BACHELOR OF COMPUTER APPLICATIONS

SEMESTER 4

DCA2201

COMPUTER NETWORKING

Unit 7

Network Layer – Advanced Internetworking

Table of Contents

1. INTRODUCTION

In the previous unit, we discussed different networks and network layer addressing. The main function of network layer is to transfer packets from source to destination. It should also take care while choosing routes. So, another major functionality of network layer is routing. In this unit, we will discuss the network layer routing and different routing algorithms. One of the main functions of the network layer is routing packets from source to destination. Routing algorithms is a part of network layer software which is responsible for deciding the output line for an incoming packet to reach a particular destination.

We will start this unit with different routing algorithms. In the next section, we will discuss multicast and broadcast routing. In the last section, we will discuss routing on the Internet.

1.1 Objectives:

After studying this unit, you should be able to:

- *Describe routing algorithms*
- *Explain multicast and broadcast routing*
- *Describe routing on the Internet*

2. ROUTING ALGORITHMS

As discussed above, routing algorithms help a network device to determine which output line or link to use to reach a specific destination. Forwarding is the process which handles each packet as it arrives and selecting the best outgoing line to use for it from the routing tables. Another router process is responsible for filling in and updating the routing tables.

Routing algorithms can be grouped into two major classes. They are ***nonadaptive*** and ***adaptive routing algorithms.*** As the name specifies, nonadaptive do not establish its routing decisions on measurements or estimates of the current topology and traffic. The routing decision (choice of the route) is computed in advance and this information is downloaded to each router. This procedure is also called ***static routing***. This is useful in situations in which the route choice is clear.

Adaptive algorithms change their routing decisions to reflect changes in the topology and changes in the traffic as well. This algorithm is also known as ***dynamic routing*** algorithm.

The optimality principle

Optimality principle is a statement about optimal routes without considering network topology or traffic. It states that if router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route. The set of routes from all sources to a given destination form a tree rooted at the destination. Such a tree is called a sink tree. A sink tree is shown in below figure 7.1

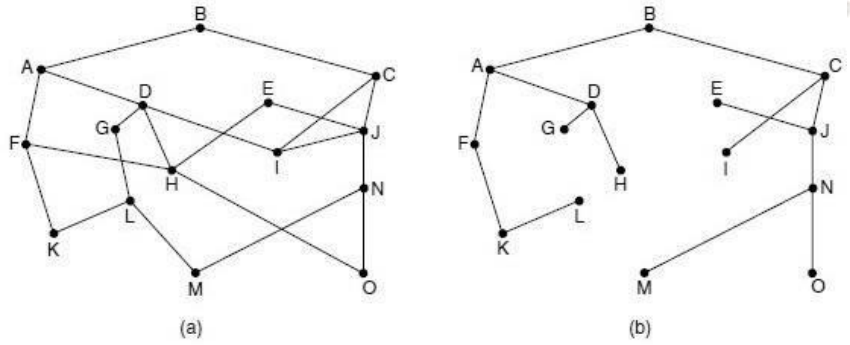


Fig 7.1: (a) A network (b) A Sink tree for router B

The goal of all routing algorithms is to discover and use the sink trees for all routers. We will discuss different routing algorithms in the following sections.

2.1 Shortest Path Algorithm

The concept behind the shortest path algorithm is to build a graph of network in which each node represents a router and each edge of the graph represents a communication line or link. To find a route between a pair of nodes, algorithm finds the shortest path between them on the graph. The shortest path can be found by measuring the number of hops. Another metric is the geographic distance between the nodes. Other metrics are also possible. Following figure 7.2 illustrates the procedure of shortest path algorithm.

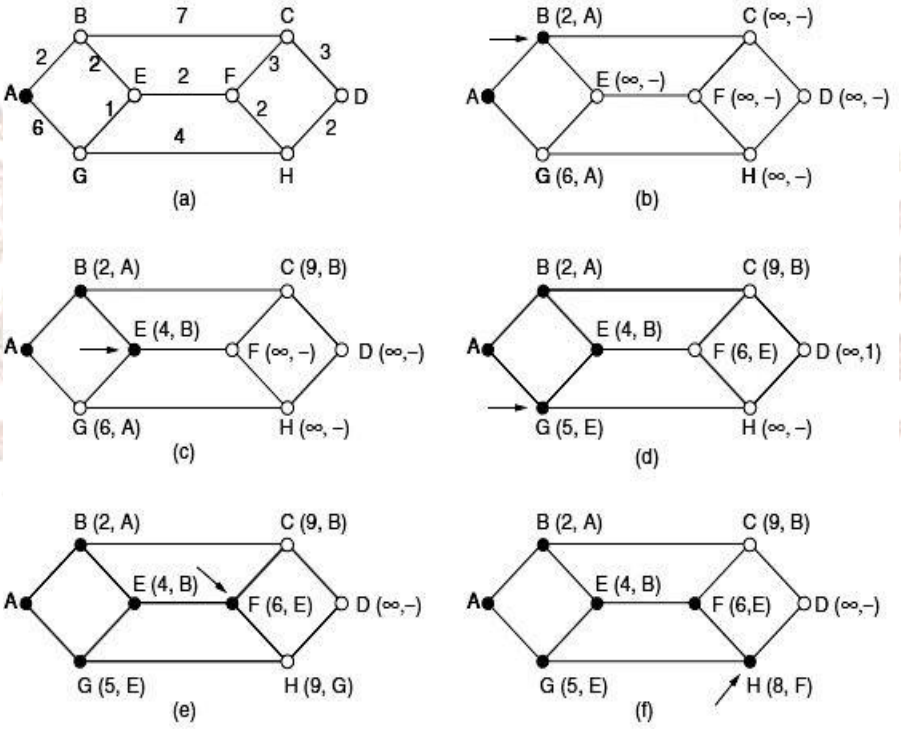


Fig 7.2: The first six steps used in computing the shortest path from A to D (the arrows indicate the working node)

Consider figure 7.2 (a), where the weight represents the distance. Here, we want to find the shortest path from A to D. We start from A, then check the adjacent nodes of A. In the figure, when counting the distance from A to B and A to G, the distance to B is shorter. So will choose B as the new working node as shown in figure 7.2 (b). Then we have to find out the adjacent nodes of B. at this point, we have chosen E as the next node as shown in figure 7.2 (c). Likewise, all nodes adjacent to the working node have been inspected and the tentative labels changed, entire graph is searched for the shortest values. Once the shortest node is found, it is made permanent and becomes the working node for the next round. Figure 7.2 shows the first six steps of the algorithm. In figure 7.2 (d) the adjacent nodes of E with

shortest distance are found out. So, the shortest in this route is F. in 7.2 (e) the shortest route from F to D is calculated, and it is through node H. So based on this algorithm shortest path from A to D is ABEFHD. In shortest path routing, whenever a new node is added or deleted, it should be updated periodically. And if any node in the shortest path fails, then the data will be lost.

2.2 Flooding

In case of flooding, every incoming packet is sent out on every outgoing line except the one it arrived on. Flooding generates a vast number of duplicate packets. Some measures are required to limit the number of duplicate packets. One technique is to use a hop counter contained in the header of each packet that is decremented at each hop and the packet being discarded when the counter reaches zero. This hop counter should be initialized to the length of the path from source to destination.

Another method to block the flood is that each router keeps track of which packets have been flooded, to avoid sending them out a second time. One way to achieve this goal is to have the source router put a sequence number in each packet it receives from its hosts. In this case, each router needs a list per source router telling which sequence numbers originating at that source have already been received. If the arriving packet is on the list, it will be discarded.

Flooding is very effective for broadcasting information because it ensures that a packet is delivered to every node in the network. But if only a single destination needs the packet, then it may be wasteful. Another benefit of flooding is that it is very robust. Even if large numbers of routers are broken down, flooding will find a path if one exists, to get a packet to its destination.

Flooding always chooses the shortest path because it chooses every possible path in parallel. Consequently, no other algorithm can produce a shorter delay. In flooding, routers only need to know their neighbours so flooding can be used as a building block for other routing algorithms. The drawback of this algorithm is that flooding can be costly in terms of wasted bandwidth. Also, messages can become duplicated in the network, further increasing the load on the networks bandwidth as well as requiring an increase in processing complexity to disregard duplicate packets.

2.3 Distance Vector Routing

In distance vector routing, each router maintains a table giving the best known distance to each destination and which link to use to reach there. These tables are updated by exchanging information with the neighbors. Distance vector routing is also known as distributed **Bellman-Ford** routing algorithm, after the researchers who developed it (Bellman, 1957; and Ford and Fulkerson, 1962). In this algorithm, each router maintains a routing table containing one entry for each router in the network. This entry has two parts: the preferred outgoing line to use for that destination and an estimate of the distance to that destination. The distance might be measured as the number of hops or using any other measurement. Each router is assumed to know the distance to its neighbors. The following figure 7.3 illustrates the working of distance vector routing algorithm.

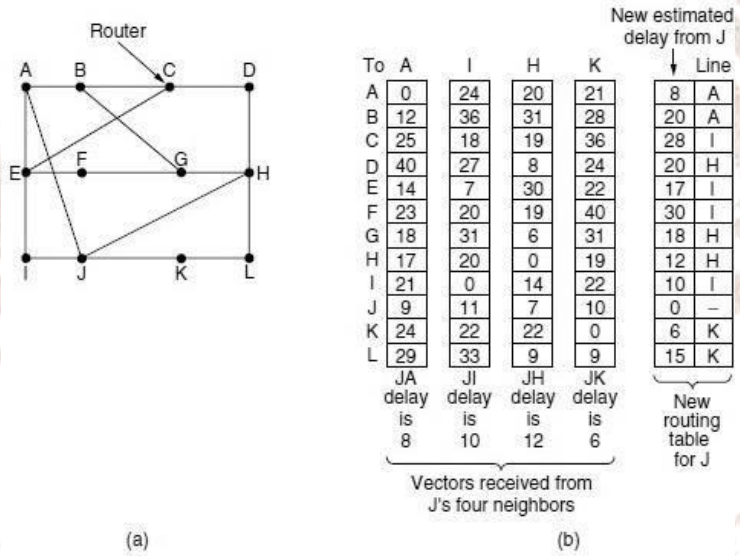


Fig 7.3: (a) A Network. (b) Inputs from A, I, H, K and the new routing table for J.

In figure, 7.3 (a) shows a network and the first four columns of 7.3 (b) shows the delay vectors received from the neighbors of router J. A claim to have a 12-msec delay to B, a 25-msec delay to C, a 40- msec delay to D, etc. Suppose that *J* has measured or estimated its delay to its neighbors, *A, I, H*, and *K*, as 8, 10, 12, and 6 msec, respectively.

Now, consider how *J* computes its new route to router *G.* It knows that it can get to A in 8 msec, and furthermore *A* claims to be able to get to *G* in 18 msec, so *J* knows it can count on a delay of 26 msec to *G* if it forwards packets bound for *G* to *A*. Similarly, it computes the delay to G via I, H, and K as 41 (31 + 10), 18 (6 + 12), and 37 (31 + 6) msec, respectively. The

best of these values is 18, so it makes an entry in its routing table that the delay to G is 18 msec and that the route to use is via H. The same calculation is performed for all the other destinations, with the new routing table shown in the last column of the figure 7.3(b).

The Count-to-Infinity Problem

Distance vector routing is useful as a simple technique by which routers can collectively compute shortest paths, but it has a serious drawback that it reacts rapidly to good news, but slowly to bad news. To see how fast good news propagates, consider the five-node (linear) network shown in figure 7.4, where the delay metric is the number of hops.

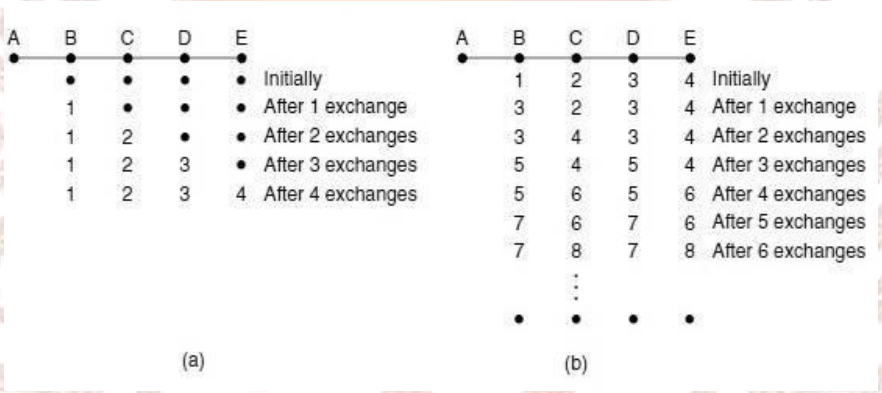


Fig 7.4: The Count-to-Infinity Problem

Suppose *A* is down initially and all the other routers know this. In other words, they have all recorded the delay to *A* as infinity. When A comes up, by vector change other routers know about this. When A is up, its neighbor B learns that its left-hand neighbor has zero delay to A. So, B makes an entry in its routing table showing that A is one hop away to the left. At this point, all other routers still think that A is down. Routing table entries for A is shown in the second row of figure 7.4. During the next exchange, Router C identified that B has a path of length 1 to A, so it updates its routing table with a length 2, as shown in third row of figure 7.4. Similarly, D will update the length as 3 during the next exchange and then E will update the length as 4. So, we can say that the good news is spreading at the rate of one hop per exchange. For a network with longest path of N hops, within N exchanges every router will get the news about newly alive links and routers.

Now let's see another case, Consider the situation of figure 7.4 (b), where all the links and routers are initially up. We can see that routers B, C, D and E have distance to A of 1, 2, 3 and 4 hops respectively.

Suppose, suddenly either A goes down or the link between A and B is cut, then during the next packet exchange, B does not hear anything from A. But while checking the other neighbor C which says it has a path to A of length 2. Even if the path is through B only, B will not Suspect that the path runs through B itself and thinks that C might have ten other separate paths to A of length 2. As a result, B thinks it can reach A via C, with a path length of 3. D and E do not update their entries for A on this exchange. As shown in third row of figure 7.4 (b), during the next exchange, C notices that each of its neighbors claims to have a path to A of length 3. So, it updates its new distance to A as 4. Similarly, the update progresses as shown in figure 7.4 (b) and gradually, all routers work their way up to infinity. This problem is known as the ***count-to-infinity*** problem. Here, the number of exchanges required depends on the numerical value used for infinity. For this reason, it is best to set infinity to the longest path plus 1.

2.4 Link State Routing

As we discussed in the previous section, distance vector routing took too long to converge after the network topology changed, due to count to infinity problem. As a result, it is replaced by an entirely new algorithm, called **link state routing.** The idea behind link state routing can be stated in five steps as discussed below. Each router must do the following five steps:

- Discover its neighbors and learn their network addresses.
- Set the distance or cost metric to each of its neighbors.
- Construct a packet telling all it has just learned.
- Send this packet to and receive packets from all other routers.
- Compute the shortest path to every other router.

Learning about the neighbors

When the router is booted, its first task is to find the neighbors. It achieves this goal by sending a special HELLO packet on each point-to-point line. The router on the other end is expected to send back a reply giving its name. These names must be globally unique.

Measuring link costs

Each link should have a distance or cost metric for finding the shortest paths. The cost to reach neighbors can be set automatically, or configured by the network operator. Cost can

be calculated as a factor of bandwidth or delay of the links. A direct way to calculate delay is to send over the line a special ECHO packet that the other side is required to send back immediately. By measuring the round-trip time and dividing it by two, the sending router can estimate the delay.

Construct link state packets

Once the information such as neighboring node and cost to reach each node is collected, the next step is for each router to build a packet containing all the data. The packet starts with the identity of the sender, followed by a sequence number and age and a list of neighbors. The cost to each neighbor is also given. An example network is shown in figure 7.5.

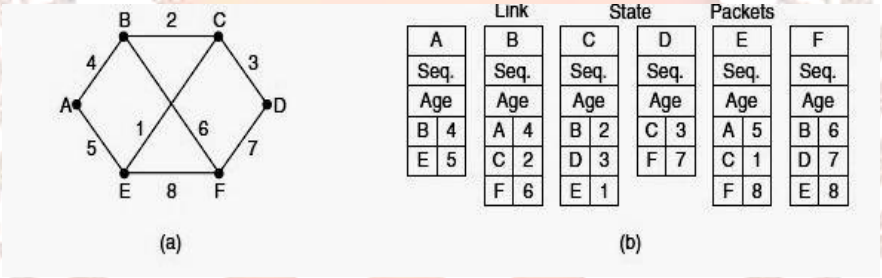


Fig 7.5: (a) A Network. (b) The link state packets for this network

Figure 7.5 (b) shows the link state packets for all six routers. Link state packets can be built periodically or when some significant event occurs, such as a line or neighbor going down or alive again.

Distributing the link state packets

The hardest part of the algorithm is distributing link state packets. All of the routers must get all of the link state packets quickly and reliably. If different routers use different topology, the routes they compute can have inconsistencies such as loops, unreachable machines etc.

The fundamental idea is to use flooding to distribute the link state packets to all routers. To keep the flood in check, each packet contains a sequence number that is incremented for each new packet sent. This algorithm has a few problems. First is, if the sequence numbers wrap around, it will create confusion. The solution here is to use a 32-bit sequence number. Second, if a router ever crashes, it will lose track of its sequence number. If it starts again at 0, the next packet it sends will be rejected as a duplicate. Another problem is, if the sequence number is corrupted, and 35,570 is received instead of 5, packets 6 through 35,570 will be rejected considering the current sequence number as 35,570.

The solution to all these problems is to include the age of each packet after the sequence number and decrease it once per second. When the age hits zero, the information from that router is discarded. The Age field is also decremented by each router during the initial flooding process, to make sure no packet can get lost and live for an indefinite period of time.

Computing the new routes

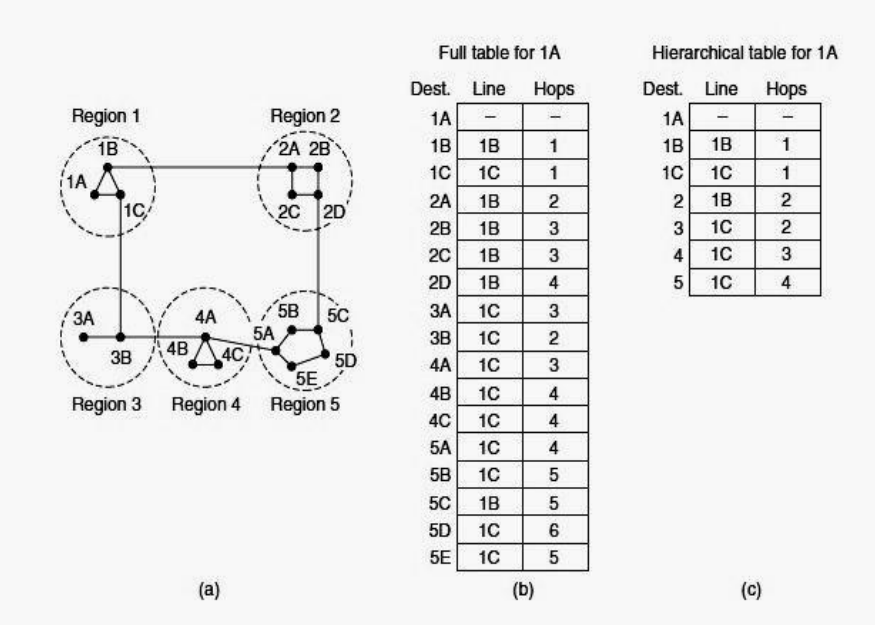
Once a router has accumulated a full set of link state packets, it can construct the entire network graph because every link is represented. Every link is, in fact, represented twice, once for each direction. The different directions may even have different costs. By using certain algorithms like Dijkstra's algorithm, we can calculate the shortest path to each destination.

Compared to distance vector routing, link state routing requires more memory and computation. For a network with n routers, each of which has k neighbors, the memory required to store the input data is proportional to kn, which is at least as large as a routing table listing all the destinations. Also, the computation time grows faster than kn.

Variants of link state routing called IS-IS (Intermediate System to Intermediate System) and OSPF (Open Shortest Path First) are the routing algorithms that are most widely used inside large networks and the Internet today.

2.5 Hierarchical Routing

As networks grow in size, the router routing tables grow proportionally. Not only is router memory consumed by ever-increasing tables, but more CPU time is needed to scan them and more bandwidth is needed to send status reports about them. At a certain point, the network may grow to the point where it is no longer feasible for every router to have an entry for every other router, so the routing will have to be done hierarchically, as it is in the telephone network. When hierarchical routing is used, the routers are divided into **regions**. Each router knows all the details about how to route packets to destinations within its own region but knows nothing about the internal structure of other regions. When different networks are interconnected, it is natural to regard each one as a separate region to free the routers in one network from having to know the topological structure of the other ones.



Full table for 1A

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

Hierarchical table for 1A

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

Fig 7.6: Hierarchical routing

Figure 7.6 shows an example of hierarchical routing in a two-level hierarchy with five regions. The full routing table for router *1A* has 17 entries, as shown in figure 7.6 (b). When routing is done hierarchically, as shown in figure 7.6 (c), there are entries for all the local routers, as before, but all other regions are condensed into a single router, so all traffic for region 2 goes via the *1B-2A* line, but the rest of the remote traffic goes via the *1C-3B* line. Hierarchical routing has reduced the table from 17 to 7 entries. As the ratio of the number of regions to the number of routers per region grows, the savings in table space also increases.

SELF-ASSESSMENT QUESTIONS – 1

1. _____is responsible for deciding the output line for an incoming packet to reach a particular destination.
2. Routing algorithm which does not establish its routing decisions on measurements or estimates of the current topology and traffic is known as _____.
3. Non adaptive routing algorithm is also called _____.
4. Adaptive routing algorithm is also called _____.
5. Optimality principle is a statement about optimal routes without considering network topology or traffic. (True/False)
6. The set of routes from all sources to a given destination form a tree rooted at the destination. Such a tree is called _____
7. The routing in which every incoming packet is sent out on every outgoing line except the one it arrived on, is known as _____.
8. Distance vector routing is also known as _____.
9. Distance vector routing took too long to converge after the network topology changed, so it is replaced by an entirely new algorithm, called
10. When hierarchical routing is used, the routers are divided into

3. MULTICAST AND BROADCAST ROUTING

Sending a packet to all destinations simultaneously is called *broadcasting*. Sending a packet to a subset of destinations or a group of destinations is known as *Multicasting.*

Broadcast Routing

Some applications such as a service distributing weather report, or a live radio program will work best by sending to all machines and anyone interested can read the data. Sending packets to all destinations simultaneously is called broadcasting. Flooding is a better method for broadcasting.

Another broadcast routing algorithm is reverse path forwarding. The idea behind this algorithm is shown in figure 7.7. The idea is that, when a broadcast packet arrives at a router, the router checks to see if the packet arrived on the link that is normally used for sending packets toward the source of the broadcast. If so, there is a better chance that the broadcast packet itself followed the best route from the router and is therefore the first copy to arrive at the router. In this case, the router forwards copies of it onto all links except the one it arrived on. However, the broadcast packet arrived on a link other than the preferred one for reaching the source, then the packet is considered as duplicate and is discarded.

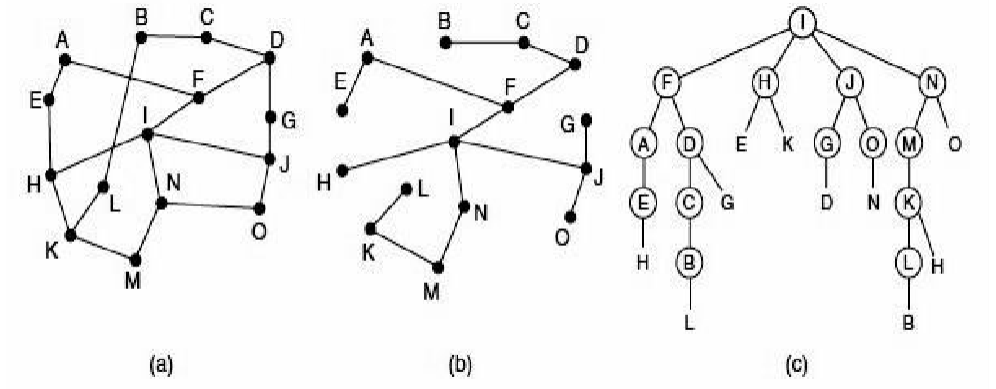


Fig 7.7: Reverse path forwarding. (a) A network. (b) A Sink tree. (c) The tree built by reverse path forwarding

Above figure 7.7 shows an example of reverse path forwarding. Figure 7. (a) shows a network. Figure 7.7 (b) shows a sink tree for router *I* of that network, and figure 7.7(c) shows how the reverse path algorithm works. On the first hop, *I* send packets to *F, H, J,* and *N*, as

indicated by the second row of the tree. Each of these packets arrives on the preferred path to I and is so indicated by a circle around the letter. On the second hop, eight packets are generated, two by each of the routers that received a packet on the first hop. As it turns out, all eight of these arrive at previously unvisited routers, and five of these arrive along the preferred line. Of the six packets generated on the third hop, only three arrive on the preferred path (at C, E, and K); the others are duplicates. After five hops and 24 packets, the broadcasting terminates, compared with four hops and 14 packets had the sink tree been followed exactly. The main benefit of reverse path forwarding is that it is efficient and easy to implement.

Another broadcasting algorithm which improves the behavior of reverse path forwarding is the one which makes explicit use of the sink tree or any other convenient spanning tree for the router initiating the broadcast. A spanning tree is a subset of the network that includes all the routers but contains no loops. Sink trees are spanning trees. If each router knows which of its lines belong to the spanning tree, it can copy an incoming broadcast packet onto all the spanning tree lines except the one it arrived on. This method makes excellent use of bandwidth, generating the absolute minimum number of packets necessary to do the job.

Multicast routing

Broadcasting packets are wasteful if the group consists of 1000 machines on a million-node network. So, we need a way to send messages to well-defined groups that are numerically large in size but small compared to the network as a whole. Sending a message to such a group is called *multicasting,* and the routing algorithm used is called *multicast routing.* All *multicasting* schemes require some way to create and destroy groups and to identify which routers are members of a group.

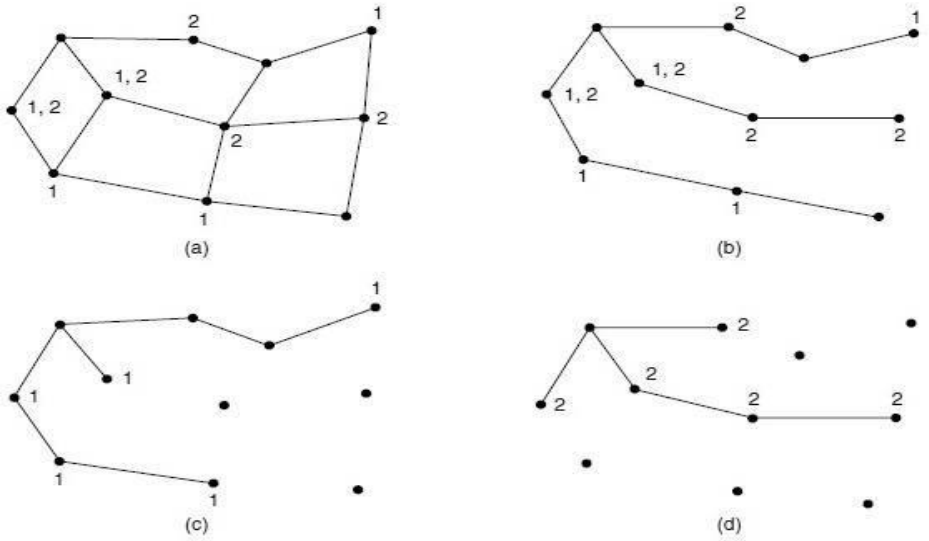


Fig 7.8: (a) A Network. (b) A Spanning tree for the leftmost router. (c) A multicast tree for group 1. (d) A multicast tree for group 2.

As an example, consider the two groups, 1 and 2, in the network shown in Figure 7.8 (a). Some routers are attached to hosts that belong to one or both of these groups, as indicated in the figure. A spanning tree for the leftmost router is shown in figure 7.8(b). This tree can be used for broadcast but is exertion for multicast, as can be seen from the two pruned versions that are shown next. In figure 7.8 (c), all the links that do not lead to hosts that are members of group 1have been removed. The result is the multicast spanning tree for the leftmost router to send to group 1. Packets are forwarded only along this spanning tree, which is more efficient than the broadcast tree because there are 7 links instead of 10. Figure 7.8 (d) shows the multicast spanning tree after pruning for group 2. It is efficient too, with only five links this time. It also shows that different multicast groups have different spanning trees.

SELF-ASSESSMENT QUESTIONS – 2

11. Sending a packet to all destinations simultaneously is called_____.
12. A _____ is a subset of the network that includes all the routers but contains no loops.
13. Sending a message to a group is called _____.

4. ROUTING IN THE INTERNET

In this section, we will discuss the Internet's routing protocols. Their job is to determine the path taken by a datagram between source and destination. An autonomous system (AS) is a collection of routers under authority of a single administrator, and that all run the same routing protocol among themselves. Different routing protocols are discussed below:

4.1 Intra-AS Routing in the Internet: Routing Information Protocol (RIP)

An intra-AS routing protocol is used to determine how routing is performed within an autonomous system (AS). This is also known as *interior gateway protocols.* Two routing protocols have been used for routing within an autonomous system on the Internet. They are: *Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).*

RIP is a distance-vector protocol that traces its origins and its name to the Xerox Network Systems (XNS) architecture. In RIP (and also in OSPF), costs are actually from source router to a destination subnet. RIP uses the term hop, which is the number of subnets traversed along the shortest path from source router to destination subnet, including the destination subnet. In RIP, routing updates are exchanged between neighbors approximately every 30 seconds using a *RIP response message.* The response message sent by a router or host contains a list of up to 25 destination subnets within the AS, as well as the sender's distance to each of those subnets. Response messages are also known as *RIP advertisements.*

Each router maintains a RIP table known as a routing table. A router's routing table includes both the router's distance vector and the router's forwarding table. RIP has many distance vector characteristics such as: RIP sends out periodic routing updates in every 30 seconds, with every updates it sends out full routing table, it uses a form of distance as it's metric, it uses Bellman-Ford Distance Vector algorithm to determine the best "path" to a particular destination, it supports IP and IPX routing and RIP has a maximum hop count of 15 hops. A metric of 16 hops in RIP is considered a poison route or infinity metric.

RIP has four timers update, invalid, hold down and flush timer,

I. update timer - after that broadcast sent 30sec
II. invalid timer - after expiration, route declare as an invalid 180sec
III. hold down - what does happen after hold down timer expires 180sec

IV. Flush timer - after expiration, route entry deleted from routing table 240sec

4.2 Intra-AS Routing in the Internet: Open Shortest Path First (OSPF)

OSPF (Open Shortest Path First) is an intradomain routing protocol. Intradomain routing protocol which used distance vector design, is suitable for small systems but not suitable when the networks grow larger. It also suffers count to infinity problem. Then the internet switched over to a link state protocol and in 1988, link state protocol for intradomain routing is developed and is called OSPF. It drew on a protocol called IS-IS (Intermediate-System to Intermediate-System), which became an ISO standard. Because of their shared heritage, the two protocols are much more alike than different.

OSPF had a long list of requirements that had to be satisfied. First is that the algorithm had to be published in the open record. Second, it had to support a variety of distance metrics, including physical distance, delay, and so on. Third, it had to be a dynamic algorithm. The fourth requirement is that it had to support routing based on the type of service. Fifth, OSPF had to do load balancing by splitting the load over multiple lines. Sixth, support for hierarchical systems was needed. Seventh, some amount of security is needed to prevent from spoofing routers by sending them false routing information. Finally, an arrangement was needed for dealing with routers that were connected to the Internet via a tunnel. OSPF supports both point-to-point links (e.g., SONET) and broadcast networks (e.g., most LANs).

When a router boots, it sends HELLO messages on all of its point-to-point lines and multicasts them on LANs to the group consisting of all the other routers. From the responses, each router learns who its neighbors are.

Table 7.1: The five types of OSPF messages

Message Type	Description
Hello	Used to discover who the neighbors are
Link state update	Provides the sender's costs to its neighbors
Link state ack	Acknowledges link state update
Database description	Announces which updates the sender has
Link state request	Requests information from the partner

During normal operation, each router periodically floods link state update messages to each of its adjacent routers. These messages give its state and provide the costs used in the topological database. The flooding messages are acknowledged, to make them reliable. Database Description messages give the sequence numbers of all the link state entries currently held by the sender. Either partner can request link state information from the other one by using Link state request messages.

4.3 Inter-AS Routing: Border Gateway Protocol (BGP)

Within a single autonomous system, OSPF and IS-IS are the protocols that are commonly used. Between different autonomous systems, a different protocol, called *BGP (Border Gateway Protocol),* is used. A different protocol is needed because the goals of an intradomain protocol and an interdomain protocol are not the same. A routing policy is implemented by deciding what traffic can flow over which of the links between autonomous systems. One common policy is that a customer ISP pays another provider ISP to deliver packets to any other destination on the Internet and receive packets sent from any other destination. The customer ISP is said to buy *transit service* from the provider ISP.

Characteristics of Border Gateway Protocol (BGP):

- Inter-Autonomous System Configuration: The main role of BGP is to provide communication between two autonomous systems.
- BGP supports Next-Hop Paradigm.
- Coordination among multiple BGP speakers within the AS (Autonomous System).
- Path Information: BGP advertisement also includes path information, along with the reachable destination and next destination pair.
- Policy Support: BGP can implement policies that can be configured by the administrator. For example: - a router running BGP can be configured to distinguish between the routes that are known within the AS and those which are known from outside the AS.
- Runs Over TCP.
- BGP conserve network Bandwidth.
- BGP supports CIDR.
- BGP also supports Security.

Now we will discuss how routers run BGP, announce routes to each other and select paths over which to forward packets. BGP is a form of distance vector protocol, but it is quite different from intradomain distance vector protocols such as RIP. Instead of maintaining just the cost of the route to each destination, each BGP router keeps track of the path used. This approach is called a path vector protocol. The path consists of the next hop router, the sequence of Autonomous systems or AS path that the route has followed. Finally, pairs of BGP routers communicate with each other by establishing TCP connections. Operating this way provides reliable communication and also hides all the details of the network being passed through.

We need some way to propagate BGP routes from one side of the ISP to the other so that they can be sent on to the next ISP. This task could be handled by the intradomain protocol, but because BGP is very good at scaling large networks, a variant of BGP is often used. It is called *iBGP (internal BGP)* to distinguish it from the regular use of BGP as *eBGP (external BGP).*

BGP Route Information Management Functions:

- *Route Storage: Each BGP stores information about how to reach other networks.*
- *Route Update: In this task, Special techniques are used to determine when and how to use the information received from peers to properly update the routes.*
- *Route Selection: Each BGP uses the information in its route databases to select good routes to each network on the internet network.*
- *Route advertisement: Each BGP speaker regularly tells its peer what is knows about various networks and methods to reach them.*

SELF-ASSESSMENT QUESTIONS – 3

14. Two routing protocols have been used for routing within an autonomous system on the Internet are_____and _____.
15. RIP Response messages are also known as _____.
16. Link state protocol for intradomain routing is developed and is called
17. _____ is an example of an inter-AS Routing Protocol

5. SUMMARY

Let us recapitulate the important concepts discussed in this unit:

- Routing algorithms is a part of network layer software which is responsible for deciding the output line for an incoming packet to reach a particular destination.
- In *nonadaptive routing,* routing algorithms do not establish its routing decisions on measurements or estimates of the current topology and traffic. The routing decision is computed in advance and this information is downloaded to each router. This procedure is also called static routing.
- *Adaptive* algorithms change their routing decisions to reflect changes in the topology and changes in the traffic as well. This algorithm is also known as dynamic routing algorithm.
- The optimality principle states that if router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route.
- In case of flooding, every incoming packet is sent out on every outgoing line except the one it arrived on.
- Sending a packet to all destinations simultaneously is called *broadcasting.*
- Sending a packet to a subset of destinations or a group of destinations is known as *Multicasting.*
- An intra-AS routing protocol is used to determine how routing is performed within an autonomous system (AS). This is also known as *interior gateway protocols.*
- Two routing protocols have been used for routing within an autonomous system in the Internet. They are: *Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).*
- OSPF (Open Shortest Path First) is an intradomain routing protocol.
- Between different autonomous systems, a different protocol, called *BGP (Border Gateway Protocol),* is used.

6. TERMINAL QUESTIONS

1. Explain optimality principle.
2. Write short notes on shortest path algorithm and flooding.
3. Explain distance vector routing.
4. Describe link state routing.
5. Differentiate between multicasts and broadcast routing.
6. Explain routing on the Internet.

7. ANSWERS

Self-Assessment Questions

1. Routing algorithm
2. Non adaptive routing algorithm
3. Static routing
4. Dynamic routing
5. (a) True
6. Sink tree
7. Flooding
8. Distributed Bellman-Ford routing
9. Link State Routing
10. Regions
11. Broadcasting
12. Spanning tree
13. Multicasting
14. Routing information protocol (RIP) and Open Shortest Path First (OSPF)
15. RIP advertisements
16. OSPF
17. BGP (Border Gateway Protocol)

Terminal Questions

1. Optimality principle is a statement about optimal routes without considering network topology or traffic. It states that if router *J* is on the optimal path from router *I* to router

K, then the optimal path from J to K *also falls along the same route*. (Refer section 2 for more details).

2. The concept behind the shortest path algorithm is to build a graph of network in which each node represents a router and each edge of the graph represents a communication line or link. In case of flooding, every incoming packet is sent out on every outgoing line except the one it arrived on. Flooding generates a vast number of duplicate packets. (Refer section 2.1 and 2.2 for more details)
3. In distance vector routing, each router maintains a table giving the best-known distance to each destination and which link to use to reach there. These tables are updated by exchanging information with the neighbours. Distance vector routing is also known as the distributed Bellman-Ford routing algorithm. (Refer section 2.3 for more details).
4. Distance vector routing took too long to converge after the network topology changed, due to count to infinity problem. As a result, it is replaced by an entirely new algorithm, called **link state routing.** (Refer section 2.4 for more details).
5. Sending a packet to all destinations simultaneously is called broadcasting. Sending a packet to a subset of destinations or a group of destinations is known as Multicasting. (Refer section 3 for more details).
6. Internet's routing protocol's job is to determine the path taken by a datagram between source and destination. An autonomous system (AS) is a collection of routers under authority of a single administrator, and that all run the same routing protocol among themselves. (Refer section 4 for more details).

References:

- Andrew S. Tanenbaum, David J. Wetherall, "*Computer Networks,"* Fifth edition.
- Larry L. Peterson, Bruce S. Davie, *"Computer Networks – a Systems Approach,"* Fifth edition.
- James F. Kurose, Keith W.Ross, *"Computer Networking – A top-down approach,"* Sixth edition.
- Behrouz A. Forouzan, Sophia Chung Fegan, *"Data Communication and Networking,"* Fourth edition.
- William Stallings, *"Computer Networking with Internet Protocols and Technology,"* Third edition.