UNIT-4

NETWORK LAYER

1.Delivery:

The network layer supervises the handling of the packets by the underlying physical networks. We define this handling as the delivery of a packet.

- The **delivery** of a packet is called direct if the deliverer (host or **router**) and the destination are on the same **network**.
- The **delivery** of a packet is called indirect if the deliverer (host or **router**) and the destination are on different **network**.

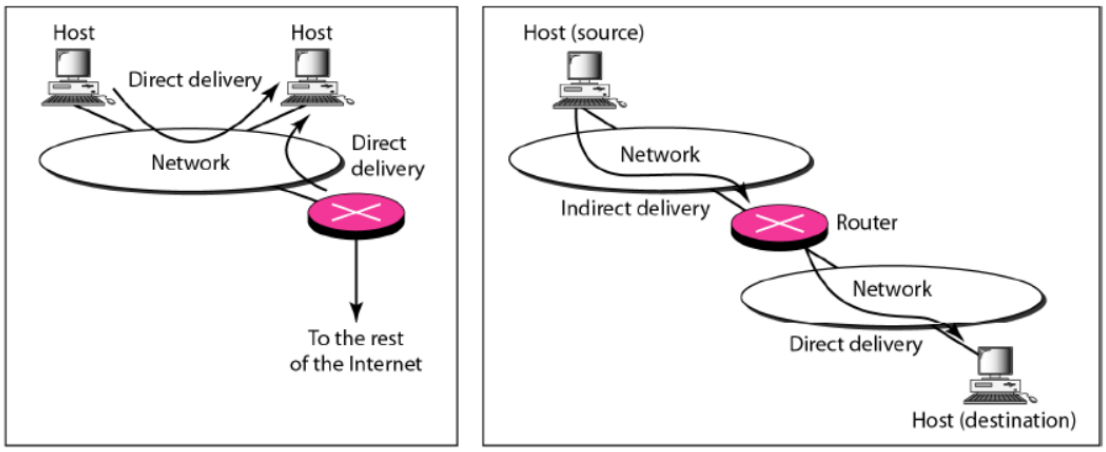


Figure: Direct and indirect delivery

2.Forwarding:

Forwarding means to place the packet in its route to its destination. Forwarding requires a host or a router to have a routing table. When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination.

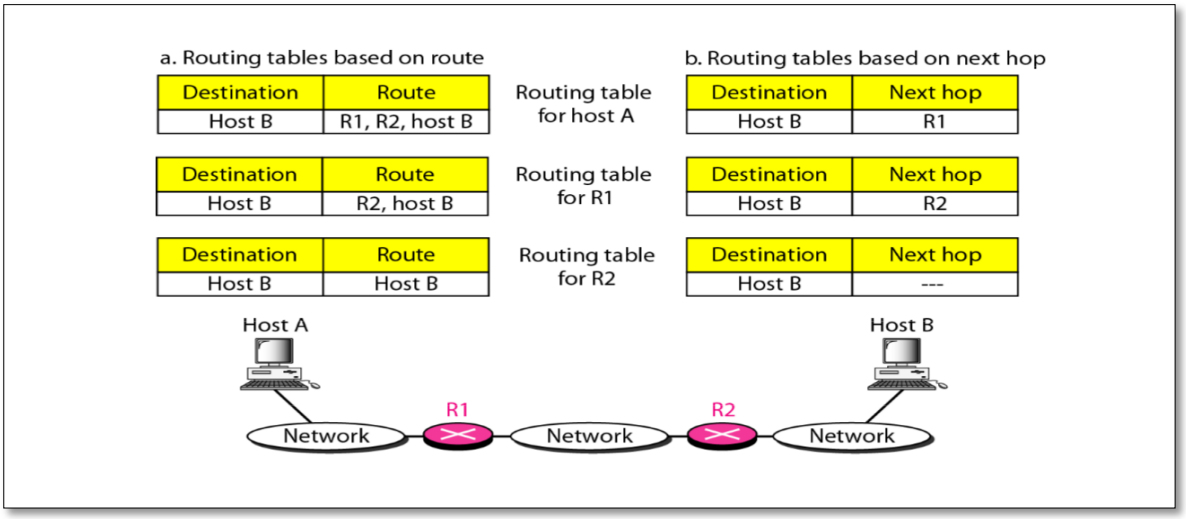
(i)Forwarding Techniques:

Several techniques can make the size of the routing table manageable and also handle issues such as security. We briefly discuss these methods here.

Next-Hop Method Versus Route Method

One technique to reduce the contents of a routing table is called the next-hop method. In this technique, the routing table holds only the address of the next hop

instead of information about the complete route (route method). The entries of a routing table must be consistent with one another.



. **Figure 22.2 Route method versus next-hop method**

Network-Specific Method Versus Host-Specific Method:

A second technique to reduce the routing table and simplify the searching process is called the network-specific method. Here, instead of having an entry for every destination host connected to the same physical network (host-specific method), we have only one entry that defines the address of the destination network itself. In other words, we treat all hosts connected to the same network as one single entity. For example, if 1000 hosts are attached to the same network, only one entry exists in the routing table instead of 1000.

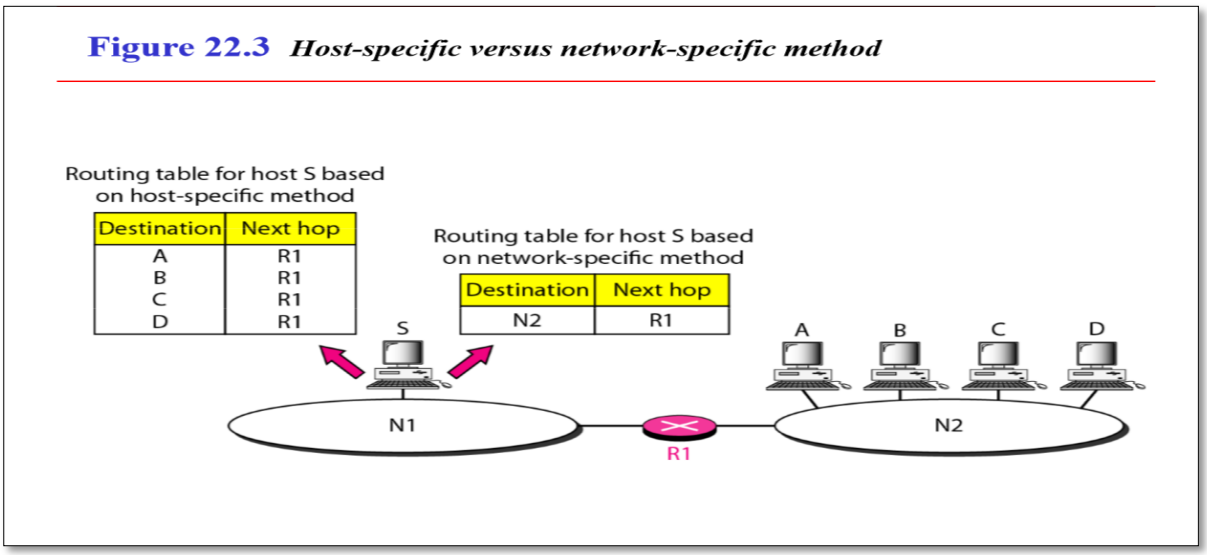


Figure 22.3 Host-specific versus network-specific method

Host-specific routing is used for purposes such as checking the route or providing security measures.

Default Method:

Another technique to simplify routing is called the default method. In Figure 22.4 host A is connected to a network with two routers. Router Rl routes the packets to hosts connected to network N2. However, for the rest of the Internet, router R2 is used. So instead of listing all networks in the entire Internet, host A can just have one entry called the default (normally defined as network address 0.0.0.0).

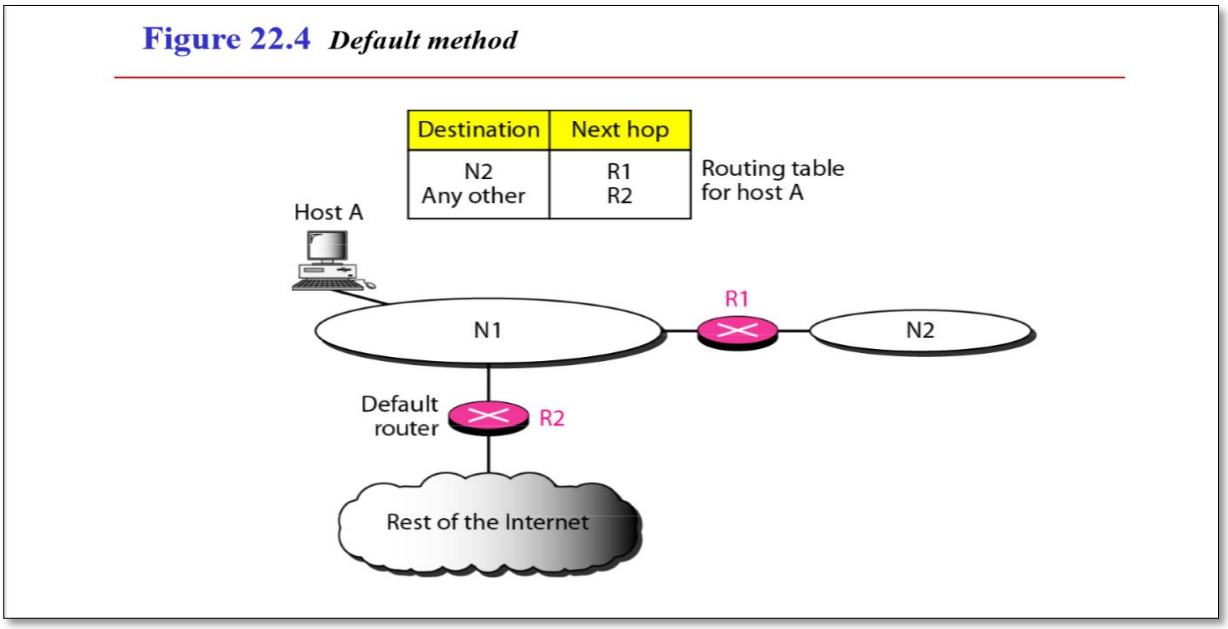
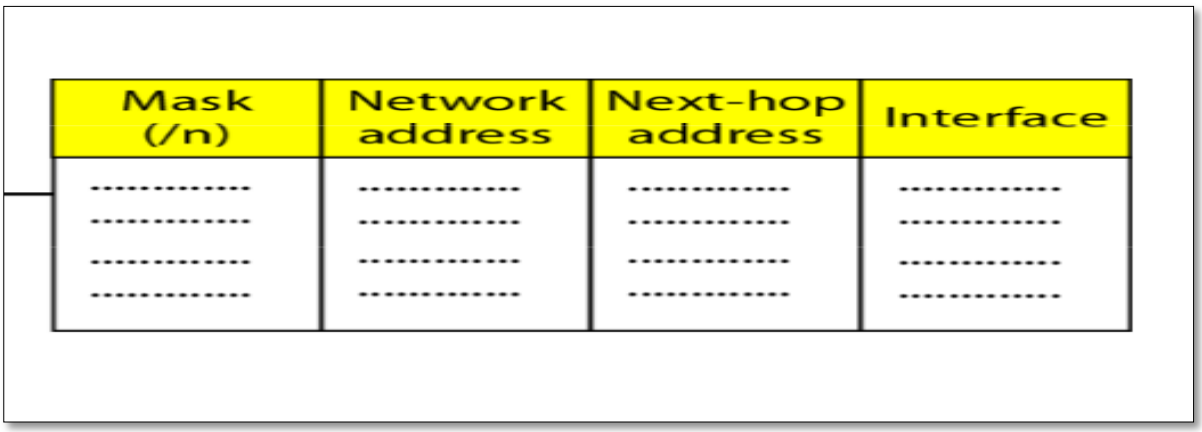


Figure 22.4 Default method

(ii)Forwarding Process:

When a packet arrives at a router's input link, the router must move the packet to the appropriate output link. For example, a packet arriving from Host H1 to Router R1 must be forwarded to the next router on a path to H2.

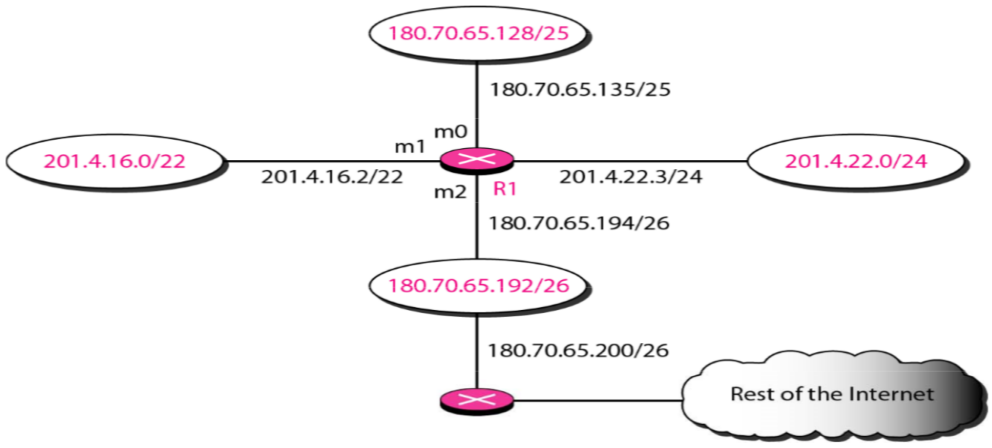
NOTE: In classless addressing, we need at least four columns in a routing table. Unfortunately, the destination address in the packet gives no clue about the network address. To solve the problem, we need to include the mask (In) in the table;



Example 22.1

Make a routing table for router R1 , using the configuration in Figure 22.6

Figure 22.6 *Configuration for Example 22.1*



Solution

Table 22.1 *Routing table for router R1 in Figure 22.6*

Mask	*Network Address*	*Next Hop*	*Interface*
/26	180.70.65.192	—	m2
/25	180.70.65.128	—	m0
/24	201.4.22.0	—	m3
/22	201.4.16.0	....	m1
Any	Any	180.70.65.200	m2

(iii)Routing Table

A host or a router has a routing table with an entry for each destination, or a combination of destinations, to route IP packets.

The routing table can be : 1.Static

2.Dynamic

Static Routing Table:

A static routing table contains information entered manually. The administrator enters the route for each destination into the table. When a table is

created, it cannot update automatically when there is a change in the Internet. The table must be manually altered by the administrator.
--A static routing table can be used in a small internet that does not change very often, or in an experimental internet for troubleshooting. Itis poor strategy to use a static routing table in a big internet such as the Internet.

Dynamic Routing Table:

A dynamic routing table is updated periodically by using one of the dynamic routing protocols such as RIP, OSPF, or BGP. Whenever there is a change in the Internet, such as a shutdown of a router or breaking of a link, the dynamic routing protocols update all the tables in the routers (and eventually in the host) automatically.
--The routers in a big internet such as the Internet need to be updated dynamically for efficient delivery of the IP packets.

Format:

A routing table for classless addressing has a minimum of four columns. However, some of today's routers have even more columns.

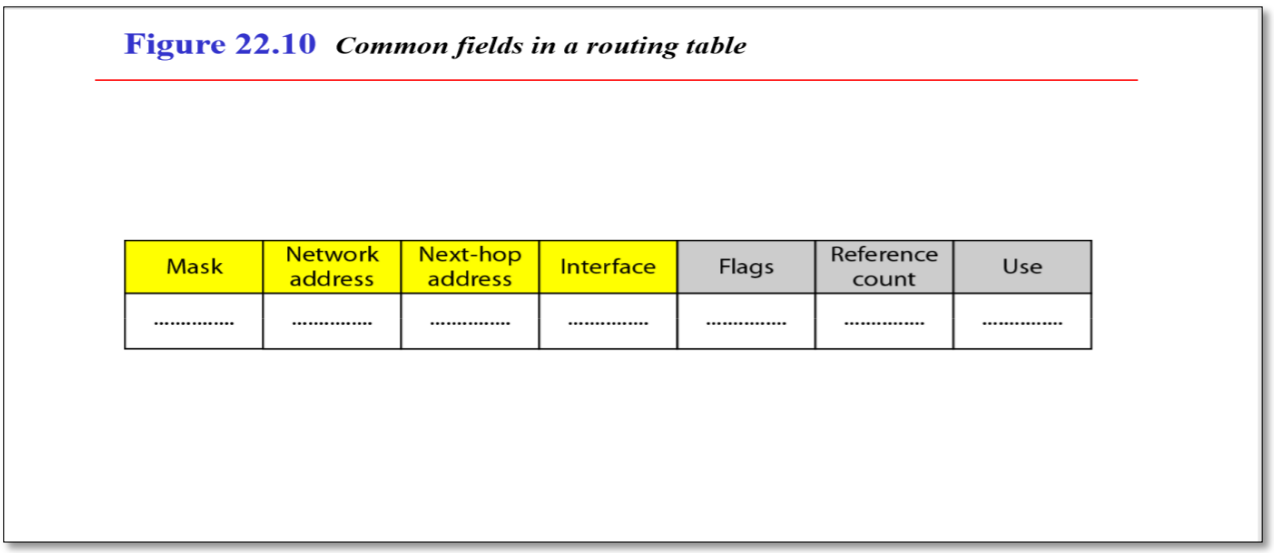


Figure 22.10 shows some common fields in today's routers

Mask: This field defines the mask applied for the entry.
Network address: This field defines the network address to which the packet is finally delivered. In the case of host-specific routing, this field defines the address of the destination host.
Next-hop address: This field defines the address of the next-hop router to which the packet is delivered.
Interface: This field shows the name of the interface.
Flags: This field defines up to five flags. Flags are on/off switches that signify either presence or absence. The five flags are U (up), G (gateway), H (host-specific), D (added by redirection), and M (modified by redirection).

a. U (up). The U flag indicates the router is up and running. If this flag is not present, it means that the router is down. The packet cannot be forwarded and is discarded.

b. G (gateway). The G flag means that the destination is in another network. The packet is delivered to the next-hop router for delivery (indirect delivery). When this flag is missing, it means the destination is in this network (direct delivery).

c. H (host-specific). The H flag indicates that the entry in the network address field is a host-specific address. When it is missing, it means that the address is only the network address of the destination.

d. D (added by redirection). The D flag indicates that routing information for this destination has been added to the host routing table by a redirection message from ICMP.

e. M (modified by redirection). The M flag indicates that the routing information for this destination has been modified by a redirection message from ICMP.

Reference count: This field gives the number of users of this route at the moment. For example, if five people at the same time are connecting to the same host from this router, the value of this column is 5.

Use: This field shows the number of packets transmitted through this router for the corresponding destination.

3.UNICAST ROUTING PROTOCOLS:

Routing protocols have been created in response to the demand for dynamic routing tables. A routing protocol is a combination of rules and procedures that lets routers in the internet inform each other of changes. It allows routers to share whatever they know about the internet or their neighbourhood. The routing protocols also include procedures for combining information received from other routers.

(i)Optimization:

A router receives a packet from a network and passes it to another network. When it receives a packet, to which network should it pass the packet? The decision is based on optimization.

=>**What is the definition of the term optimum?**

One approach is to assign a cost for passing through a network. We call this cost a metric. However, the metric assigned to each network depends on the type of protocol. Some simple protocols, such as the Routing Information Protocol (RIP), treat all networks as equals. The cost of passing through a network is the same; it is one hop count. So if a packet passes through 10 networks to reach the destination, the total cost is 10 hop counts.

Other protocols, such as Open Shortest Path First (OSPF), allow the administrator to assign a cost for passing through a network based on the type of

service required. A route through a network can have different costs (metrics). For example, if maximum throughput is the desired type of service, a satellite link has a lower metric than a fiber-optic line. On the other hand, if minimum delay is the desired type of service, a fiber-optic line has a lower metric than a satellite link. Routers use routing tables to help decide the best route. OSPF protocol allows each router to have several routing tables based on the required type of service.

Other protocols define the metric in a totally different way. In the Border Gateway Protocol (BGP), the criterion is the policy, which can be set by the administrator. The policy defines what paths should be chosen.

(ii)Intra- and Interdomain Routing:

Routing inside an autonomous system is referred to as **intradomain** routing. An autonomous system (AS) is a group of networks and routers under the authority of a single administration. Routing between autonomous systems is referred to as interdomain routing. Each autonomous system can choose one or more intradomain routing protocols to handle routing inside the autonomous system. However, only one **interdomain** routing protocol handles routing between autonomous systems

Figure 22.12 *Autonomous systems*

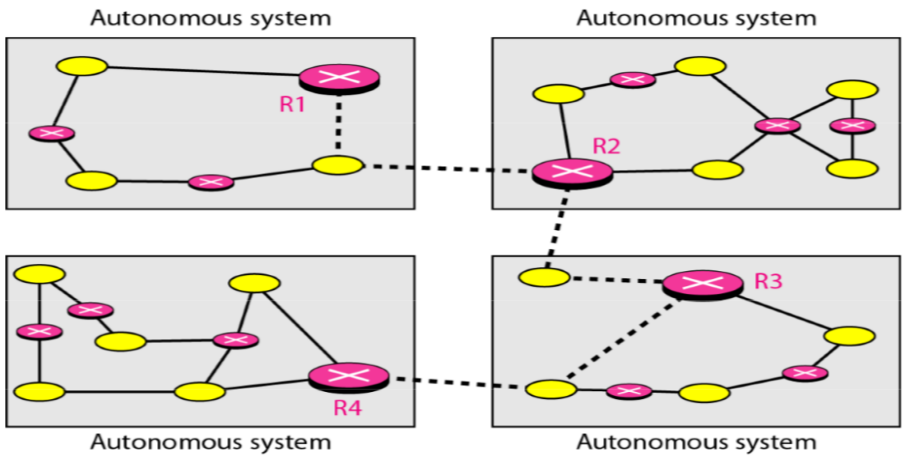
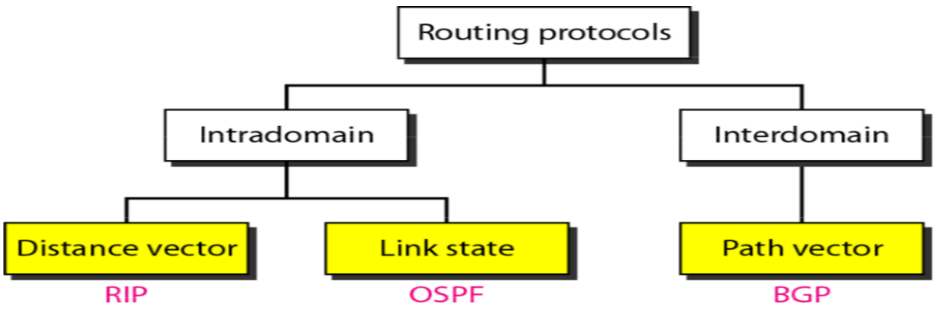


Figure 22.13 *Popular routing protocols*



(iii)Distance Vector Routing:

In **distance vector routing**, the least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node. The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).

Figure 22.14 *Distance vector routing tables*

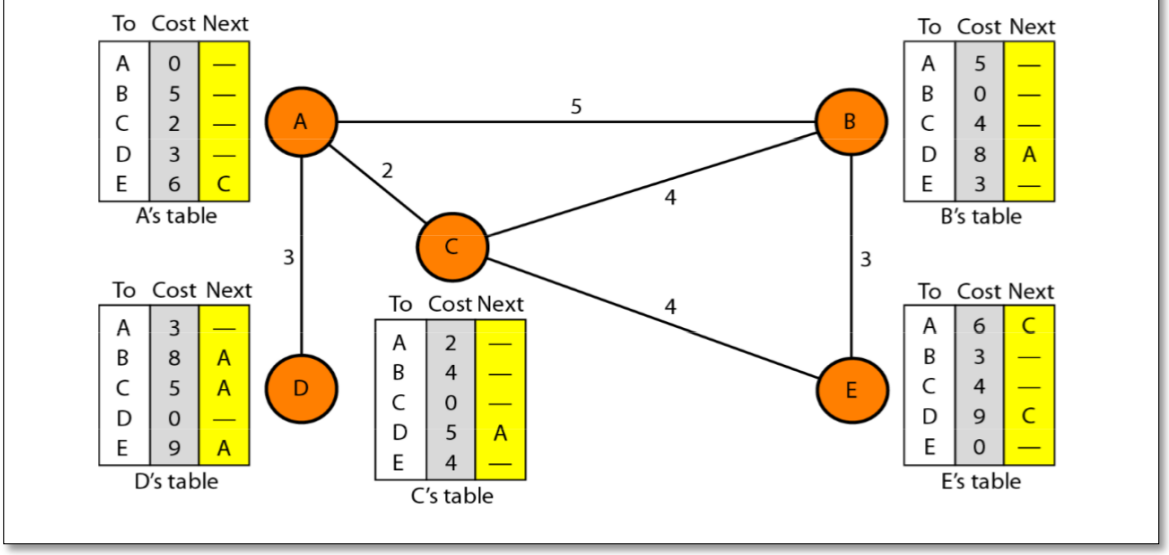
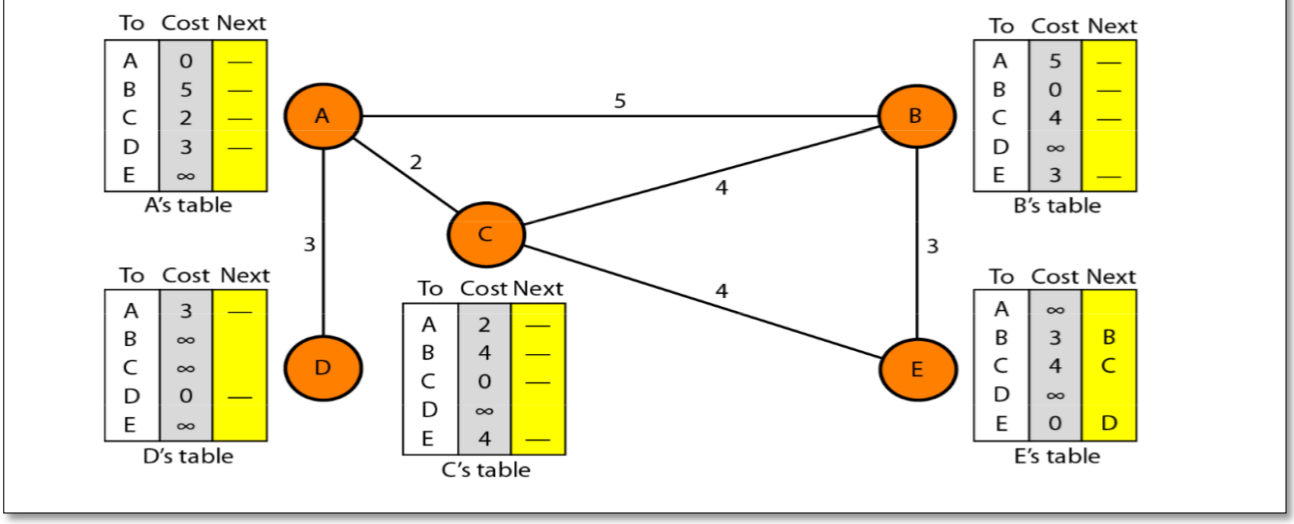


Figure 22.15 shows the initial tables for each node. The distance for any entry that is not a neighbour is marked as infinite (unreachable).

Figure 22.15 *Initialization of tables in distance vector routing*



In distance vector routing, each node shares its routing table with its immediate neighbors periodically and when there is a change.

Sharing:

The whole idea of distance vector routing is the sharing of information between neighbours.

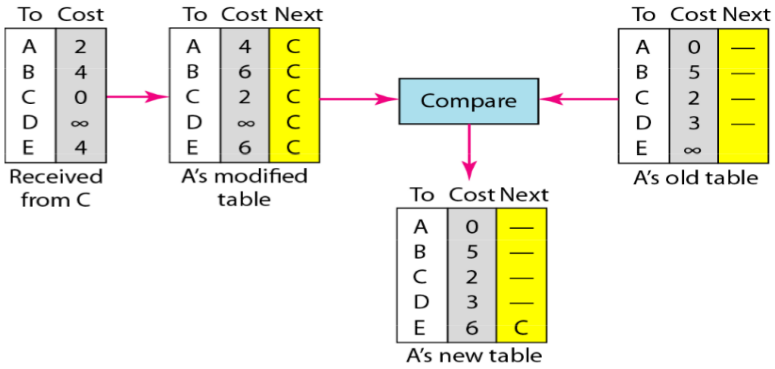
- Although node A does not know about node E, node C does. So if node C shares its routing table with A, node A can also know how to reach node E. On the other hand, node C does not know how to reach node D, but node A does.

-If node A shares its routing table with node C, node C also knows how to reach node D.

- There is only one problem. How much of the table must be shared with each neighbour? A node is not aware of a neighbour's table. The best solution for each node is to send its entire table to the neighbour and let the neighbour decide what part to use and what part to discard.

- In other words, sharing here means sharing only the first two columns.

Figure 22.16 *Updating in distance vector routing*



When to Share

-When does a node send its partial routing table (only two columns) to all its immediate neighbours? The table is sent both periodically and when there is a change in the table.

Periodic Update: A node sends its routing table, normally every 30 s, in a periodic update. The period depends on the protocol that is using distance vector routing.

Triggered Update :A node sends its two-column routing table to its neighbours anytime there is a change in its routing table. This is called a triggered update. The change can result from the following.

1. A node receives a table from a neighbour, resulting in changes in its own table after updating.
2. A node detects some failure in the neighbouring links which results in a distance change to infinity.

RIP

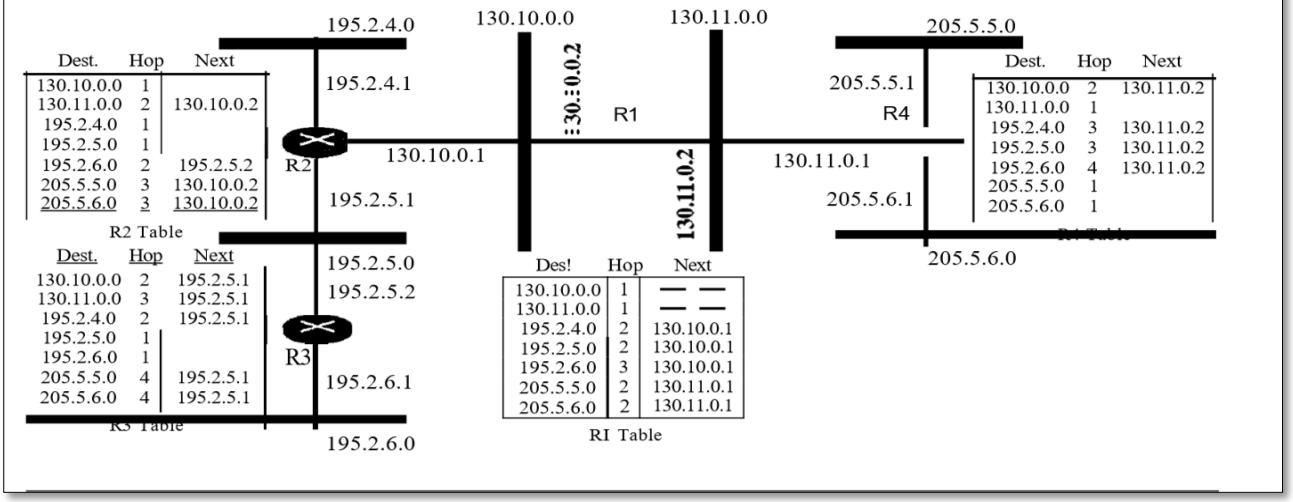
The Routing Information Protocol (RIP) is an intradomain routing protocol used inside an autonomous system. It is a very simple protocol based on distance vector routing. RIP implements distance vector routing directly with some considerations:

1. In an autonomous system, we are dealing with routers and networks (links). The routers have routing tables; networks do not.
2. The destination in a routing table is a network, which means the first column defines a network address.
3. The metric used by RIP is very simple; the distance is defined as the number of links (networks) to reach the destination. For this reason, the metric in RIP is called a hop count.

4. Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops.
5. The next-node column defines the address of the router to which the packet is to be sent to reach its destination.

Figure 22.19 shows an autonomous system with seven networks and four routers. The table of each router is also shown. Let us look at the routing table for Rl . The table has seven entries to show how to reach each network in the autonomous system.

Figure 22.19 *Example ofa domain using RIP*

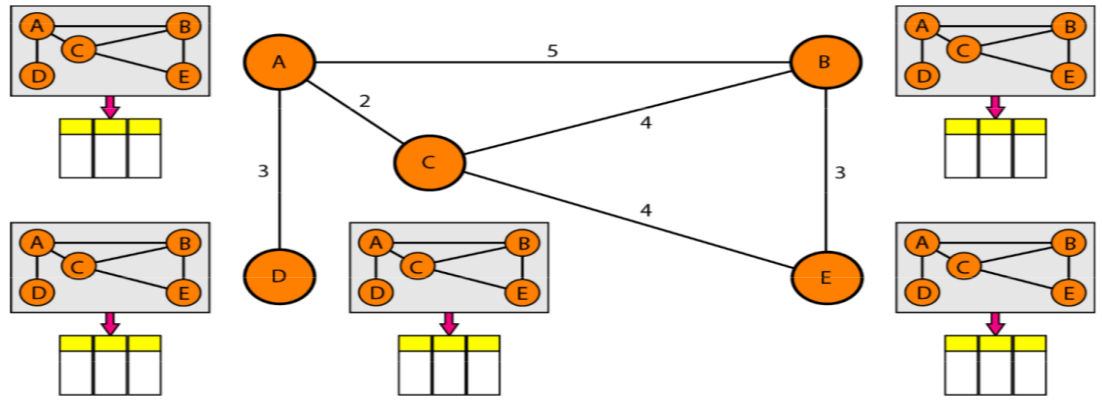


Router R1 is directly connected to networks 130.10.0.0 and 130.11.0.0, which means that there are no next-hop entries for these two networks. To send a packet to one of the three networks at the far left, router R1 needs to deliver the packet to R2. The next-node entry for these three networks is the interface of router R2 with IP address 130.10.0.1. To send a packet to the two networks at the far right, router R1 needs to send the packet to the interface of router R4 with IP address 130.11.0.1. The other tables can be explained similarly.

(iv)Link State Routing:

Link state routing has a different philosophy from that of distance vector routing. In link state routing, if each node in the domain has the entire topology of the domain the list of nodes and links, how they are connected including the type, cost (metric), and condition of the links (up or down)-the node can use Dijkstra's algorithm to build a routing table.

Figure 22.20 *Concept of link state routing*

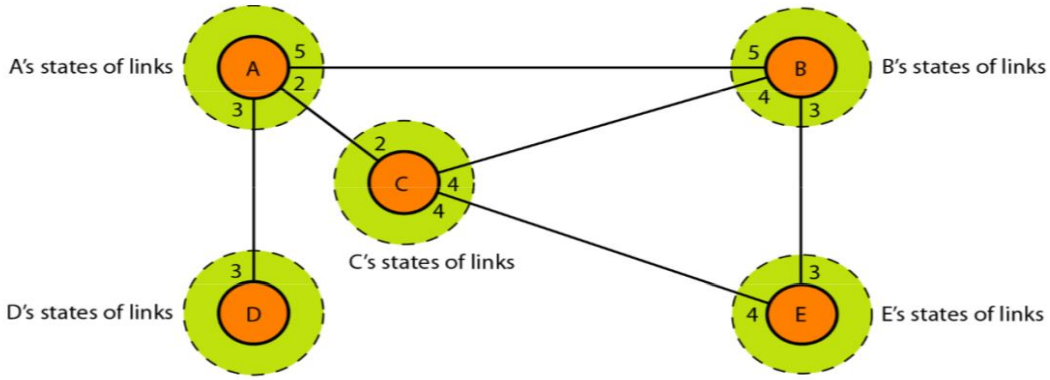


The figure shows a simple domain with five nodes. Each node uses the same topology to create a routing table, but the routing table for each node is unique because the calculations are based on different interpretations of the topology. This is analogous to a city map. While each person may have the same map, each needs to take a different route to reach her specific destination.

The topology must be dynamic, representing the latest state of each node and each link. If there are changes in any point in the network (a link is down, for example), the topology must be updated for each node.

Link state routing is based on the assumption that, although the global knowledge about the topology is not clear, each node has partial knowledge: it knows the state (type, condition, and cost) of its links. In other words, the whole topology can be compiled from the partial knowledge of each node.

Figure 22.21 *Link state knowledge*



Building Routing Tables

In link state routing, four sets of actions are required to ensure that each node has the routing table showing the least-cost node to every other node.

]. Creation of the states of the links by each node, called the link state packet (LSP).

2. Dissemination of LSPs to every other router, called flooding, in an efficient and reliable way.

3. Formation of a shortest path tree for each node.

4. Calculation of a routing table based on the shortest path tree.

Creation of Link State Packet (LSP) A link state packet can carry a large amount of information. For the moment, however, we assume that it carries a minimum amount of data: the node identity, the list of links, a sequence number, and age. The first two, node identity and the list of links, are needed to make the topology. The third, sequence number, facilitates flooding and distinguishes new LSPs from old ones. The fourth, age, prevents old LSPs from remaining in the domain for a long time. LSPs are generated on two occasions:

1. When there is a change in the topology of the domain. Triggering of LSP dissemination is the main way of quickly informing any node in the domain to update its topology.

2. On a periodic basis. The period in this case is much longer compared to distance vector routing. As a matter of fact, there is no actual need for this type of LSP dissemination. It is done to ensure that old information is removed from the domain. The timer set for periodic dissemination is normally in the range of 60 min or 2 h based on the implementation. A longer period ensures that flooding does not create too much traffic on the network.

Flooding of LSPs After a node has prepared an LSP, it must be disseminated to all other nodes, not only to its neighbours. The process is called flooding and based on the following:

1. The creating node sends a copy of the LSP out of each interface.

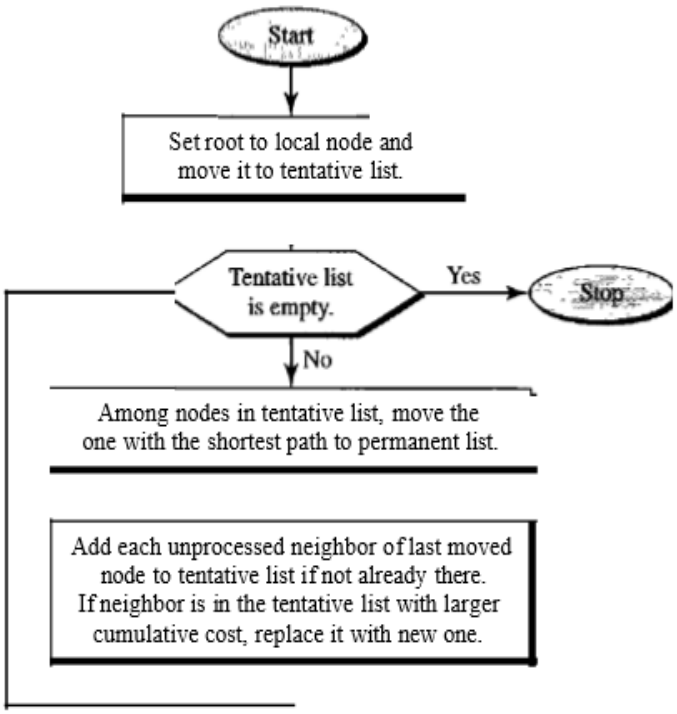
2. A node that receives an LSP compares it with the copy it may already have. If the newly arrived LSP is older than the one it has (found by checking the sequence number), it discards the LSP. I fit is newer, the node does the following:

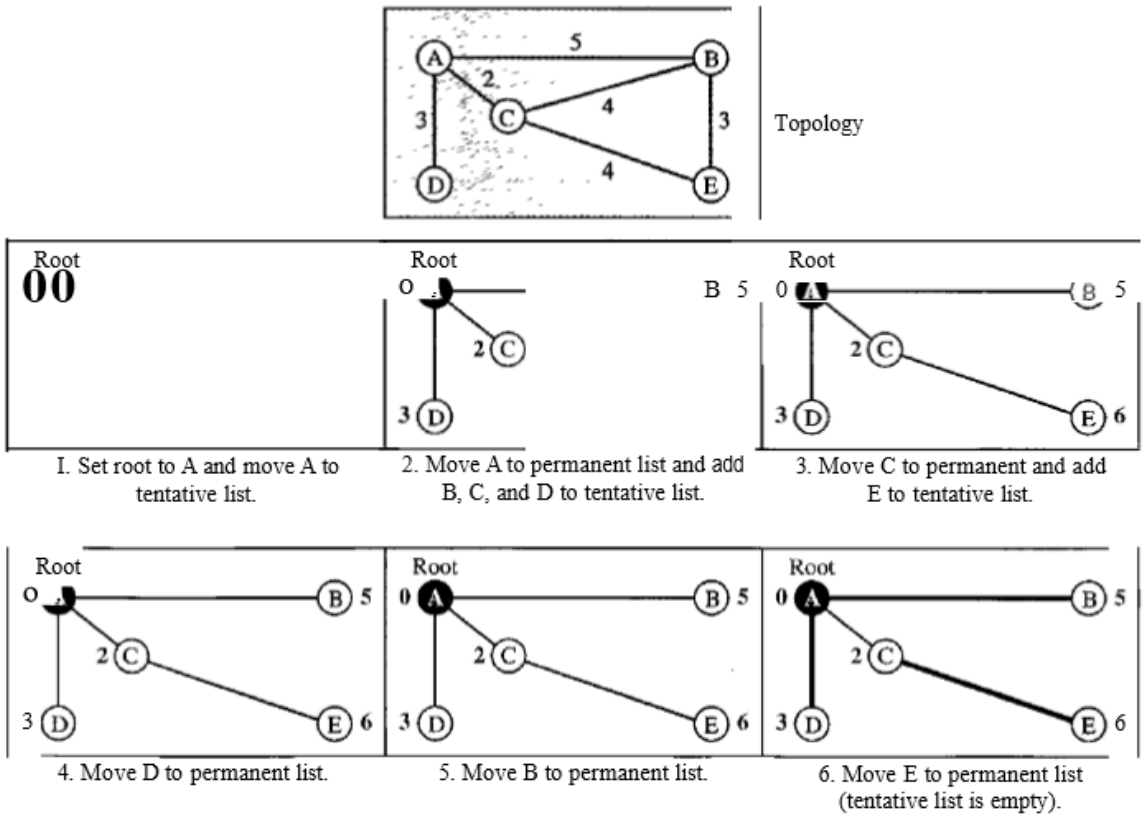
a. It discards the old LSP and keeps the new one.

b. It sends a copy of it out of each interface except the one from which the packet arrived. This guarantees that flooding stops somewhere in the domain (where a node has only one interface).

Formation of Shortest Path Tree: Dijkstra Algorithm After receiving all LSPs, each node will have a copy of the whole topology. However, the topology is not sufficient to find the shortest path to every other node; a shortest path tree is needed. A tree is a graph of nodes and links; one node is called the root. All other nodes can be reached from the root through only one single route. A shortest path tree is a tree in which the path between the root and every other

node is the shortest. What we need for each node is a shortest path tree with that node as the root. The Dijkstra algorithm creates a shortest path tree from a graph. The algorithm divides the nodes into two sets: tentative and permanent. It finds the neighbours of a current node, makes them tentative, examines them, and if they pass the criteria, makes them permanent.
The following shows the steps. At the end of each step, we show the permanent (filled circles) and the tentative (open circles) nodes and lists with the cumulative costs.





1. We make node A the root of the tree and move it to the tentative list. Our two lists are
Permanent list: empty Tentative list: A(O)
2. Node A has the shortest cumulative cost from all nodes in the tentative list. We move A to the permanent list and add all neighbours of A to the tentative list. Our new lists are
Permanent list: A(O) Tentative list: B(5), C(2), D(3)
3. Node C has the shortest cumulative cost from all nodes in the tentative list. We move C to the permanent list. Node C has three neighbours, but node A is already processed, which makes the unprocessed neighbours just B and E. However, B is already in the tentative list with a cumulative cost of 5. Node A could also reach node B through C with a cumulative cost of6. Since 5 is less than 6, we keep node B with a cumulative cost of5 in the tentative list and do not replace it. Our new lists are
Permanent list: A(O), e(2) Tentative list: B(5), 0(3), E(6)
4. Node D has the shortest cumulative cost of all the nodes in the tentative list. We move D to the permanent list. Node D has no unprocessed neighbour to be added to the tentative list. Our new lists are
Permanent list: A(O), C(2), 0(3) Tentative list: B(5), E(6)
5. Node B has the shortest cumulative cost of all the nodes in the tentative list. We move B to the permanent list. We need to add all unprocessed neighbours of B to the tentative list (this is just node E). However, E(6) is already in the list

with a smaller cumulative cost. The cumulative cost to node E, as the neighbour of B, is 8. We keep node E(6) in the tentative list. Our new lists are
Permanent list: A(O), B(5), C(2), 0(3) Tentative list: E(6)
6. Node E has the shortest cumulative cost from all nodes in the tentative list. We move E to the permanent list. Node E has no neighbour. Now the tentative list is empty. We stop; our shortest path tree is ready. The final lists are
Permanent list: A(O), B(5), C(2), D(3), E(6) Tentative list: empty
Calculation of Routing Table from Shortest Path Tree Each node uses the shortest path tree protocol to construct its routing table. The routing table shows the cost of reaching each node from the root. Table 22.2 shows the routing table for node A.

Table 22.2 *Routing table for node A*

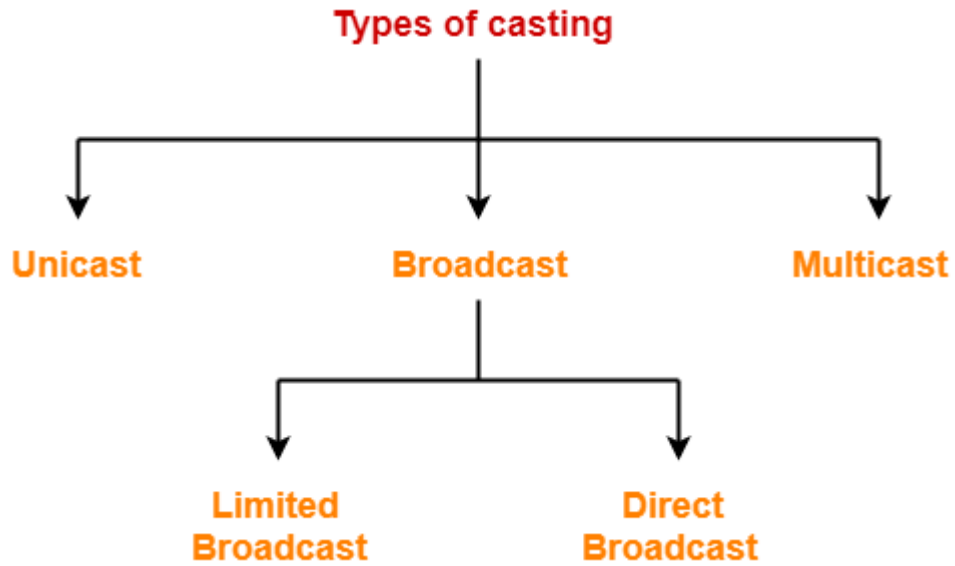
Node	*Cost*	*Next Router*
A	0	-
B	5	-
C	2	-
D	3	-
E	6	C

4.MULTICAST ROUTING PROTOCOLS:

Casting in Networking-

Transmitting data(stream of packets)over the network is termed as **casting.**

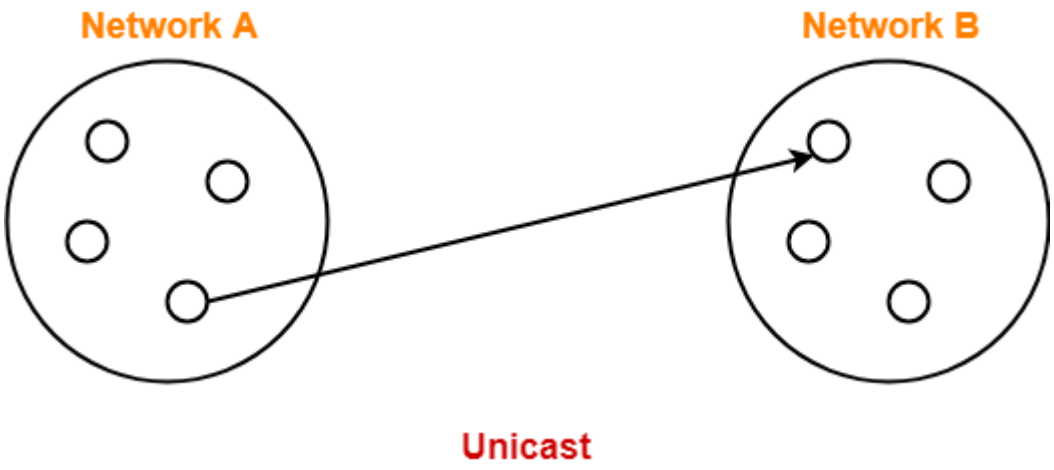
Types Of Casting-



1. Unicast
2. Broadcast
3. Multicast

1. Unicast-

- Transmitting data from one source host to one destination host is called as **unicast**.
- It is a one to one transmission.



Example-

Host A having IP Address 11.1.2.3 sending data to host B having IP Address 20.12.4.2.

Here,

- Source Address = IP Address of host A = 11.1.2.3
- Destination Address = IP Address of host B = 20.12.4.2

2. Broadcast-

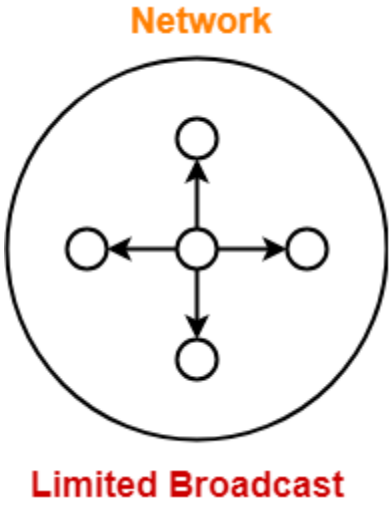
- Transmitting data from one source host to all other hosts residing in the same or other network is called as **broadcast**.
- It is a one to all transmission.

Based on recipient's network, it is classified as-

A. Limited Broadcast
B. Direct Broadcast

A. Limited Broadcast-

- Transmitting data from one source host to all other hosts residing in the same network is called as **limited broadcast**.



NOTE

Limited Broadcast Address for any network

= All 32 bits set to 1

= 11111111.11111111.11111111.11111111

= 255.255.255.255

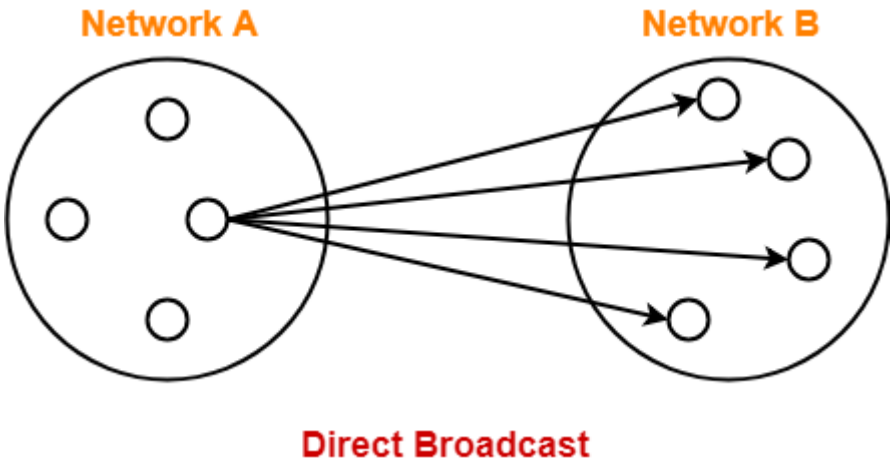
Example-

Host A having IP Address 11.1.2.3 sending data to all other hosts residing in the same network.Here,

- Source Address = IP Address of host A = 11.1.2.3
- Destination Address = 255.255.255.255

- ## B. Direct Broadcast-

- Transmitting data from one source host to all other hosts residing in some other network is called as **direct broadcast**.



NOTE

Direct Broadcast Address for any network is the IP Address where-

- Network ID is the IP Address of the network where all the destination hosts are present.
- Host ID bits are all set to 1.

Example-

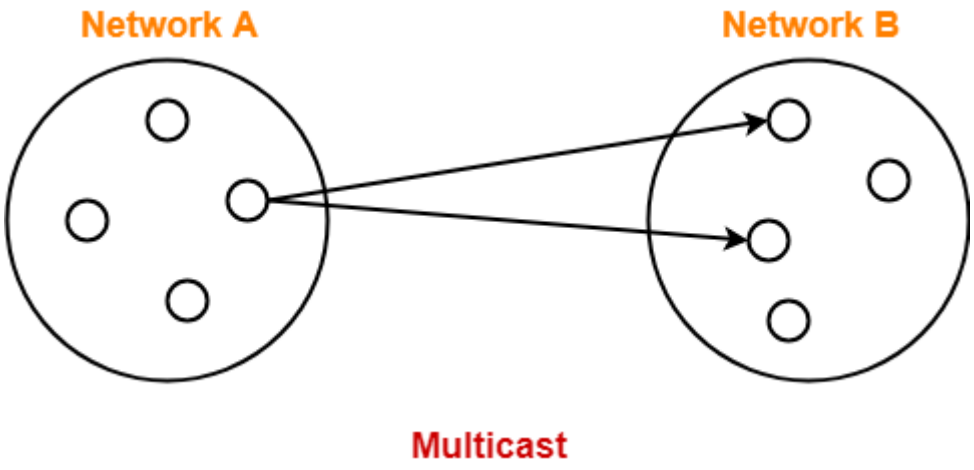
Host A having IP Address 11.1.2.3 sending data to all other hosts residing in the network having IP Address 20.0.0.0

Here,

- Source Address = IP Address of host A = 11.1.2.3
- Destination Address = 20.255.255.255

3. Multicast-

- Transmitting data from one source host to a particular group of hosts having interest in receiving the data is called as **multicast**.
- It is a one to many transmission.



Examples-

- Sending a message to a particular group of people on whatsapp
- Sending an email to a particular group of people
- Video conference or teleconference

MAC Address Vs IP Address-

The following table summarizes the differences between MAC Address and IP Address-

MAC Address	IP Address
It stands for Media Access Control Address.	It stands for Internet Protocol Address.
MAC Address identifies the physical address of a computer on the internet.	IP Address identifies the connection of a computer on the internet.

Manufacturer of NIC card assigns the MAC Address.	Network Administrator or ISP assigns the IP Address.
Reverse Address Resolution Protocol (RARP) is used for resolving physical (MAC) Address into IP address.	Address Resolution Protocol (ARP) is used for resolving IP Address into physical (MAC) address.

Multicast Routing:

we first discuss the idea of optimal routing, common in all multicast protocols. We then give an overview of multicast routing protocols.

Optimal Routing: Shortest Path Trees

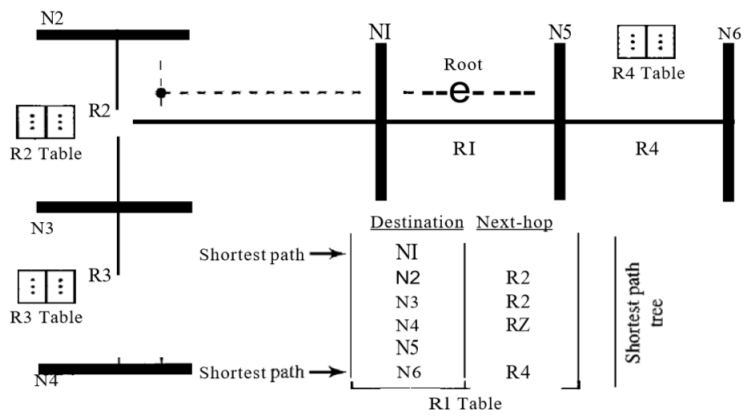
The process of optimal interdomain routing eventually results in the finding of the shortest path tree. The root of the tree is the source, and the leaves are the potential destinations. The path from the root to each destination is the shortest path. However, the number of trees and the formation of the trees in unicast and multicast routing are different.

Unicast Routing

In unicast routing, when a router receives a packet to forward, it needs to find the shortest path to the destination of the packet. The router consults its routing table for that particular destination. The next-hop entry corresponding to the destination is the start of the shortest path. In unicast routing, each router needs only one shortest path tree to forward a packet; however, each router has its own shortest path tree.

Figure 22.36 shows the situation.

Figure 22.36 *Shortest path tree in unicast routing*



In unicast routing, each router in the domain has a table that defines a shortest path tree to possible destinations.

Multicast Routing

When a router receives a multicast packet, the situation is different from when it receives a unicast packet. A multicast packet may have destinations in more than one network. Forwarding of a single packet to members of a group requires a shortest path tree. If we have n groups, we may need n shortest path trees. We can imagine the complexity of multicast routing.

->**Two** approaches have been used to solve the problem:

1.source-based trees

2.group-shared trees

1.Source-Based Tree:

In the source-based tree approach, each router needs to have one shortest path tree for each group. The shortest path tree for a group defines the next hop for each network that has loyal member(s) for that group.

In **Figure 22.37**, we assume that we have only five groups in the domain: GI, G2, G3, G4, and G5. At the moment GI has loyal members in four networks, G2 in three, G3 in two, G4 in two, and G5 in two. We have shown the names of the groups with loyal members on each network.

Figure 22.37 *Source-based tree approach*

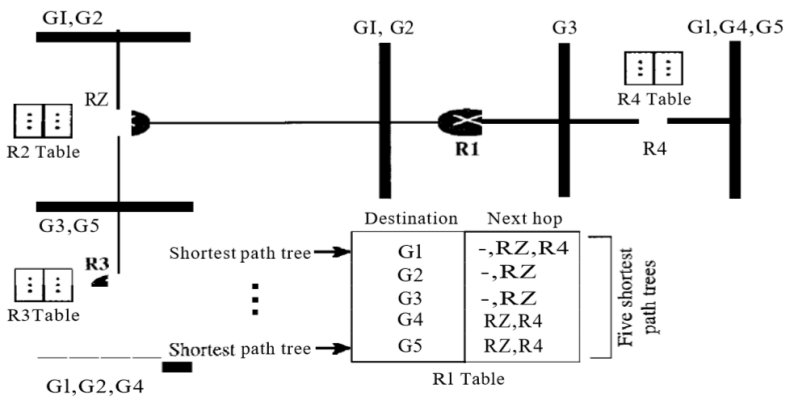


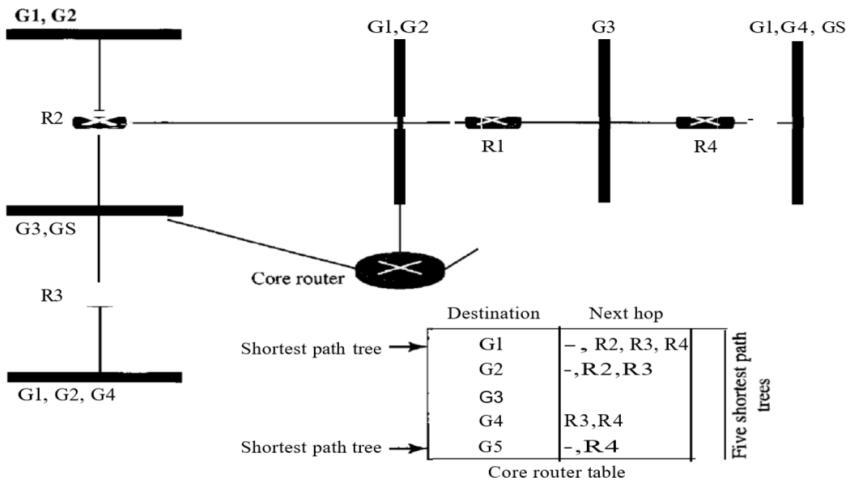
Figure 22.37 also shows the multicast routing table for router RI. There is one shortest path tree for each group; Therefore there are five shortest path trees for five groups. If router R1 receives a packet with destination address G1, it needs to send a copy of the packet to the attached network, a copy to router R2, and a copy to router R4 so that all members of G1 can receive a copy.

- In this approach, if the number of groups is *m*, each router needs to have *m* shortest path trees, one for each group.

Group-Shared Tree:

In the group-shared tree approach, instead of each router having *m* shortest path trees, only one designated router, called the centre core, or rendezvous router, takes the responsibility of distributing multicast traffic. The core has *m* shortest path trees in its routing table. The rest of the routers in the domain have none. If a router receives a multicast packet, it encapsulates the packet in a unicast packet and sends it to the core router. The core router removes the multicast packet from its capsule, and consults its routing table to route the packet. Figure 22.38 shows the idea.

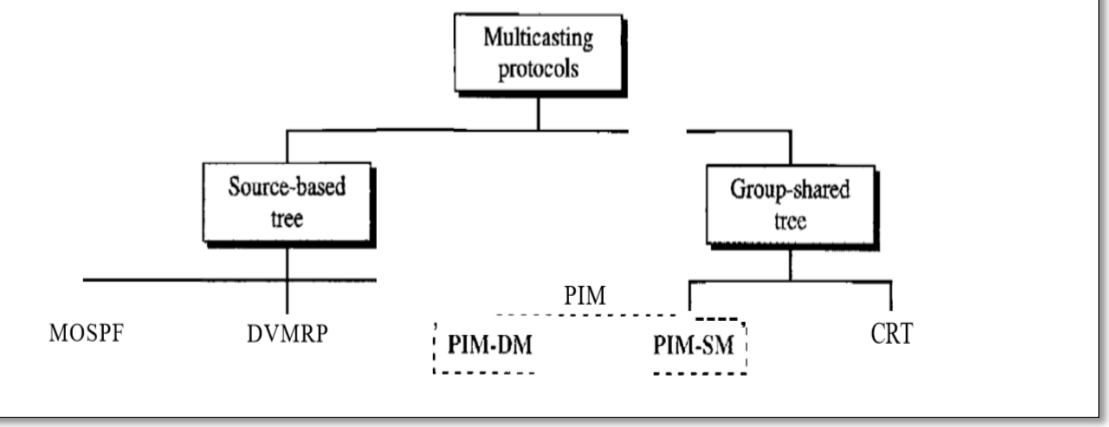
Figure 22.38 *Group-shared tree approach*



In the group-shared tree approach, only the core router, which has a shortest path tree for each group, is involved in multicasting.

(iv)Routing Protocols:

Figure 22.39 *Taxonomy of common multicast protocols*



Multicast Link State Routing: MOSPF

The routing table is a translation of the shortest path tree. Multicast link state routing is a direct extension of unicast routing and uses a source-based tree

approach. Although unicast routing is quite involved, the extension to multicast routing is very simple and straightforward.
-Multicast link state routing uses the source-based tree approach.
Recall that in unicast routing, each node needs to advertise the state of its links. For multicast routing, a node needs to revise the interpretation of state. A node advertises every group which has any loyal member on the link. Here the meaning of state is "what groups are active on this link. "

The only problem with this protocol is the time and space needed to create and save the many shortest path trees. The solution is to create the trees only when needed. When a router receives a packet with a multicast destination address, it runs the Dijkstra algorithm to calculate the shortest path tree for that group. The result can be cached in case there are additional packets for that destination.

MOSPF Multicast Open Shortest Path First (MOSPF) protocol is an extension of the OSPF protocol that uses multicast link state routing to create source-based trees. MOSPF is a data-driven protocol; the first time an MOSPF router sees a datagram with a given source and group address, the router constructs the Dijkstra shortest path tree.

Multicast Distance Vector: DVMRP

Multicast Distance Vector Routing Unicast distance vector routing is very simple; extending it to support multicast routing is complicated. Multicast routing does not allow a router to send its routing table to its neighbours. The idea is to create a table from scratch by using the information from the unicast distance vector tables. Multicast distance vector routing uses source-based trees, but the router never actually makes a routing table. When a router receives a multicast packet, it forwards the packet as though it is consulting a routing table. We can say that the shortest path tree is evanescent. After its use (after a packet is forwarded) the table is destroyed.

To accomplish this, the multicast distance vector algorithm uses a process based on four decision-making strategies. Each strategy is built on its predecessor.

1.Flooding
2. Reverse Path Forwarding (RPF)
3. Reverse Path Broadcasting (RPB)
4. Reverse Path Multicasting (RPM)

DVMRP The Distance Vector Multicast Routing Protocol (DVMRP) is an implementation of multicast distance vector routing. It is a source-based routing protocol, based on RIP.

CRT

The Core-Based Tree (CBT) protocol is a group-shared protocol that uses a core as the root of the tree. The autonomous system is divided into regions, and a core (centre router or rendezvous router) is chosen for each region.

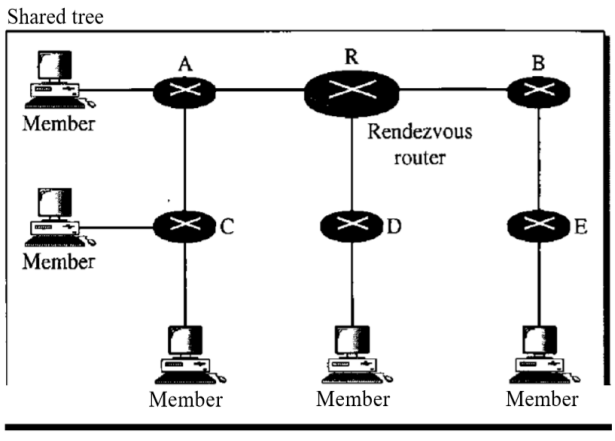
Formation of the Tree After the rendezvous point is selected, every router is informed of the unicast address of the selected router. Each router then sends a unicast join message (similar to a grafting message) to show that it wants to join the group. This message passes through all routers that are located between the sender and the rendezvous router.

Each intermediate router extracts the necessary information from the message, such as the unicast address of the sender and the interface through which the packet has arrived, and forwards the message to the next router in the path. When the rendezvous router has received all join messages from every member of the group, the tree is formed. Now every router knows its upstream router (the router that leads to the root) and the downstream router (the router that leads to the leaf).

If a router wants to leave the group, it sends a leave message to its upstream router. The upstream router removes the link to that router from the tree and forwards the message to its upstream router, and so on.

Figure 22.44 shows a group-shared tree with its rendezvous router.

Figure 22.44 *Group-shared tree with rendezvous router*



This approach is simple except for one point. How do we select a rendezvous router to optimize the process and multicasting as well? Several methods have been implemented. However, this topic is beyond the scope of this book, and we

leave it to more advanced books. In summary, the Core-Based Tree (CBT) is a group-shared tree, centre-based protocol using one tree per group. One of the routers in the tree is called the core. A packet is sent from the source to members of the group following this procedure:

1. The source, which mayor may not be part of the tree, encapsulates the multicast packet inside a unicast packet with the unicast destination address of the core and sends it to the core. This part of delivery is done using a unicast address; the only recipient is the core router.

2. The core decapsulates the unicast packet and forwards it to all interested interfaces .

3. Each router that receives the multicast packet, in tum, forwards it to all interested interfaces.

PIM

Protocol Independent Multicast (PIM) is the name given to two independent multicast routing protocols: Protocol Independent Multicast, Dense Mode (PIM-DM) and Protocol Independent Multicast, Sparse Mode (PIM-SM). Both protocols are unicast protocol-dependent, but the similarity ends here. We discuss each separately.

PIM-DM

PIM-DM is used when there is a possibility that each router is involved in multicasting (dense mode). In this environment, the use of a protocol that broadcasts the packet is justified because almost all routers are involved in the process.

PIM-DM is used in a dense multicast environment, such as a LAN.

PIM-DM uses RPF and pruning and grafting strategies to handle multicasting. However, itis independent of the underlying unicast protocol.

PIM-SM

PIM-SM used when there is a slight possibility that each router is involved in multicasting (sparse mode). In this environment, the use of a protocol that broadcasts the packet is not justified; a protocol such as CBT that uses a group-shared tree is more appropriate.

PIM-SM is used in a sparse multicast environment such as a WAN.

PIM-SM is a group-shared tree routing protocol that has a rendezvous point (RP) as the source of the tree. Its operation is like CBT; however, it is simpler because

it does not require acknowledgment from a join message. In addition, it creates a backup set of RPs for each region to cover RP failures.

One of the characteristics of PIM-SM is that it can switch from a group-shared tree strategy to a source-based tree strategy when necessary. This can happen if there is a dense area of activity far from the RP. That area can be more efficiently handled with a source-based tree strategy instead of a group-shared tree strategy.

PIM-SM is similar to CRT but uses a simpler procedure.