UNIT-5

NETWORK LAYER

5.1 Network Layer:

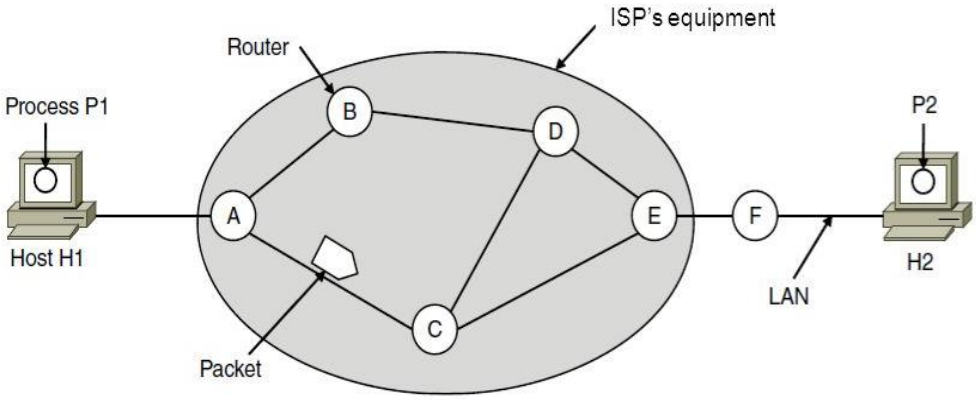
- Network layer is responsible for **host to host** delivery of data packets.
- **Routing** the data packets from source to destination is done by network layer itself.

5.1.1 Services provided to Transport Layer

- Network layer provides services to the Transport layer by **encapsulating TCP segment into packet**.
- Network layer protects TCP segment by hiding details about application, port number and other information at different routers and topology in network.
- The services should be independent of the router technology.
- The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.

5.1.2 Store and Forward Packet Switching:

- Network layer stores every packet in a routing table and checks the checksum field whether the packet is correct or not
- If it is correct, then the packet is **stored and forward** to the next router in network. That type of packet transfer is called store and Forward Packet switching.
- Here a packet is stored in routing table memory.

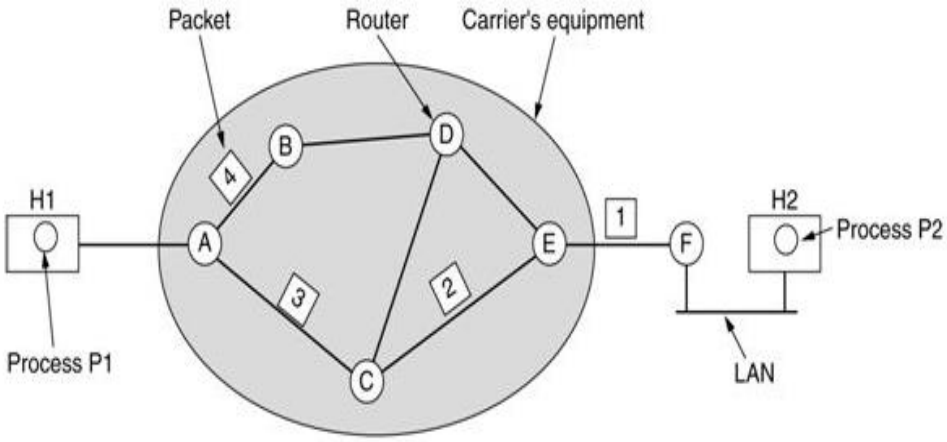


5.1.3 Network layer provide 2 types of services:

1. Connection-less Service
2. Connection-oriented Service

Connection-less Service: (Datagram Subnet)

- In connectionless service, packets are injected into a subnet called Datagram subnet.
- All the packets are treated individually and routed independently of each other. I.e. All packets must not follow the same path.
- Packets are called are Datagrams.
- No advance connection setup is needed.



In the above example, there are 6 routers (A,B,C,D,E,F) between Host H1 and H2

Packet1 → H1 → A → C → E → F → H2

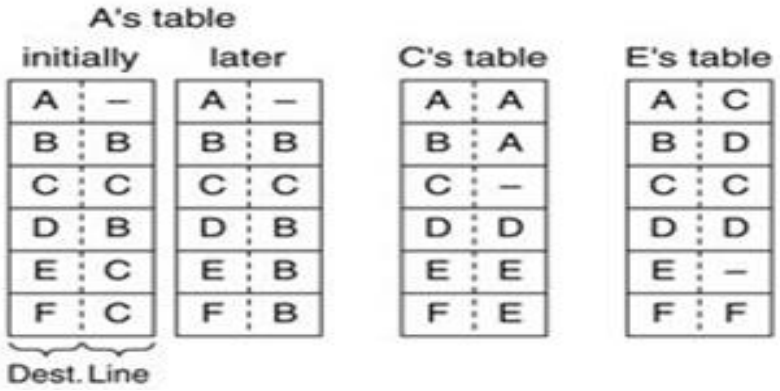
Packet2 → H1 → A → C → E → F → H2

Packet3 → H1 → A → C → E → F → H2

Here the packets **1, 2, 3** follows same path, but packet 4 follows path different path

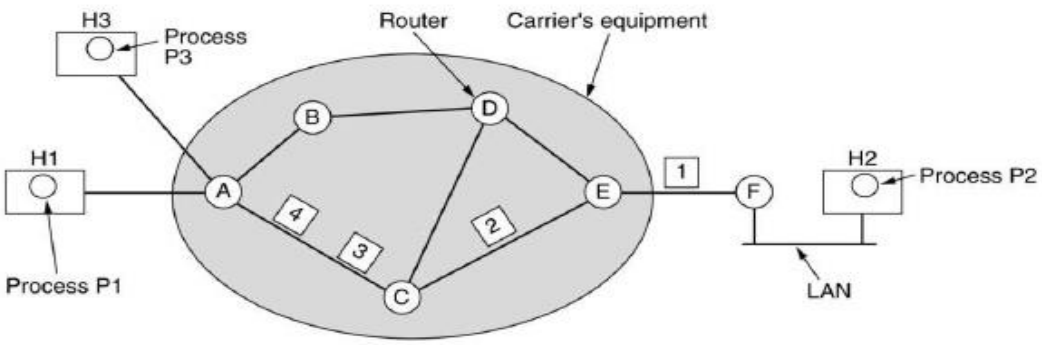
Packet4 → H1 → A → B → D → E → F → H2

Routing Tables in datagram subnet



Connection Oriented Service: (Virtual Circuit)

- A path should be set before data transmission that path is called Virtual circuit.
- All the packets must be transmitted through the same path.
- In Virtual circuit (VC) Switching, routing table contains connection information rather than router information and the network is called a virtual-circuit network.
- Used in Used in ATM, Frame- relay and X.25



Case 1: (H1 to H2)

H1 → A → C → E → F → F → H2

A's Table

H1	1
C	1

B's Table

A	1
E	1

C's Table

C	1
F	1

Case 2: (H3 to H4)

H3 → A → C → E → F → F → H2

A's Table

H3	1
C	1

B's Table

A	2
E	2

C's Table

C	2
F	2

Comparison of Datagram Network and Virtual-Circuit Network

Issue	Datagram network	Virtual-circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

5.1.4 Routing Algorithms

- The main function of the network layer is routing packets from the source machine to the destination machine.
- The algorithm that manages the tables and taking routing decisions is called Routing Algorithm.
- Routing algorithms are mainly used to find a shortest path between sender and receiver.

Optimality Principle

- Every Routing algorithm must follow an **optimality principle** for the data transmission.
- Routing algorithms find shortest path by removing cycles from a network graph, so that a **sink tree** is obtained from that graph with **no cycles and loops**.
- A **finite number of attempts** are used for data transmission within the shortest path otherwise the transmission between all routers may be infinite.

Properties of Routing Algorithms

- Correctness
- Simplicity
- Robustness
- Stability
- Fairness
- Optimality

Two types of Routing Algorithms

1. Non –Adaptive (Static Routing Algorithm)
2. Adaptive (Dynamic Routing Algorithm)

Non-Adaptive algorithms

- These algorithms do not base their routing decisions on any measurements or estimates of the current topology and traffic.
- Here the choice of route is computed in advance.
- This procedure is sometimes called **static routing.**
  Examples: Dijkstra's, Flooding Algorithm

Adaptive algorithms

- Adaptive algorithms change their routing decisions based on current traffic and topology, so that routing tables are updated dynamically.
- These algorithms are called **dynamic routing** algorithms.
  Examples: Distance Vector and Link state Routing Algorithm

Routing Algorithms:

a. Shortest Path Routing
b. Distance Vector Routing
c. Hierarchical Routing
d. Flooding
e. Broadcast Routing
f. Multi-Casting Routing

g. Link State Routing

a. Shortest Path Algorithm

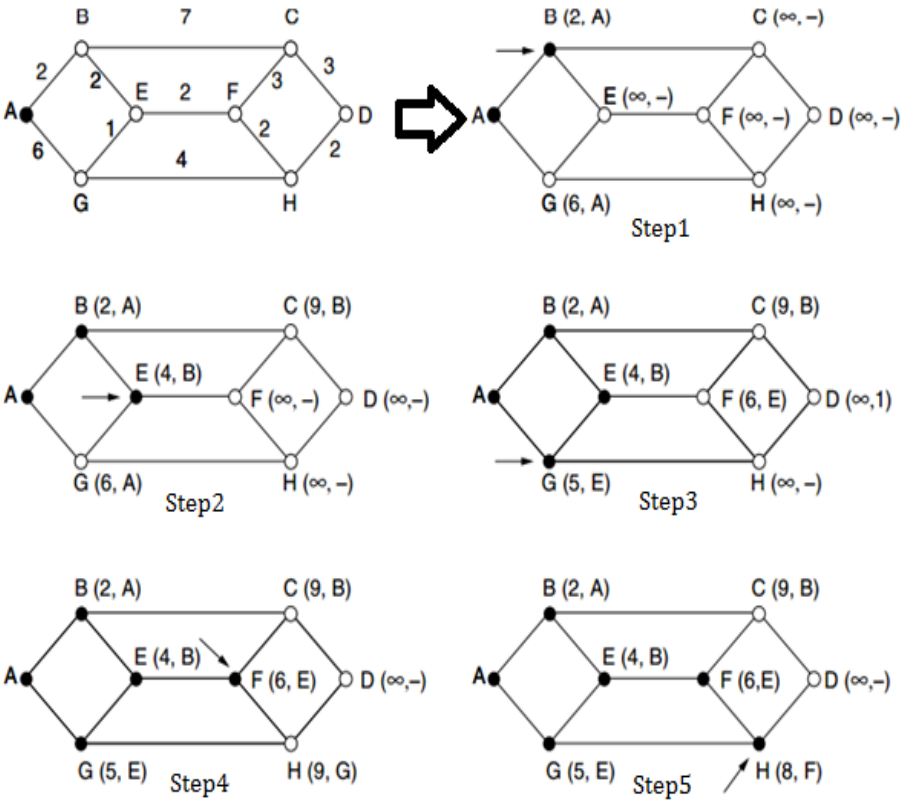
- There are several algorithms for computing the shortest path between two nodes of a graph.
- One of the algorithms is **Dijkstra's algorithm** is used to find the shortest paths between a source and all destinations in the network.
- Each node is labelled (in parentheses) with its distance from the source node along the best known path.

Algorithm:

- Given a network topology and a set of weights describing the cost to send data across each link in the network
- Find the shortest path from a specified source to all other destinations in the network.
- Initially, mark the source node as permanent.
- Designate the source node as the working node.
- Set the tentative distance to all other nodes to infinity. Identify Successors for each node to generate the shortest path.
- While some nodes are not marked permanent
- Compute the tentative distance from the source to all nodes adjacent to the working node. If this is shorter than the current tentative distance replaces the tentative distance of the destination and record the label of the working node there.
- Examine ALL tentatively labelled nodes in the graph. Select the node with the smallest value and make it the new working node. Designate the node permanent.

Example

Find shortest path from A to D for the graph shown below:



Case 1:

If u choose the path A → B → E → G → H → D

Tota1 distance = 2 + 2 + 1 + 4 + 2 = 11

- After finding shortest path now all the routers tables are updated with the shortest distance from neighbours except router ‘C’ and router ‘F’.
- After some other attempts of finding shortest paths, labels of routers ‘C’ and ‘D’ also updated.
- At that time every router has completed the construction of routing tables with the information (shortest distance information) about its neighbours.

Case 2:

- After constructing the routing tables for every router, check the distance (or) find out the shortest path to transfer data from one router to another (‘A’ to ‘D’).

If u choose the path A → B → E → F → H → D

Tota1 distance = 2 + 2 + 2 + 2 + 2 = 10 (shortest path)

Routing Table for 'A':

	Distance	Via
A	-	-
B	2	B
C	9	B
D	10	B
E	4	B
F	6	B
G	5	B
H	8	B

b. Distance Vector Routing:

- The distance vector routing algorithm is sometimes called **by Distributed Bellman-Ford algorithm (or) Fulkerson Algorithm.**
- It is one of the **dynamic routing algorithms**, which find shortest paths for the network based on current traffic and topology.
- In this algorithm, every router has a **routing table** that shows it the best route for any destination.
- These tables are updated by **exchanging information with the neighbors**. Eventually, every router knows the best link to reach each destination.
- This algorithm was **used in the original ARPANET**.

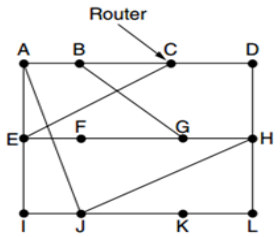
Algorithm

- It counts the weight of the links directly connected to it and saves the information to its table.

- In a specific period of time, it sends its table to its neighbour routers (not to all routers) and receives the routing table of each of its neighbors.
- Based on the information in its neighbors routing tables, it updates its own.

Example

A typical graph and routing table for J's Neighbors (A, I, H, K) is shown below:



(a) A network

To	A	I	H	K
A	0	24	20	21
B	12	36	31	28
C	25	18	19	36
D	40	27	8	24
E	14	7	30	22
F	23	20	19	40
G	18	31	6	31
H	17	20	0	19
I	21	0	14	22
J	9	11	7	10
K	24	22	22	0
L	29	33	9	9
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6

Vectors received from J's four neighbors

(b) Input from *A*, *I*, *H*, *K*

New estimated delay from J

Line	
8	A
20	A
28	I
20	H
17	I
30	I
18	H
12	H
10	I
0	–
6	K
15	K

New routing table for J

(c) the new routing table for *J*.

- In distance Vector routing, suppose if router 'J' wants to send the data packets to router 'c',
- Firstly, it identifies its neighbors (A, I, H, K).
- Calculate the distance or find the shortest path from its neighbor's router to router 'c'.
- Every time at each router the routing table is updated dynamically.
- Based on the information from its neighbor routers it selects the shortest path and forward the data packet to router 'c' by constructing new routing table for 'j'.

Protocols used in Distance Vector Algorithm

Protocols used in Distance vector routing algorithm is **RIP** (Routing Information Protocol), **IGRP** (Interior Gateway Routing protocol).

Drawback in Distance Vector Algorithm

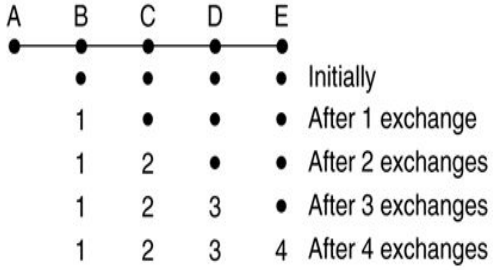
1. Convergence is slow

2. Count-to-infinity problem: The distance from sender to receive is infinity.

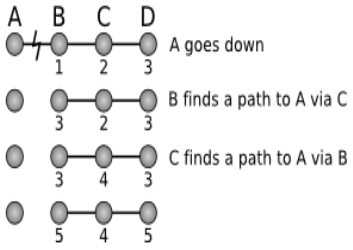
- This problem occurs due to updating of routing tables for every transaction based on neighbours (or) it occurs when an interface goes down.
- Good News travels quickly, bad new travels slowly (Count-to infinity problem).

a) Propagation of Good News:

- Initially A is down and all the routers know this.
- When A comes up (active), the other routers learn about it via the vector exchanges.



a) Routing table Entires for 'A' when 'A' is active



b) shows what happens when 'A' fails, each node is very slow to realize the cost to 'A' is INFINITY

b) Propagation of Bad News:

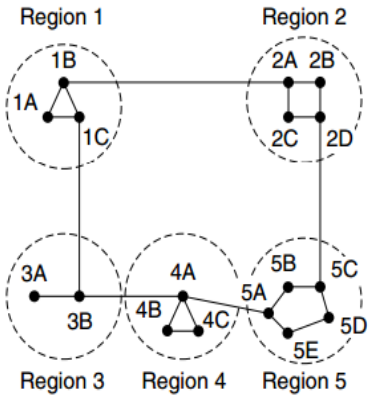
When ‘A’ goes down, the information, B thinks that there is path to A though ‘c’ but it doesn’t think that ‘C’ itself goes to ‘A’ via ‘B’. Every time the distance is increases between the routers and this problem is treated as “Count-to-infinity” problem.

3. Serious drawback in distance vector routing is sometimes router doesn’t know about complete information of network.

c. Hierarchical routing

- It is used to reduce the number of routing tables with in a subnet.
- If subnet has 720 routers then 720 routing tables with 720 entries are required at each router.
- This process consumes large memory space, more CPU time and high bandwidth. So that routers can’t handle network traffic efficiently.
- To overcome this problem subnet is organized as hierarchical levels.

- In **hierarchical routing**, routers are classified in groups known as **regions**. Each router has only the information about the routers in its own region and has no information about routers in other regions. So routers just save one record in their table for every other region.
- In this example, we have classified our network into five regions (see below).



Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

- If A wants to send packets to any router in region 2 (2A, 2B, 2C, 2D), it sends them to B, and so on.
- The above example shows two-level hierarchical routing. We can also use three- or four-level hierarchical routing.
- In three-level hierarchical routing, the network is classified into a number of **clusters**. Each cluster is made up of a number of regions, and each region contains a number or routers.
- Hierarchical routing is **widely used in Internet** routing and makes use of several routing protocols.

Advantages

- In this type of routing, the tables can be summarized i.e. Hierarchical routing **reduces the table from 17 to 7 entries**. So network efficiency improves.

Disadvantage

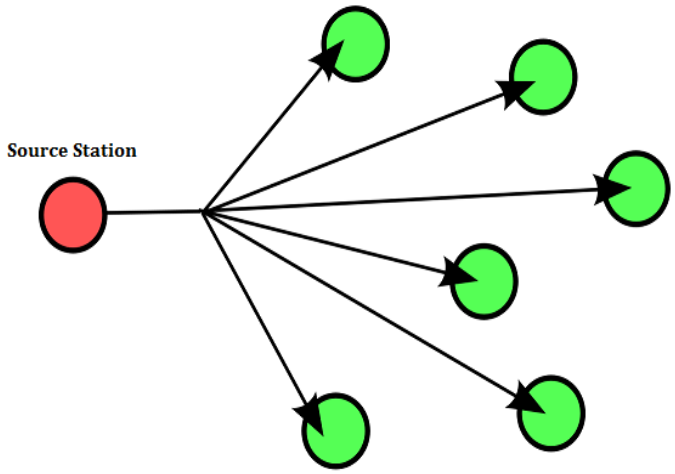
- Maintaining sub optimal routes where the average path length increases.

d. Broadcast Routing

- Sending a data packet to all destinations simultaneously is called Broadcasting.

(or)

- Sending message to all the routers within the subnet is called Broadcasting.



Applications:

- **Television** – To broadcast television to all the stations connected to a network. (For Entertainment)
- **Radio** – For Broadcasting radio
- **Military** – To send an important message to all the soldiers (for communication).
- **Database Updation** – In Distributed Systems, all the databases are updated immediately (**Stock Markets**).
- **Weather Reporting** – To generate weather report dynamically for period of time.

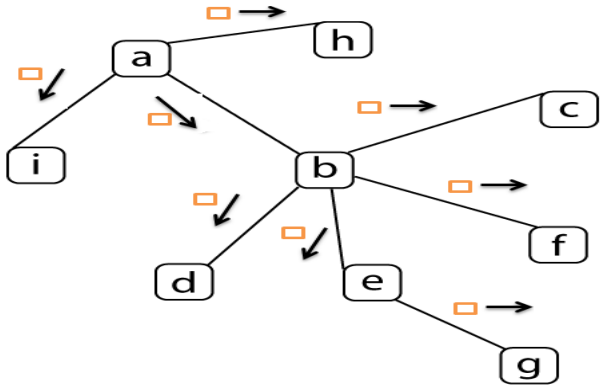
Methods involved in Broadcasting are:

1. Ordinary Method (nothing but Broadcast)
2. Flooding
3. Multi-Destination
4. Spanning tree (or) Sink tree

5. Reverse Path Forwarding

e. Flooding:

- When a routing algorithm is implemented, each router must make decisions based on local knowledge, not the complete picture of the network.
- Flooding is a Static routing algorithm in which every incoming packet is sent through every outgoing link except the one it arrived on.
- In Flooding every incoming packet is copied to all other nodes except the node that arrive on it.
- In Flooding, Every node is responsible for sending data to neighbours.



Here' a' sends packet to 'i' and 'h', then packet reach to 'B' then 'B' sends the packet to 'C' and 'd'. Likewise the packets are sent to all the nodes in a network.

Drawback:

One major problem of this algorithm is that it generates a **large number of duplicate packets** on the network.

Solution:

- One solution is to include a **hop counter** in the header of each packet. Hop Count is number of nodes that a packet may have to pass through on the way to its destination. This counter is decremented at each hop along the path. When this counter reaches zero the packet is discarded. Ideally, the hop counter should become zero at the destination hop, indicating that there are no more intermediate hops and destination is reached.

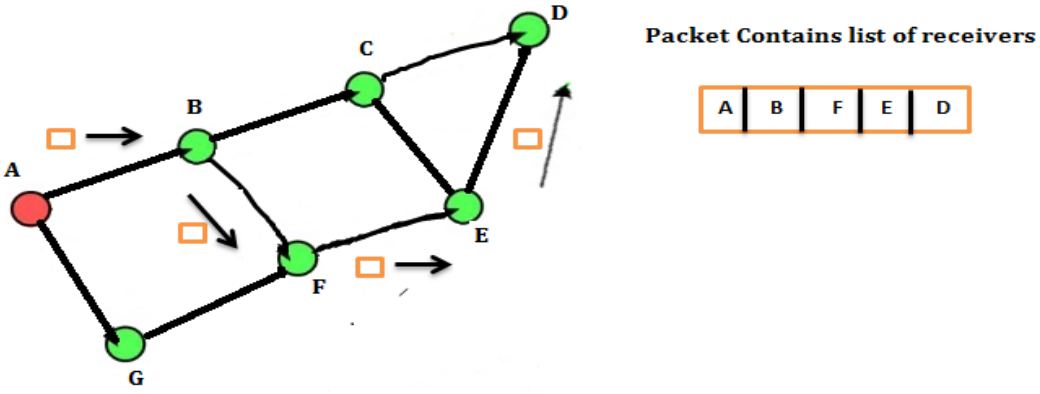
- Generating a **sequence number** to each packet at source router, so that the duplicate packets will be avoided.
- Another solution is to use **selective flooding.** In selective flooding the routers do not send every incoming packet out on every output line. Instead packet is sent only on those lines which are approximately going in the right direction.

Uses of Flooding:

- In Military Applications, the network must remain robust in the face of hostility.
- Sending Routing Updates periodically to all the routers in the network.

f. Multi-Destination:

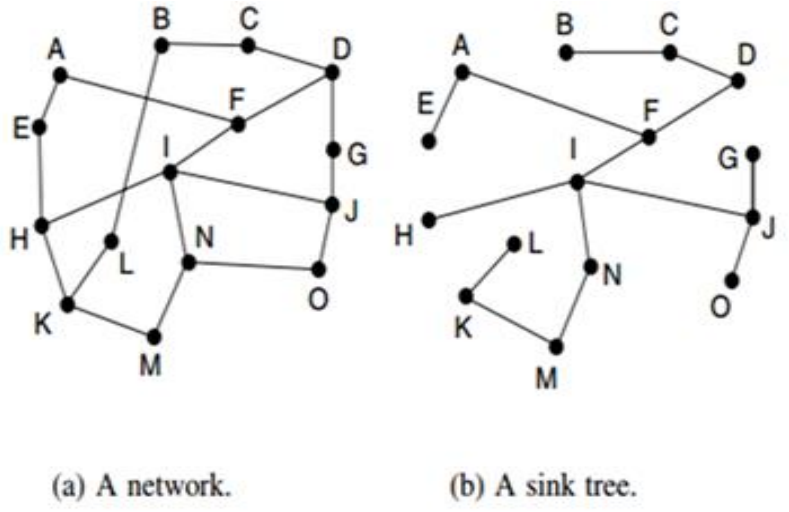
- In multi-destination routing, each packet contains either a **list of destinations** or a bit map indicating the desired destinations.
- In this method every packet has a **list of receivers in Header** so that it controls duplicate packets.
- When a packet arrives at a router, the router checks all the destinations to determine the set of output lines that will be needed.



- Here initially packet is send to ‘A’, then ‘A’ checks the header next connection is ‘B’. So ‘A’ simply forwards the packet to ‘B’.
- So B received the received packet and then forward to F.
- ‘F’ sends data to next destination (i.e. E), after receiving the data packet ‘E’ sends data to ‘D’.

g. Sink Tree (or) Spanning tree

- In sink tree **every node has complete information about all the routers** in that tree so that every node simply forwards a packet to its neighbour.
- In sink tree, packets are broadcast **without creating a duplicate**.
- All sink trees are Spanning tress.
- **A sink tree (or) spanning tree** is a subset of the network that includes all the routers but contains no loops. Sink trees are spanning trees.



(a) A network. (b) A sink tree.

Advantages:

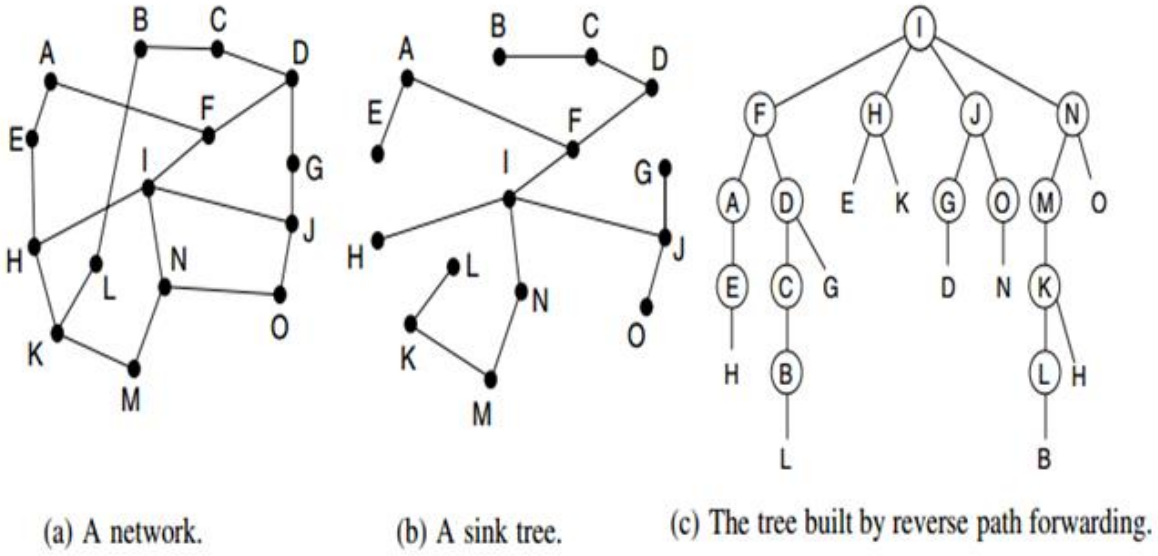
- This method makes excellent use of bandwidth.
- It generates only minimum number of packets necessary to do the job. So that we can duplicate packets.

Disadvantage:

- Sometimes the router doesn't have complete knowledge of entire network.

Reverse Path Forwarding:

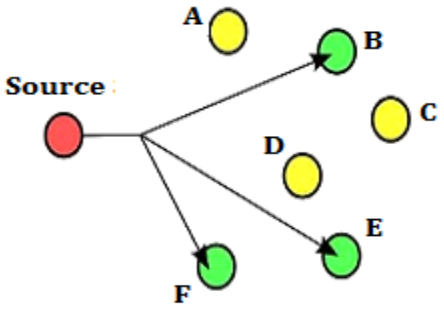
- When the router does not have complete information about sink tree then subnet selects reverse path forwarding method (without knowing any spanning tree).
- In this method, if a packet arrives on the line used for traffic to source of broadcast then forward packet on all lines, except the one it arrived on otherwise discard the packets.



(a) A network. (b) A sink tree. (c) The tree built by reverse path forwarding.

h. Multicasting

- Multicast IP Routing protocols are used to distribute data (for example, audio/video streaming broadcasts) to multiple recipients.
- Using multicast, a source can send a single copy of data to a single multicast address, which is then distributed to an entire group of recipients.
- Sending data to a **group of nodes** at a time is treated as Multicasting and its routing algorithm is multicast routing.
- Multicasting requires **group management** to create and destroy the groups and to allow processes to join and leave groups.
- The goal of Multicasting is **efficient data distribution**.



Applications:

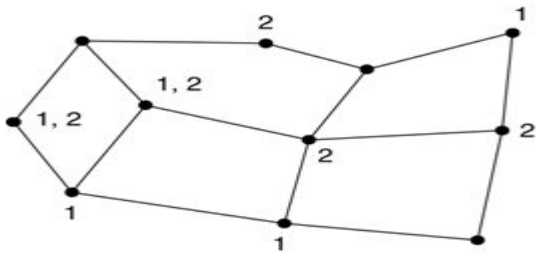
- Broadcasts of Radio or Video
- Videoconferencing
- Shared Applications
- Distributed Computing

Disadvantage:

- One potential disadvantage of this algorithm is that it scales poorly to large networks.

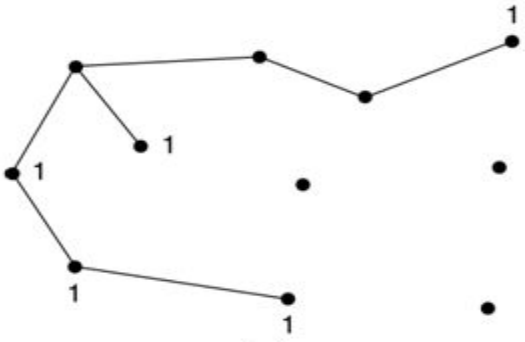
Example:

Consider a network with two groups 1 and 2. Some routers are attached to hosts that belong to one or both of these groups as shown in below.

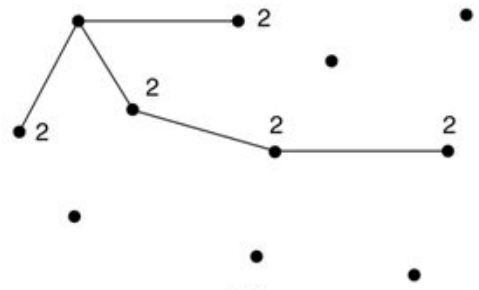


Subnet

- When a process sends a multicast packet to a group, the first router examines its spanning tree and prunes it by removing all the lines that do not lead to hosts that are members of the group.
- Multicast packets are forwarded only along the approximate spanning tree.



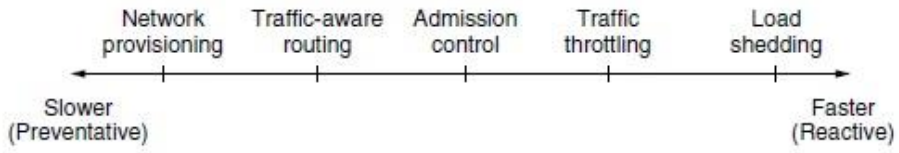
A multicast tree for group 1



A multicast tree for group 2

5.1.5 Congestion Control

Congestion is a network problem, occurs when multiple sources transmit their data through a common channel and makes the channel filled with large amounts of packets greater than the bandwidth of the channel. The presence of congestion means that the load is temporarily greater than the resources can handle. Two solutions come in mind are to increase the resources or decrease the load. Network layer uses 5 different techniques to overcome congestion problem. These techniques vary from slower preventative methods to faster reactive methods.



a. Network Provisioning

Network resources can be added dynamically when there is serious congestion, for example, turning on spare routers or enabling lines that are normally used only as backups or purchasing bandwidth on the open market. More often, links and routers that are regularly heavily utilized are upgraded at the earliest opportunity. This is called Network Provisioning and happens on a time scale of months, driven by long term traffic trends.

b. Traffic-aware routing

Splitting traffic across multiple paths is also helpful. To make the most of the existing network capacity, routes can be personalized depending on the traffic patterns. For example, routes may be changed to shift traffic away from heavily used paths by changing the shortest path weights. This is called traffic-aware routing.

c. Admission control

Sometimes it is not possible to increase capacity of the network. The only way to avoid the congestion is to decrease the load. In a virtual-circuit network, new connections can be refused if they would cause the network to become congested. This is called Admission Control.

d. Traffic Throttling

When the congestion is about to happen the network can deliver feedback to the sources whose traffic flows are responsible for the problem. The networks can request the sources to throttle their traffic, or it can slow down the traffic itself. Two difficulties with this approach are how to identify the beginning of congestion, and how to inform the source that needs to slow down. To tackle the first issue, routers can monitor the average load, queueing delay, or packet loss. In all cases, raising numbers indicate growing congestion. To tackle the second issue, routers must participate in a feedback process with the sources.

e. Load Shedding

Finally, when all techniques of congestion control fails, the network is forced to discard packets that it cannot deliver. The general name for this is Load Shedding. A good policy for choosing which packets to discard can help to prevent congestion collapse.