Indicates the type of extension header (if present). Whereas in some cases it indicate the protocol contained within upper-layer pkt, such as TCP, UDP.

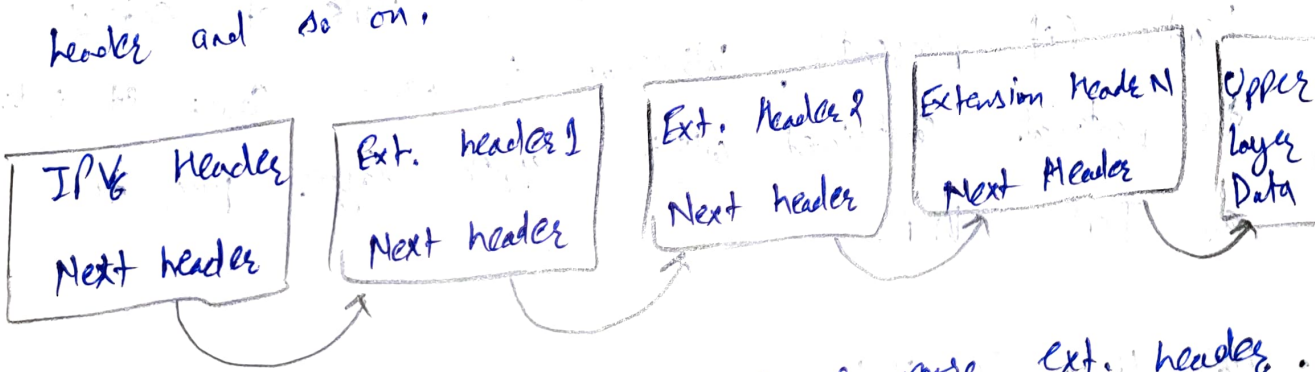
Hop Limit (8 bits): It is same as TTL in IPV4 pkt. It indicates the max. no. of intermediate nodes IPV6

pkt is allowed to travel. Its value gets decremented by one, by each node that forwards the pkt and pkt is discarded if value decrements to 0. This is used to discard the pkt that are stuck in infinite loop bcoz of some routing error.

- Source address (128 bits): Source add. is 128 bits IPV6 add. of the original source of pkt.

- Destination address (128 bits): Destination add. field indicates the IPV6 add. of the final destination. All the intermediate nodes can use this info. in order to correctly route the pkt.

- Extension Headers: In order to rectify the limitation of IPV4 option field, Extension Headers are introduced in IPV6. It is very imp. mechanism. Next header field of IPV6 fixed header pt. to the first extension header and this first extension header pt. to the second extension header and so on.



IPV6 pkt may contain zero, one or more ext. headers. but these should be present in their recommended order

Ext. Header	Description
Hop-by-Hop option	Examined by all devices on the path
Destination options (with Routing option)	Examined by destination of the pkt.
Routing Header	Methods to take Routing decision.
Fragment Header	Contains parameters of fragmented datagram done by source.
Authentication Header	Verify authenticity
Encapsulating Security Payload	Carries encrypted data.

* Difference b/w IPV4 & IPV6:

IPV4	IPV6
1) 32 bit address	128 bit address
2) numeric add. that consists of 4 fields which are seperated by dot (.).	alphanumeric add. that consists of 8 field, which are seperated by Colon.

3) 5 diff. classes of IP add. that include Class A, B, C, D, E.	does not contain classes.
4) limited no. of IP add.	large no. of IP add.
5) Supports VLSM (Virtual Length Subnet Mask)	does not support.
6) manual & DHCP confi.	supports manual, DHCP, auto confi. and renumbering.
7) generates 4 billion unique add.	340 ~~de~~ undecillion.
8) end-to end connection integrity is unachievable.	achievable.
9) IP add. is represented in decimal.	Hexadecimal.
10) Security depends on app.	IPSEC is developed for security purpose.
11) Fragmentat^n is done by senders and forwarding routers	done only by senders.
12) Broadcasting	Multicasting.
13) 4 octets.	8 fields. each field contains 2 octets.

* Address Mapping:

→ An internet is made up of a combination of physical networks connected by internetworking devices such as routers. A pkt starting from a source host may pass through several diff. phy. n/w before finally reaching the destination host. The hosts & routers are recognized at the n/w level by their logical (IP) addresses.

→ A physical add. is a local add. It must be unique locally. It is called a phy. add. because it is usually implemented in H/W. An eg. of phy. add. is the 48-bit MAC add. in the Ethernet protocol, which is imprinted on the NIC (Network Interface Card) installed in the host or router.

→ The phy. add. & logical add. are two diff. identifiers. This means that delivery of a pkt to a host or a router requires two level of addressing: logical & physical.

→ A logical add. is map to its corresponding phy. add. and vice versa. These can be done by using either static or dynamic mapping.

1) → Satic mapping involves in the creation of a table that associates a logical addd. with a phy. addd.

2) This table is stored in each m/c on the n/w. "A static mapping table must be updated periodically."

→ in dynamic mapping each time a m/c knows one of the two addresses (logical or physical). It can use a protocol to find the other one.

Mapping Logical to Physical Address : ARP

→ Anytime a host or a router has an IP datagram to send to another host or router, it has the "logical (IP) addd. of the receiver." The logical (IP) addd. is obtained from the DNS if the sender is the host or it is found in a routing table if the send is a router.

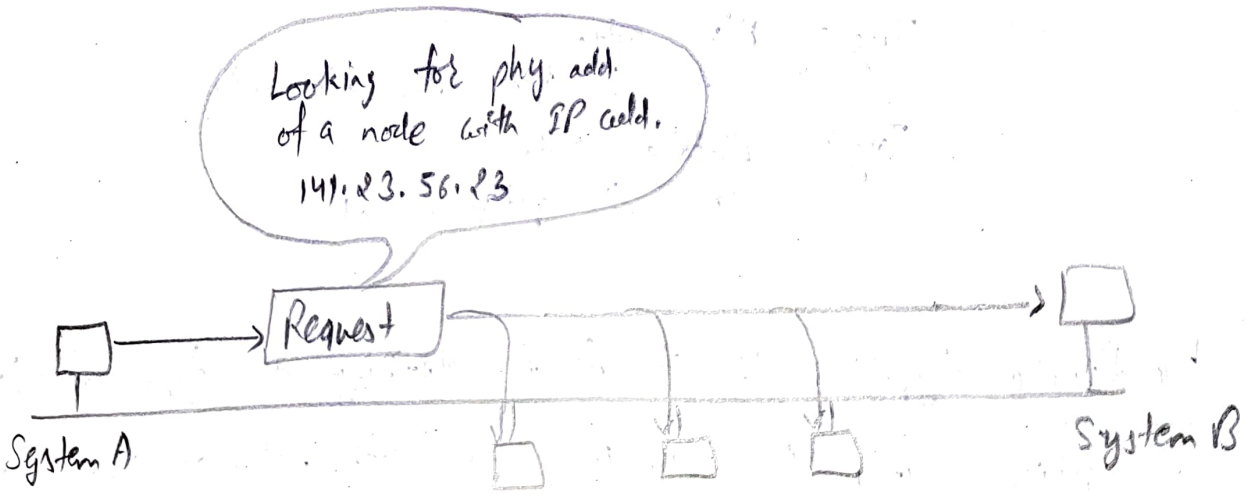
The IP datagram must be encapsulated in a frame to be able to pass through phy. n/w. This means that the sender needs the phy. addd. of the receiver.

The host and the router sends an ARP query pkt. The pkt includes the phy. and IP addd. of the sender and IP addd. of the receiver. Because the sender does not know the phy. addd. of the receiver, the query is

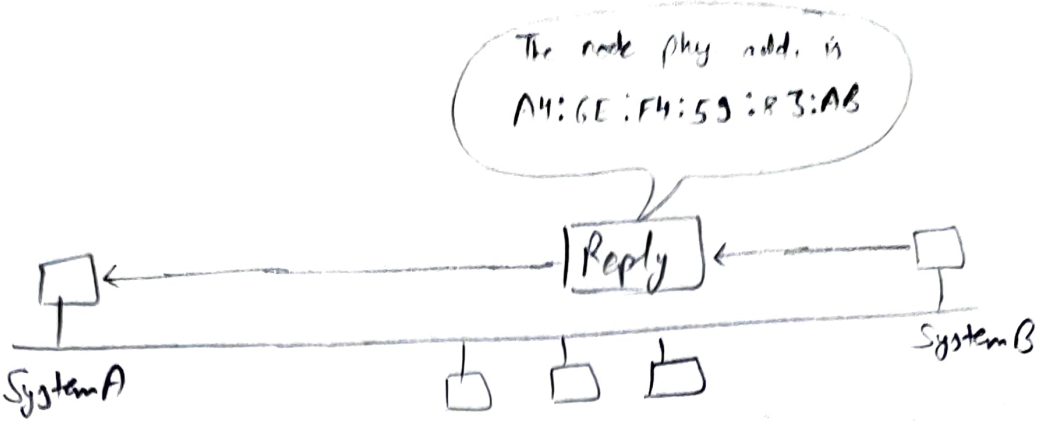
broadcast over the n/w.

→ Every host or router on the n/w receives and processes the ARP query pkt. but only the intended recipient recognized its IP add. and sends back an ARP response pkt. "The response pkt. contains the recipient's IP and phy. add." The pkt. is unicast directly to the inquirer by using the phy. add. received in the query pkt.

ARP (Address Resolution Protocol) Operation:



[ARP request is broadcast]



[ARP reply is unicast]

ARP Packet:

← 8 bits →	← 8 bits →	← 16 bits →
H/W Type		Protocol Type
H/W Length	Protocol Length	Operation Req. 1, Reply 2
Sender H/W addr. eg. (6 bytes for Ethernet)		
Sender protocol addr. eg. (4 bytes for IP)		
(Not filled in req.) Target H/W addr. eg. (6 bytes for Ethernet)		
Target Protocol addr. eg. (4 bytes for IP)		

Hardware type: 16 bit field defining the type of n/w. on which ARP is running. eg. Ethernet is type 1.

Protocol type: 16 bit field defining the protocol. eg. IPV4 is 0800_{16}.

Hardware length: 8 bit field defining the length of phy. addr. in bytes. eg. for ethernet value is 6.

- **Protocol length:** 8 bit field defining the length of logical addr. in bytes. Eg. for IPV4 the value is 4.

  Operation: 16 bit field defining the type of pkt.
  1) ARP request 2) ARP reply

- **Sender H/W addr.:** This is a variable length field defining the phy. addr. of the sender. Eg. for ethernet this field is 6 bytes long.

- **Sender Protocol addr.:** This is a variable-length field defining the logical addr. of the sender. Eg. for IP protocol, the field is 4 bytes long.

- **Target H/W addr.:** This is variable-length field defining the phy. addr. of the target. Eg. Ethernet, this field is 6 bytes long.

Target Protocol addr.: This is a variable-length field defining the logical addr. of the target. Eg. for IPV4, field is 4 bytes long.

Encapsulation of ARP Packet:

An ARP pkt. is encapsulated directly into a data link frame.

Steps:

1) The sender knows the IP add. of the target.

2) IP asks ARP to create an ARP req. msg., filling in the sender phy. addd., the sender IP addd. and the target IP addd.

3) The msg. is passed to the DLL where it is encapsulated in a frame by using the phy. addd. of the sender "as the source addd. and the phy. broadcast addd. as the destination addd."

4) Every host or router receives the frame. Because the frame contains a broadcast destination addd., all stations remove the msg. and pass it to ARP. "All m/c except the one targeted drop the pkt." The target m/c recognizes its IP addd.

5) The target m/c replies with an ARP reply msg. that contains its phy. addd. "The msg. is unicast."

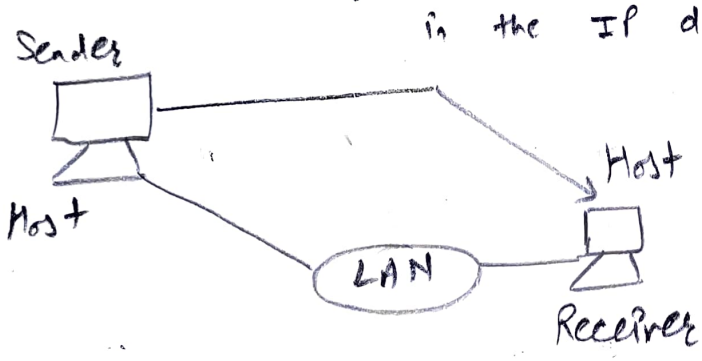
6) "The sender receives the reply msg." It knows the phy. addd. of the target m/c.

7) "The IP ~~addd.~~ datagram, which carries data for the target m/c, is now encapsulated in a frame and is unicast to the destination."

Four different cases in which the services of ARP can be used:

1) The sender is a host and wants to send a pkt to another host on the same network. The logical add. that must be mapped to a phy. add. is the destination IP add. in the datagram header.

Target IP add: Destination add. in the IP datagram

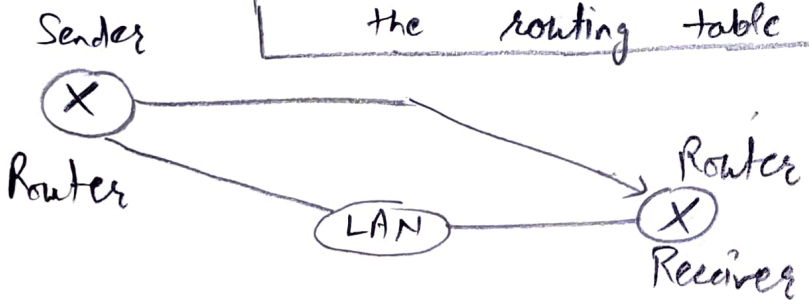


2) The sender is a host and wants to send a pkt. to another host on another nlw. The host looks at its routing table and finds the IP add. of the next hop (router) for this destination. If it does not have a routing table, it looks for the IP add. of the default router. The IP add. of the router becomes the logical add. that must be mapped to a phy. add.

Target IP add: IP add. of a router

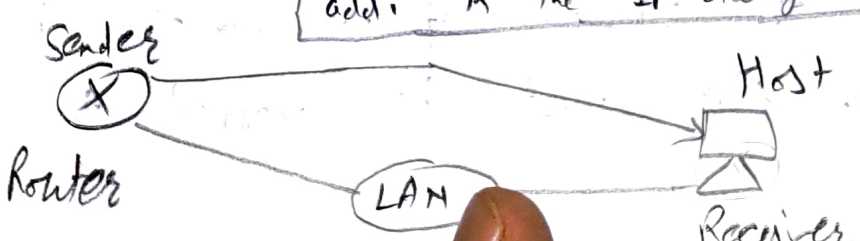
3) The sender is a router that has received a datagram destined for a host on another n/w. It checks its routing table and finds the IP add. of the next router. The IP add. of the next router becomes the logical add. that must be mapped to a phy. add.

Target IP add: IP add. of appropriate router found in the routing table



4) The sender is a router that has received a datagram destined for a host on the same n/w. The destination IP add. of the datagram becomes the logical add. that must be mapped to a physical add.

Target IP add: Destination add. in the IP datagram



POORNIMA
COLLEGE OF ENGINEERING
DETAILED LECTURE NOTES

Mapping Physical to Logical Address : RARP, BOOTP and DHCP :

A host know its physical add. but needs to know its logical add. This may happen in two cases :

1) "A diskless station is just booted". the station can find its phy. add. by checking its interface, but it does not know its IP add.

2) "An organizat" does not have enough IP addresses to assign to each station." It needs to assign IP add. on demand. The station can send its phy. add. and ask for a short time lease.

Reverse Address Resolution Protocol (RARP) :

It finds the logical add. for a mk that knows only its phy. add.

Each host or Router is assigned one or more logical (IP) add, which are unique and independent of the phy. (h/w) add. of the mlc.

→ To create an IP datagram, a host or a router needs to know its own IP addr.

→ A diskless m/c is usually booted from ROM, which has min. booting info.

→ The m/c get its phy. addr which is uniquely locally. Then it can use the phy. addr. to get the logical addr. by using the RARP protocol.

→ A RARP req. is created and broadcast on the local n/w. Another m/c on the local n/w that knows all the IP addr. will respond with a RARP reply. The requesting m/c must be running a RARP client prog. the responding m/c must be running a RARP server prog.

→ There is a serious prob. with RARP: Broadcasting is done at the data link layer.

→ If an administrator has several n/w or several subnets, it needs to assign a RARP server for each n/w or subnet. Two protocols BOOTP and DHCP are replacing RARP.

~~Bootstrap~~

Bootstrap Protocol (BOOTP):

→ The Bootstrap protocol is a client/server protocol designed to provide phy. addr. to logical addr. mapping. 'BOOTP is an app. layer protocol.'

→ The administrator may put the client and the server on the same nw or on diff. nw.

→ 'BOOTP msg. are encapsulated in a UDP pkt. and the UDP pkt. itself is encapsulated in an IP pkt.'

→ 'Although a client sends an IP datagram, it knows neither its own IP (source) addr. nor the server's IP (destination) addr.'

→ advantage of BOOTP over RARP is client and server are app.-layer processes.

→ 'The BOOTP req. is broadcast because the client does not know the IP addr. of the server.'

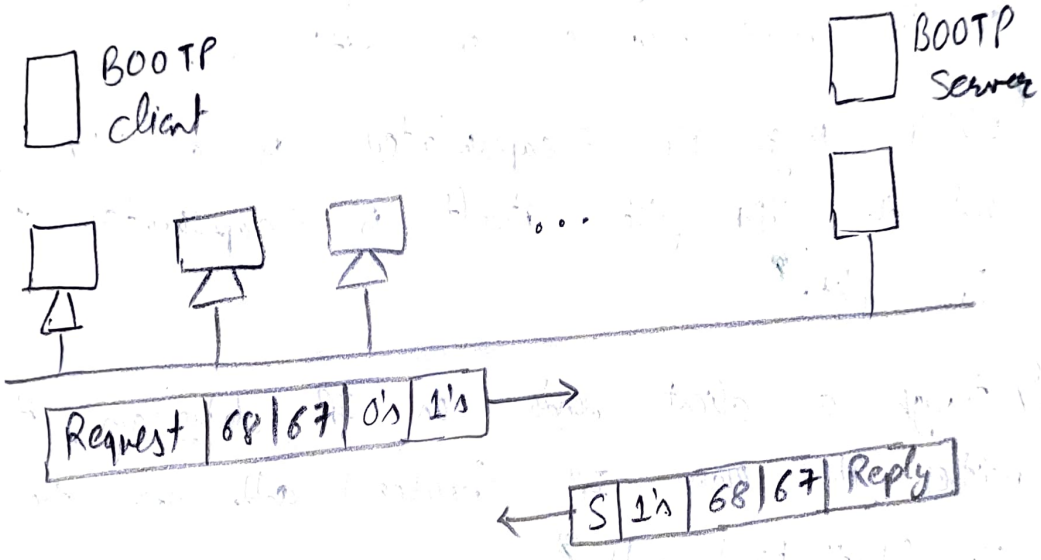
→ The relay agent knowing the unicast addr. of a BOOTP server. When it receives this type of pkt., it

encapsulates the msg. in a unicast datagram and sends the req. to the BOOTP server.

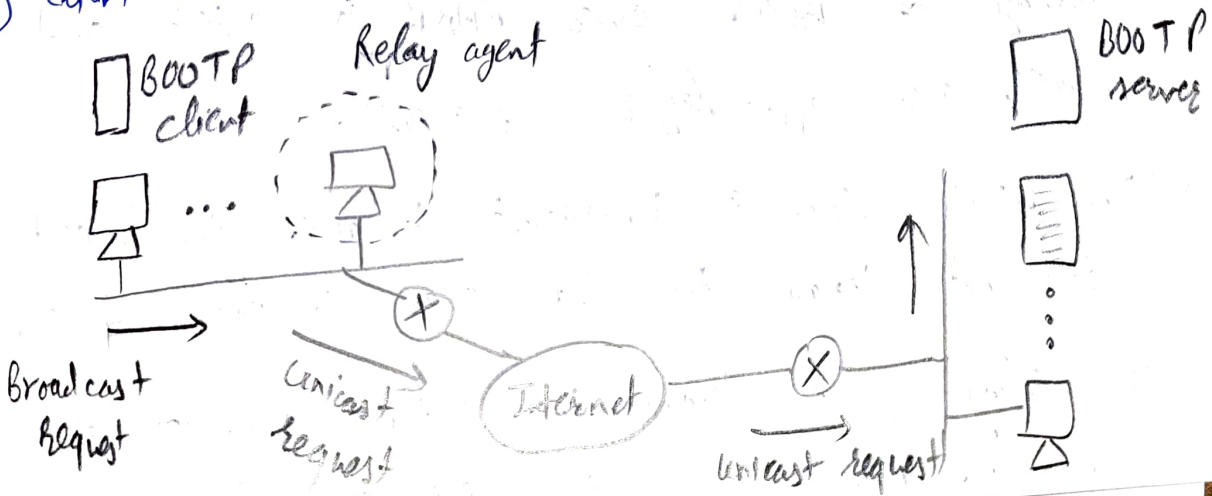
→ The pkt. carrying a unicast dest. addr., is routed by any router and reaches the BOOTP server.

→ The BOOTP server knowns the msg. comes from a relay agent bcoz one of the fields in the req. msg. defines the IP addr. of the relay agent. The relay agent, after receiving the reply, sends it to the BOOTP client.

a) Client and Server on the same n/w:



b) Client and Server on diff. n/w:



Dynamic Host Configuration Protocol (DHCP):

→ DHCP has been devised to provide static and dynamic add. allocation that can be manual or automatic.

- **Static Address Allocation:** DHCP is backward compatible with BOOTP, which means a host running the BOOTP client can request a static add. from a DHCP server. "A DHCP server has a database that statically binds phy. add. to IP add."

- **Dynamic Address Allocation:** A DHCP has a second DB with a pool of available IP add. This second DB makes DHCP dynamic. When a DHCP client requests a temporary IP add, the DHCP server goes to the "pool of available (unused) IP add. and assign an IP add. for a negotiable period of time."

→ "When a DHCP client sends a req. to a DHCP server, the server first checks its static DB." If an entry with the req. phy. add. exists in the static DB, the permanent IP add. of the client is

returned. If the entry does not exist in the static DB, the server selects an IP addr. from the available pool, assign the addr. to the client, and adds the entry to the dynamic DB.

→ The addr. assigned from the pool are temp. addr. The DHCP server issues a lease for a specific time.

When the lease expires, the client must either stop using the IP addr. or renew the lease.

The server has the option to agree or disagree with the renewal. If the server disagrees, the client stops using the addr.

* Congestion Control:

What is Congestion?: A state occurring in n/w layer when the myg. traffic is so heavy that it slows down n/w response time.

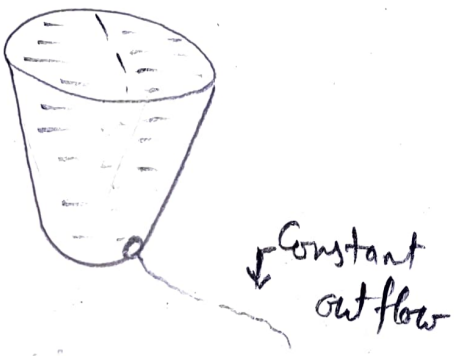
Effects of Congestion:

→ As delay ↑↑, performance ↓↓.

→ If delay ↑↑, retransmission occurs, making situation worse.

2) Congestion Control Algo:

1) Leaky Bucket Algo: Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate. When the bucket is full with water additional water entering spills over the sides and is lost.



Similarly, each n/w interface contains a leaky bucket.

1) When host want to send pkt, pkt is thrown into the bucket.

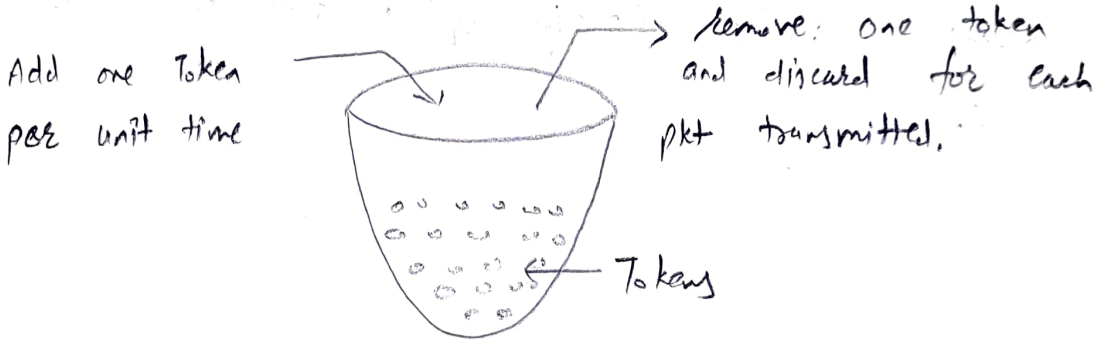
2) The bucket leaks at a constant rate, meaning the n/w interface transmits pkt at a constant rate.

3) Bursty traffic is converted to a uniform traffic by leaky buckets

4) The bucket is a finite queue that o/p at a finite rate.

2) Token Bucket Algo: The leaky bucket algo. enforces o/p pattern at the avg. rate, no matter how bursty the traffic is. So in order to deal with bursty traffic we need a flexible algo. so that data is not lost. This is called a Token bucket algo.

1) In regular intervals tokens are thrown into the bucket.
2) The bucket has a max. capacity.
3) If there is a ready pkt., a token is removed from the bucket, and the bucket is sent.
4) If there is no token in the bucket, the bucket can not be sent.



Congestion Control Techniques: Used to control or prevent Congestion. (movement is difficult. / block)

Congestion Control Techniques

Open loop Congestion Control
- Retransmission Policy
- Window Policy
- Discarding Policy
- Ack. Policy
- Admission Policy

Closed loop Congestion Control
- Backpressure
- Choke pkt. technique
- Implicit Signaling
- Explicit Signaling
  - Forward
  - Backward

1) Open loop Congestion Control: It apply to prevent congestion before it happens. The congestion control is handled either by the source or the destination.

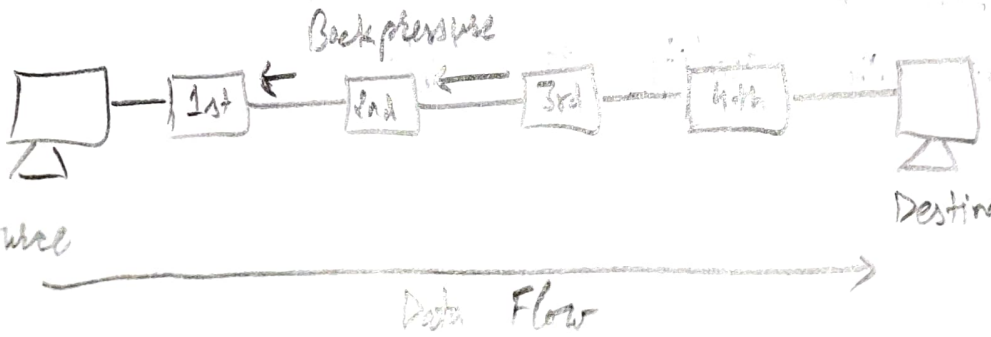
- Retransmission Policy: If the sender feels that a sent pkt is lost or corrupted, the pkt needs to be retransmitted. This transmission may increase the congestion in the n/w.
- Window Policy: Several pkt. in the Go-back-n window are resent, although some pkts may be received successfully at the receiver side. This duplicate may ↑↑ the congestion in the n/w and making it worse.
- Discarding Policy: A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discards the corrupted or less ~~&~~ sensitive package and also able to maintain the quality of mgs.

- Acknowledgment Policy: The receiver should send ack. for N pkt. rather than sending ack. for a single pkt. The receiver should send a ack. only if it has to sent a pkt or a timer expires.

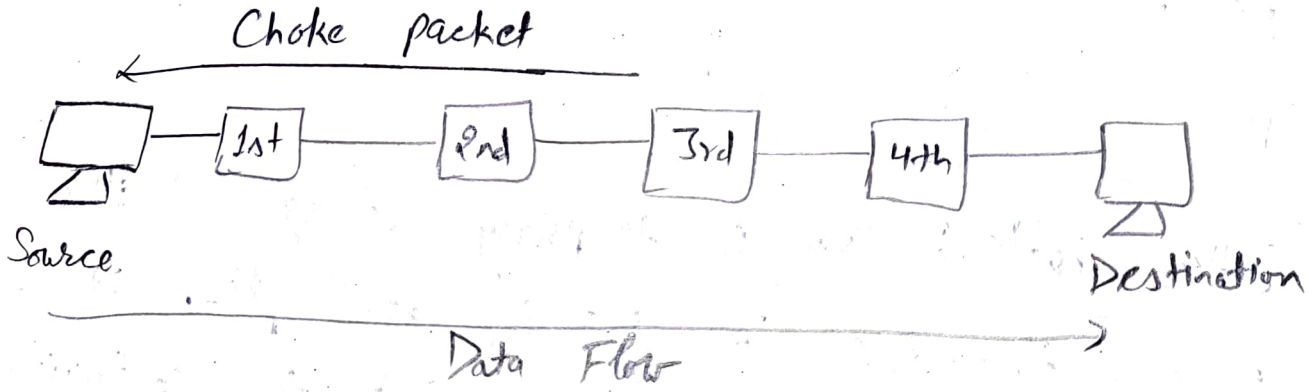
- Admission Policy: Switches in a flow should first check the resource requirement of a nlw flow before transmitting pt further. If there is a chance of a Congestion or there is a Congestion in the nlw, router should deny establishing a virtual nlw connection es to prevent further Congestion.

2) Closed loop Congestion Control: It used to treat or alleviate (relieve) Congestion after pt happens.

- Backpressure: In this a Congestion node stop receiving pkt from upstream node. This may cause the upstream node or nodes to become congested and rejects receiving data from above nodes. Backpressure is a node-to-node Congestion Control technique that propagate in the opp. direction of data flow. This tech. is applied only to virtual circuit where each node has info. of its above upstream node.



- **Choke Packet Technique:** It is applicable to both virtual n/w as well as datagram subnets. A choke pkt is a pkt sent by a node to the source to inform it of congestion. Each router monitor its resources and the utilization of each of its o/p lines. Whenever the resource utilization exceeds the threshold value which is set by administrator, the router directly sends a pkt. to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the pkt has traveled are not warned about congestion.



- **Implicit Signalling:** There is no comm^n b/w the congested nodes and the source. The source guesses that there is congestion in a n/w. for eg. when sender sends several pkt. and there is no ack. for a while, one assumption is that there is a congestion.

- **Explicit Signaling:** If a node experiences congestion it can explicitly sends a pkt. to the source or destination to inform about congestion.

  ↳ **Forward Signaling:** Signal is sent in the direction of the congestion. The destination is warned about congestion. The receiver in this case adopt policies to prevent further congestion.

  ↳ **Backward Signaling:** Signal is sent in the opp. direction of congestion. The source is warned about congestion and it needs to slow down.

* Quality of Service (QoS):

QoS is reffered as efficiency. We define QoS as, "How well or efficiently data transmissions are taking place."

How to achive QoS?

- **Jitter buffer:** This is temporary storage buffer which is used to store the incoming data pkts. It is used in pkt-based n/w to ensure that the continuity of the data streams doesn't get disturbed, it does by smoothing out the pkt arrival times during periods of nw congestion.

- **Traffic Shaping:** This technique is also known as packet shaping, is a congestion control or management technique that helps to regulate n/w data transfer by delaying the flow of least imp. or least necessary data pkts.

There are 2 types of QoS Solutions:

1) **Stateless solution:** The server is not required to keep or store the server info. or sessin deteils to itself. The routers maintain no fine-grained state about traffic, One positive factor of this is, it's scalable and robust. But also it has weak services as there is no guarantee about the kind of performance delay in a particular app which we encounter. In this, server and client are loosly coupled.

2) **Stateful Solution:** The server is required to maintain the current state and session info. The routers maintain per-flow state. It provide the powerful services such as guranteed services and high resource utilization, provide

protection, and it is much less scalable and rob the server and client are tightly bounded.

QoS Parameters:

1) Packet loss: It happens when the nlw links becom congested and the routers and switches start dropping pkt. When these pkts are dropped during real-ti comm", such as audio or video, these session can experience jitter and gaps in speech.

2) Jitter: It occurs as the result of nlw congestion, timing drift, and route changes. Too much jitter can degrade the QoS quality of audio comm".

3) Latency: It is the time delay, which is taken by packet to travel from its source to its destination. For a great system, latency should be as low as possible, idealy it should be close to zero.

4) Bandwidth: It is the capacity of a nlw channel to transmit max. possible data through the channel in a cer amount of time.

5) Mean Opinion score: It is a metric for rating the audio quality which uses a five-point scale, with a five indicating the highest or best quality.

Implementing QoS:

1) Best Effort: By applying this model, we are prioritizing all the data pkts equally. But there is no guarantee that all the data pkts will be delivered. The best effort deliver all of that data pkts.

The best-effort model is applied when n/w haven't configured with QoS policies or incase their n/w infrastructure does not support QoS.

2) Integated Services: This QoS model reserves the BW along a specific path on the n/w.

While implementing integeated services model, the IntServ-capable routers and rescarce reservation protocol is necessary. This model has limited scalability and high consumption of the n/w resources.

3) Differentiated Services: In this, the n/w elements such as routers and switches are configured to serve multiple categories of traffic with diff. priority orders.

* **Internetworking:** It is combined of 2 words, inter and networking which implies an association b/w totally diff. nodes or segments.

Internetworking started as a way to connect disparate types of computer networking technology. Computer n/w term is used to describe two or more computers that are linked to each other.

When two or more computer LANs or WANs or Comp. n/w segments are connected using devices such as Router and configure by logical addressing scheme with a protocol such as IP, then it is called as computer Internetworking.

Internetworking is enforced in layer three (N/w layer) of OSI - Iso model.

Types:

1) **Extranet:** It is a n/w of Internetwork or Internetworking that is limited in scope to a single organisation or entity but which also has limited connections to the n/w of one or more but not necessarily, trusted organizations or entities.

An extranet may also be categorized as a MAN, WAN or other type of n/w. An extranet cannot consist of a single LAN, it must have at least one connection with an external n/w.

2) Intranet: An intranet is a set of interconnected nlw or internetworking, using the internet protocol and uses IP based tools such as web browsers and ftp tools, that is under the control of a single administrative entity. That administative entity closes the intranet to the rest of the world, and allows only specific users. An intranet is the internal nlw of a company or other enterprise. A large intranet will typically have its own web server to provide users with browseable info.

3) Internet: A specific internetworking consisting of a worldwide interconnection of governmental, academic, public and private nlw based upon the Advanced Research Projects Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defense also home to the World Wide Web (WWW) and referred to as the internet.

Challenges to Internetworking:

1) When we trying to connect numerous systems to support comm? b/w disparate technologies.

2) Another challenge is reliable service that should be maintained in an internetwork. Individual users and whole organizations depend upon consistent, reliable ~~ass~~ access to n/w resources.

3) N/w management should give centralized support associate degreed troubleshooting capabilities in an internetwork. Configuration, security, performance and diff. problems should be adequately addressed for the internetwork to perform easily.

4) Flexibility, the ultimate concern, is imp. for n/w enlargement and new applications and services, among diff. factors.