## **Chapter 3**

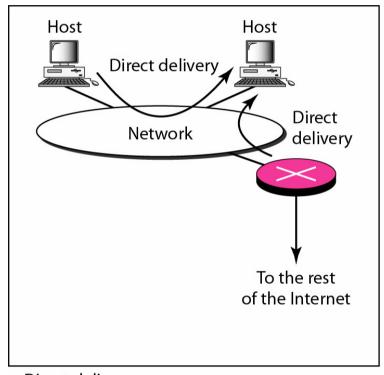
# Delivery, Forwarding, and Routing

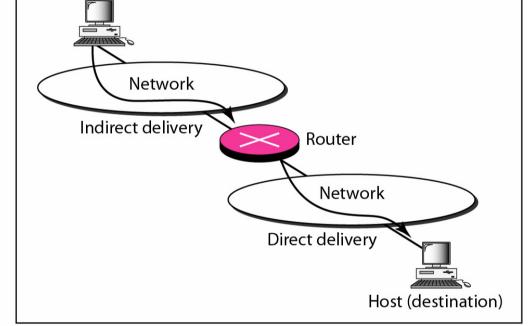
## 3-1 DELIVERY

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

**Topics discussed in this section:**Direct Versus Indirect Delivery

## Figure 3.1 Direct and indirect delivery





a. Direct delivery

b. Indirect and direct delivery

Host (source)

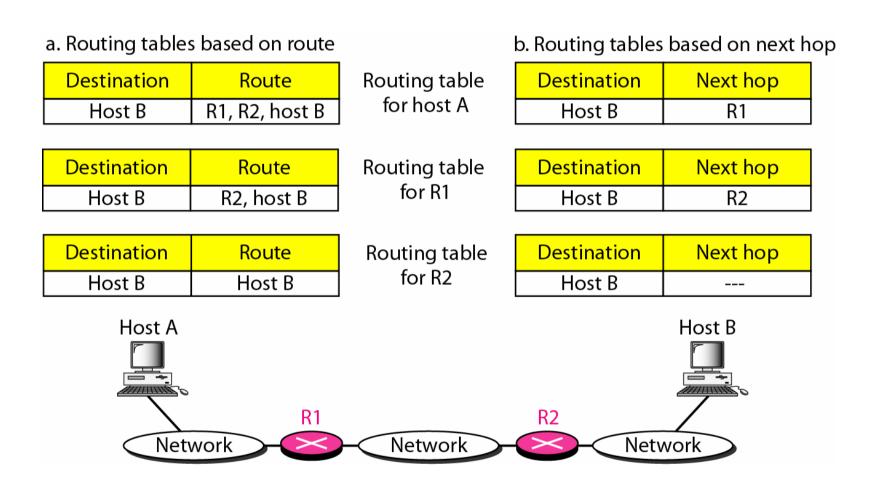
## 3-2 FORWARDING

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.

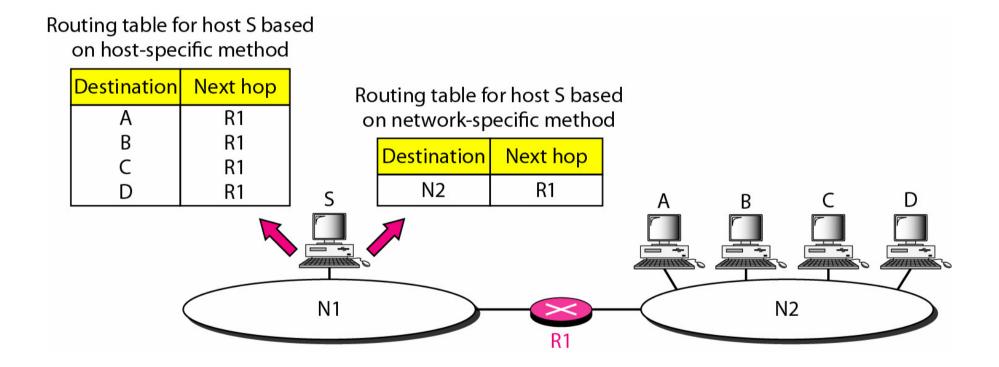
## Topics discussed in this section:

Forwarding Techniques
Forwarding Process
Routing Table

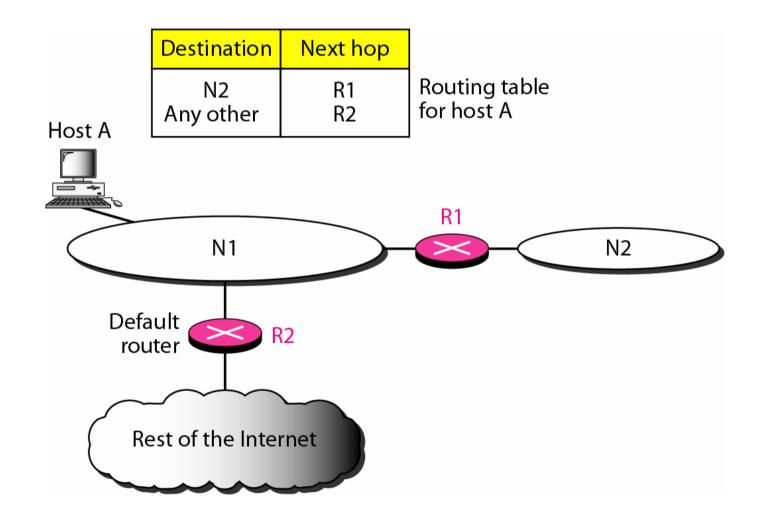
#### Figure 3.2 Route method versus next-hop method



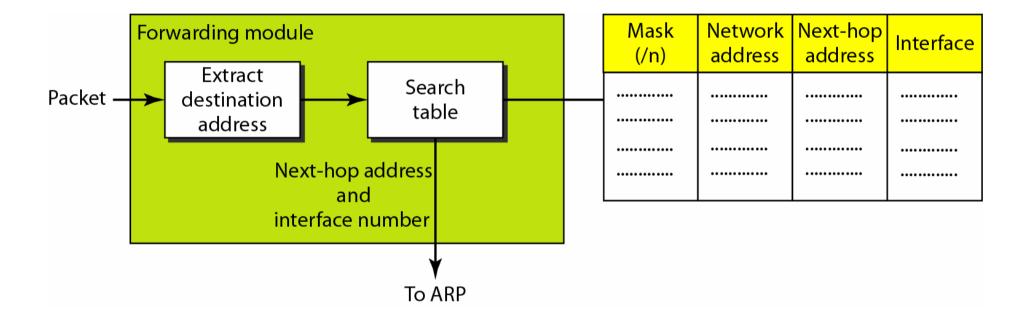
## Figure 3.3 Host-specific versus network-specific method



## Figure 3.4 Default method



### Figure 3.5 Simplified forwarding module in classless address





Note

In classless addressing, we need at least four columns in a routing table.

## Example 3.1

Make a routing table for router R1, using the configuration in Figure 3.6.

#### Solution

Table 3.1 shows the corresponding table.

## Figure 3.6 Configuration for Example 22.1

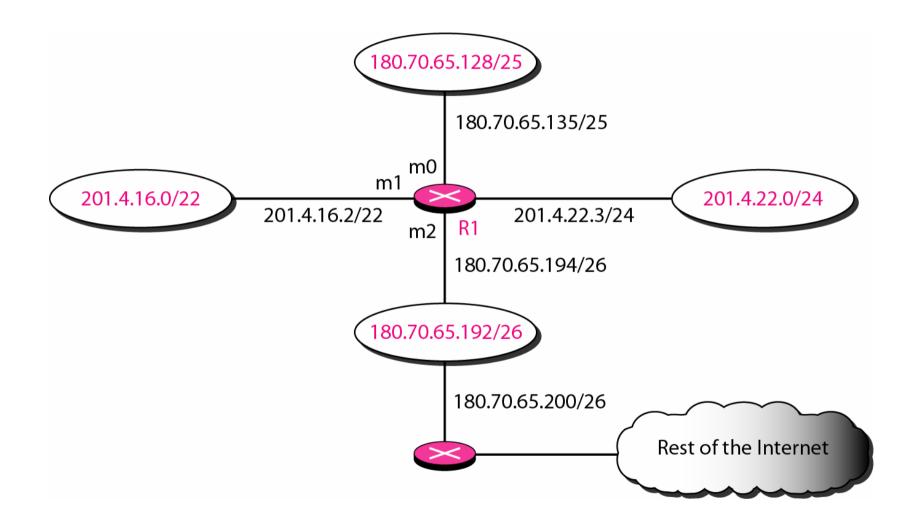


 Table 3.1 Routing table for router R1 in Figure 22.6

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



Show the forwarding process if a packet arrives at R1 in Figure 3.6 with the destination address 180.70.65.140.

### **Solution**

The router performs the following steps:

- 1. The first mask (/26) is applied to the destination address. The result is 180.70.65.128, which does not match the corresponding network address.
- 2. The second mask (/25) is applied to the destination address. The result is 180.70.65.128, which matches the corresponding network address. The next-hop address and the interface number m0 are passed to ARP for further processing.

## Example 3.3

Show the forwarding process if a packet arrives at R1 in Figure 3.6 with the destination address 201.4.22.35.

#### Solution

The router performs the following steps:

- 1. The first mask (/26) is applied to the destination address. The result is 201.4.22.0, which does not match the corresponding network address.
- 2. The second mask (/25) is applied to the destination address. The result is 201.4.22.0, which does not match the corresponding network address (row 2).



## Example 3.3 (continued)

3. The third mask (/24) is applied to the destination address. The result is 201.4.22.0, which matches the corresponding network address. The destination address of the packet and the interface number m3 are passed to ARP.

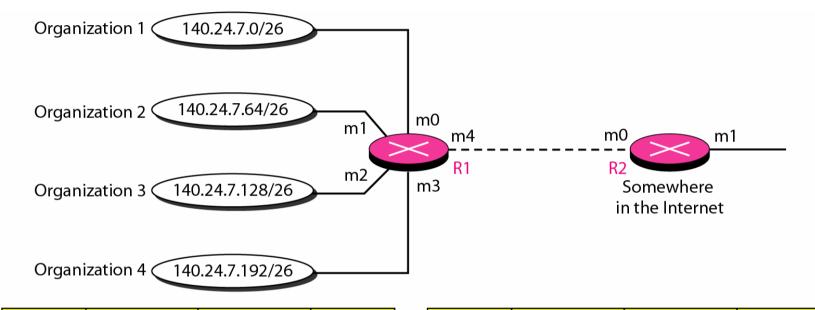
## Example 3.4

Show the forwarding process if a packet arrives at R1 in Figure 3.6 with the destination address 18.24.32.78.

#### **Solution**

This time all masks are applied, one by one, to the destination address, but no matching network address is found. When it reaches the end of the table, the module gives the next-hop address 180.70.65.200 and interface number m2 to ARP. This is probably an outgoing package that needs to be sent, via the default router, to someplace else in the Internet.

### Figure 3.7 Address aggregation



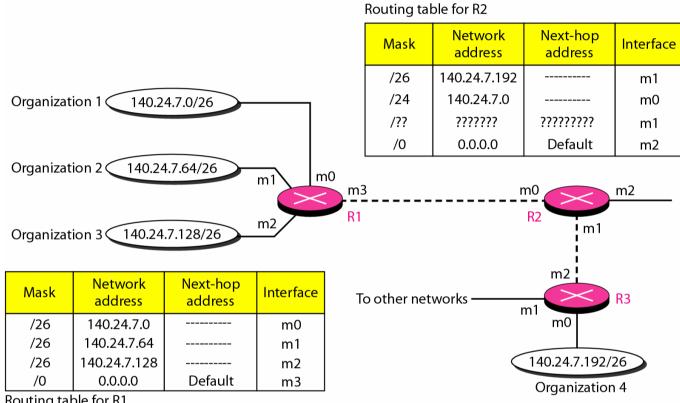
Mask	Network address	Next-hop address	Interface
/26	140.24.7.0		m0
/26	140.24.7.64		m1
/26	140.24.7.128		m2
/26	140.24.7.192		m3
/0	0.0.0.0	Default	m4

Mask	Network address	Next-hop address	Interface	
/24	140.24.7.0		m0	
/0	0.0.0.0	Default	m1	

Routing table for R2

Routing table for R1

## Figure 3.8 Longest mask matching



Routing	table	for	R1
---------	-------	-----	----

Mask	Network address	Next-hop address	Interface
/26	140.24.7.192		m0
/??	???????	????????	m1
/0	0.0.0.0	Default	m2

Routing table for R3



As an example of hierarchical routing, let us consider Figure 3.9. A regional ISP is granted 16,384 addresses starting from 120.14.64.0. The regional ISP has decided to divide this block into four subblocks, each with 4096 addresses. Three of these subblocks are assigned to three local ISPs; the second subblock is reserved for future use. Note that the mask for each block is /20 because the original block with mask /18 is divided into 4 blocks.

The first local ISP has divided its assigned subblock into 8 smaller blocks and assigned each to a small ISP. Each small ISP provides services to 128 households, each using four addresses.



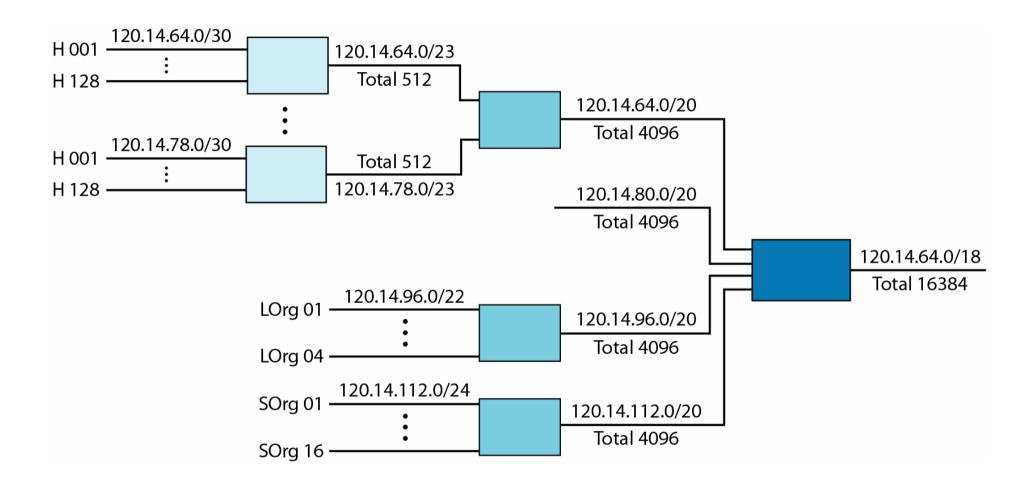
## Example 3.5 (continued)

The second local ISP has divided its block into 4 blocks and has assigned the addresses to four large organizations.

The third local ISP has divided its block into 16 blocks and assigned each block to a small organization. Each small organization has 256 addresses, and the mask is /24.

There is a sense of hierarchy in this configuration. All routers in the Internet send a packet with destination address 120.14.64.0 to 120.14.127.255 to the regional ISP.

### Figure 3.9 Hierarchical routing with ISPs



## Figure 3.10 Common fields in a routing table

Mask	Network address	Next-hop address	Interface	Flags	Reference count	Use
					••••••	

## Example 3.6

One utility that can be used to find the contents of a routing table for a host or router is netstat in UNIX or LINUX. The next slide shows the list of the contents of a default server. We have used two options, r and n. The option r indicates that we are interested in the routing table, and the option n indicates that we are looking for numeric addresses. Note that this is a routing table for a host, not a router. Although we discussed the routing table for a router throughout the chapter, a host also needs a routing table.



## Example 3.6 (continued)

\$ netstat -rn						
Kernel IP routing table						
Destination	Gateway	Mask	Flags	Iface		
153.18.16.0	0.0.0.0	255.255.240.0	U	eth0		
127.0.0.0	0.0.0.0	255.0.0.0	U	lo		
0.0.0.0	153.18.31.254	0.0.0.0	UG	eth0		

The destination column here defines the network address. The term gateway used by UNIX is synonymous with router. This column actually defines the address of the next hop. The value 0.0.0.0 shows that the delivery is direct. The last entry has a flag of G, which means that the destination can be reached through a router (default router). The Iface defines the interface.

# Example 3.6 (continued)

More information about the IP address and physical address of the server can be found by using the ifconfig command on the given interface (eth0).

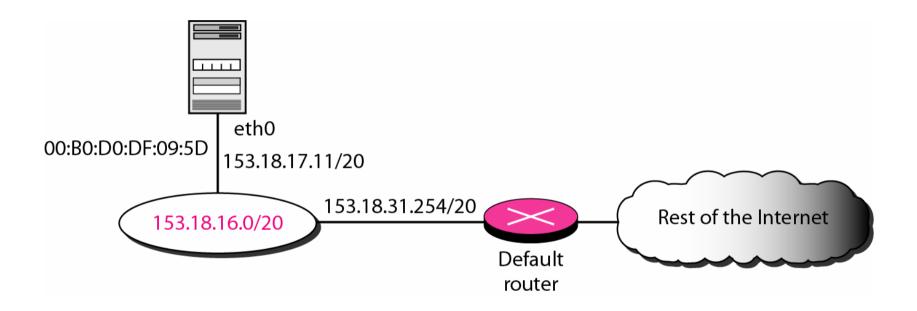
#### \$ ifconfig eth0

eth0 Link encap:Ethernet HWaddr 00:B0:D0:DF:09:5D

inet addr:153.18.17.11 Bcast:153.18.31.255 Mask:255.255.240.0

. . .

## Figure 3.11 Configuration of the server for Example 3.6



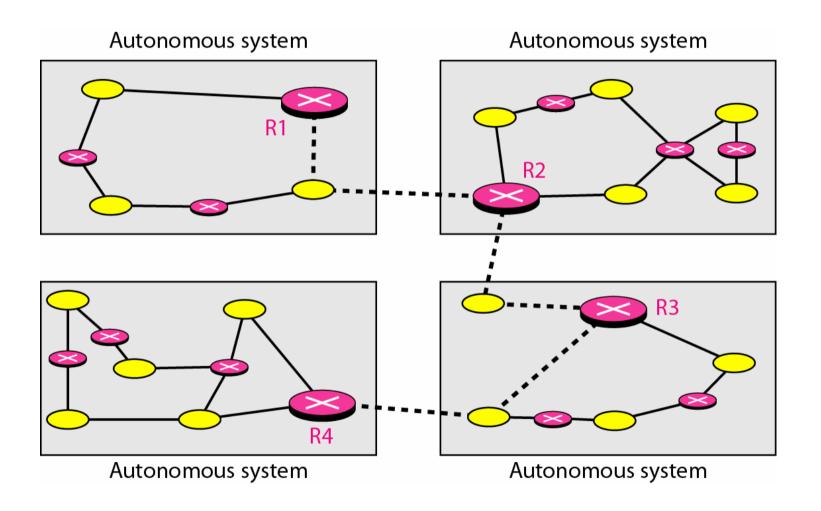
## 3-3 UNICAST ROUTING PROTOCOLS

A routing table can be either static or dynamic. A static table is one with manual entries. A dynamic table is one that is updated automatically when there is a change somewhere in the Internet. A routing protocol is a combination of rules and procedures that lets routers in the Internet inform each other of changes.

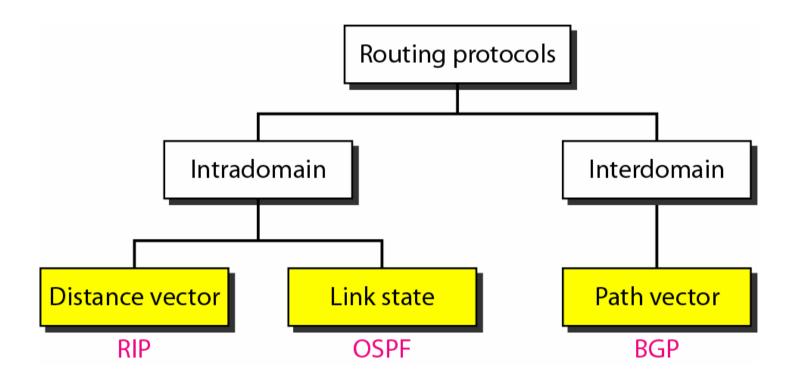
## Topics discussed in this section:

Optimization
Intra- and Interdomain Routing
Distance Vector Routing and RIP
Link State Routing and OSPF
Path Vector Routing and BGP

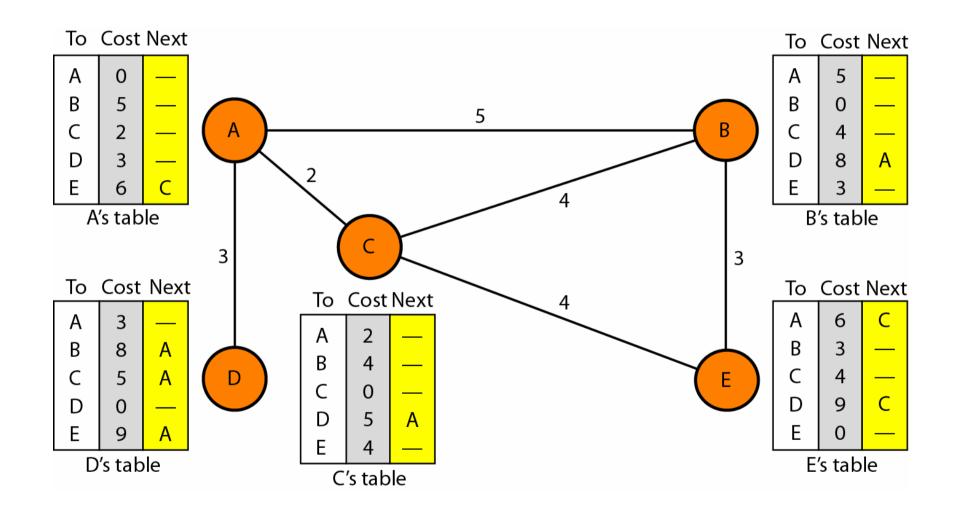
## Figure 3.12 Autonomous systems



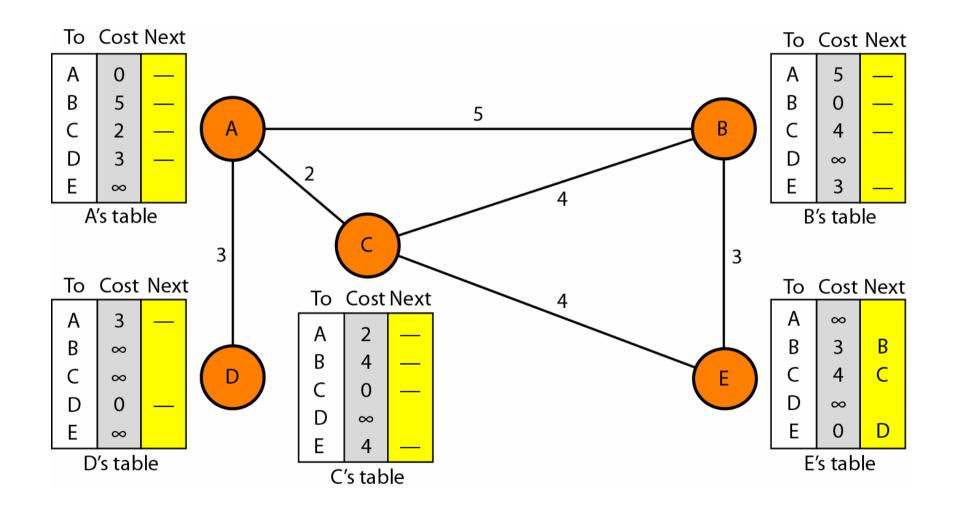
## Figure 3.13 Popular routing protocols



### Figure 3.14 Distance vector routing tables



## Figure 3.15 Initialization of tables in distance vector routing

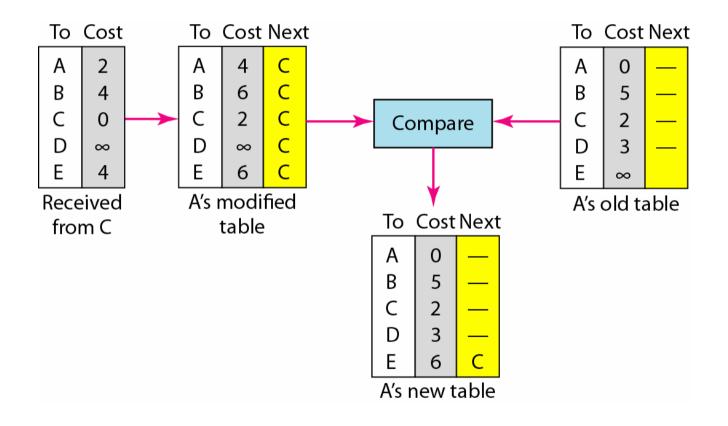




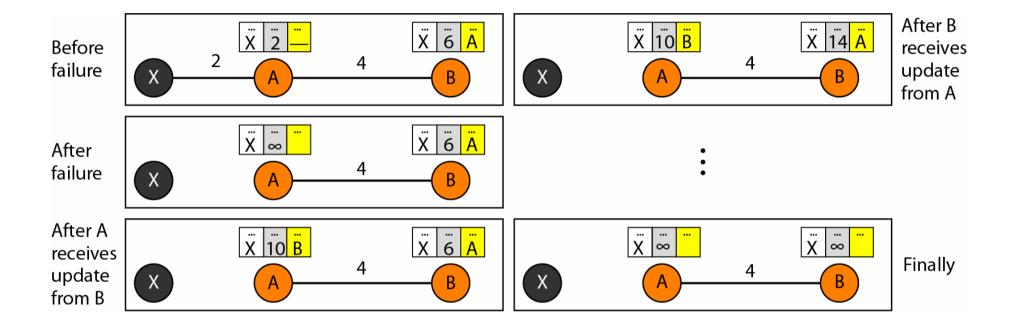
## Note

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

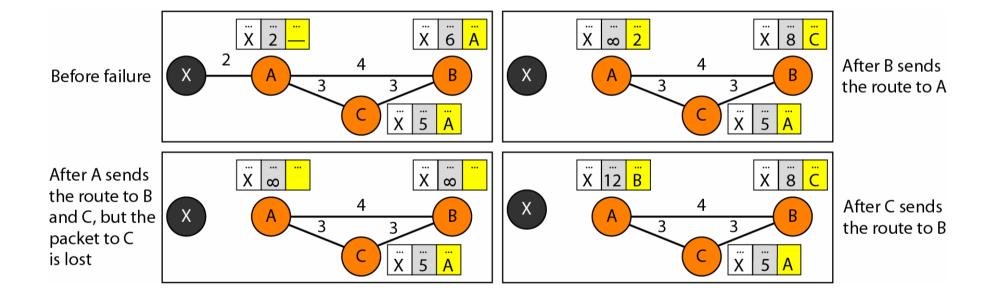
## Figure 3.16 Updating in distance vector routing



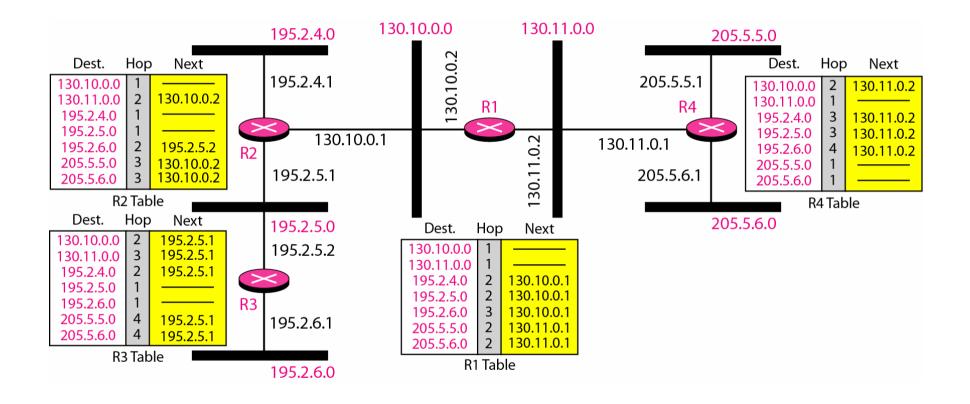
## Figure 3.17 Two-node instability



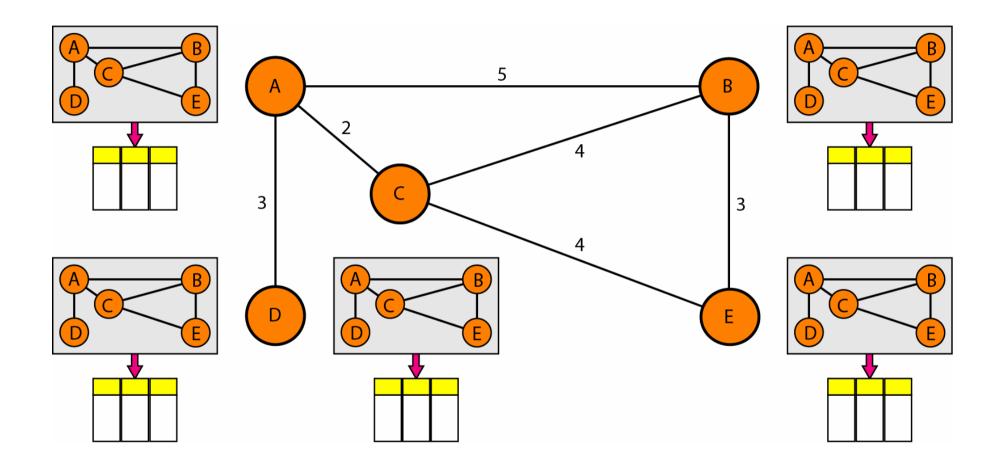
## Figure 3.18 Three-node instability



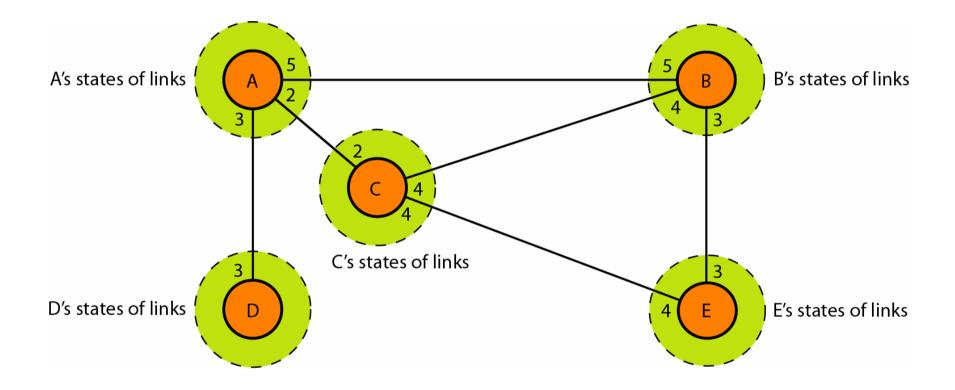
### Figure 3.19 Example of a domain using RIP



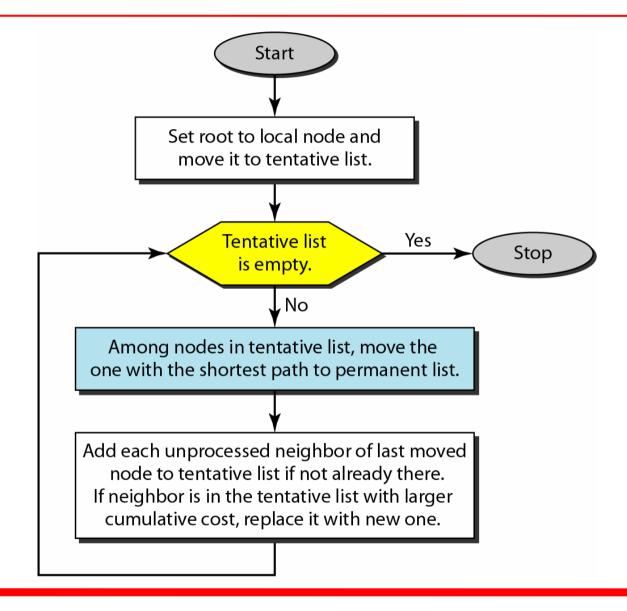
## Figure 3.20 Concept of link state routing



## Figure 3.21 Link state knowledge



#### Figure 3.22 Dijkstra algorithm



## Figure 3.23 Example of formation of shortest path tree

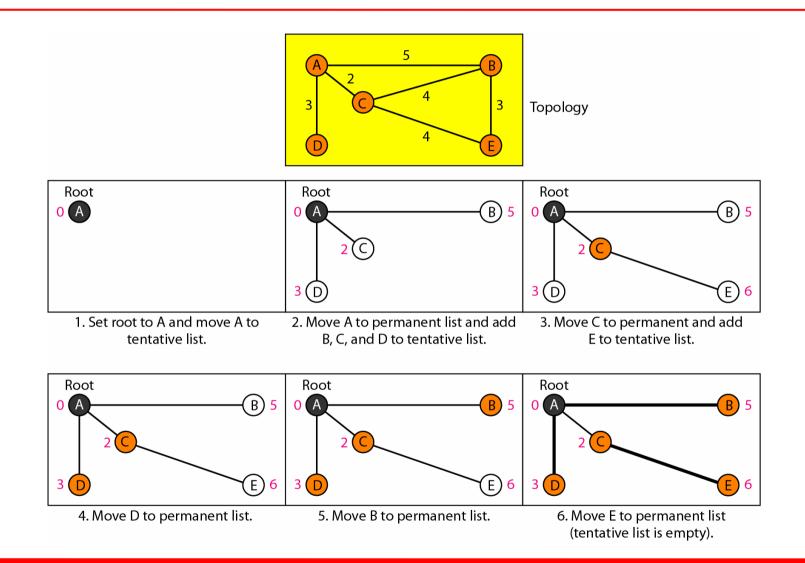
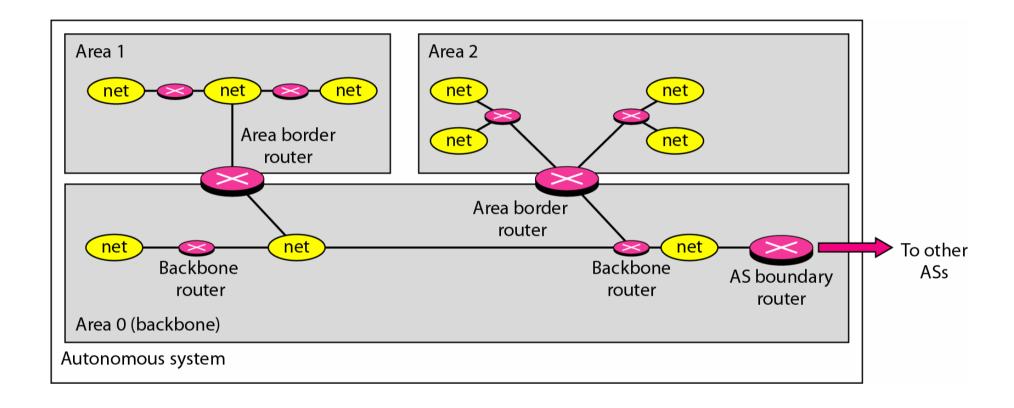


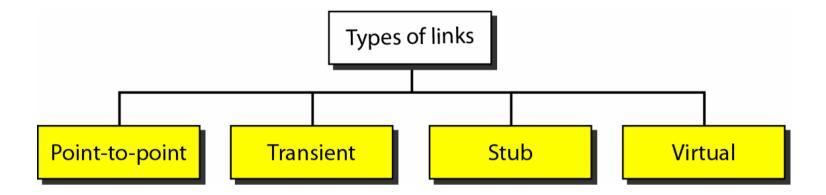
 Table 3.2
 Routing table for node A

Node	Cost	Next Router
A	0	
В	5	_
С	2	_
D	3	_
Е	6	С

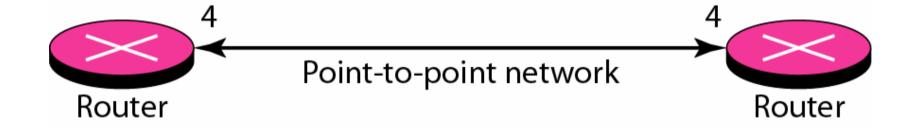
#### Figure 3.24 Areas in an autonomous system



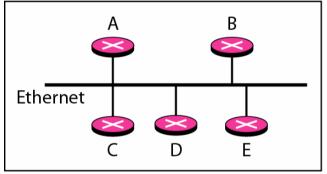
# Figure 3.25 Types of links



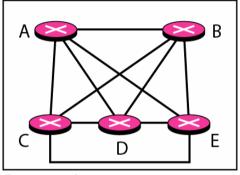
## Figure 3.26 Point-to-point link



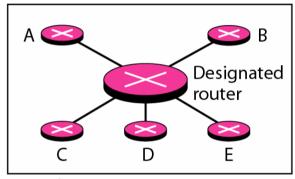
#### Figure 3.27 Transient link



a. Transient network

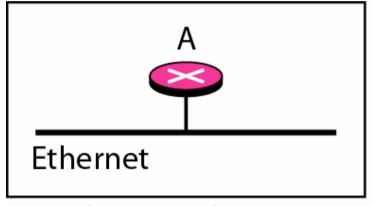


b. Unrealistic representation

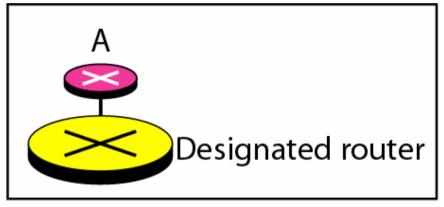


c. Realistic representation

## Figure 3.28 Stub link

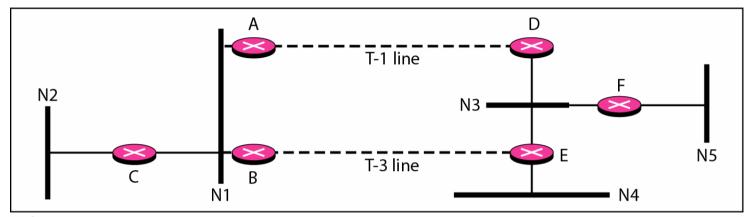


a. Stub network

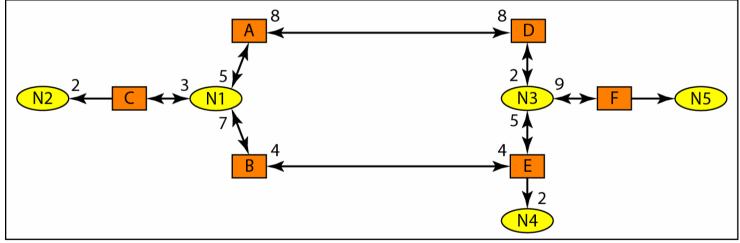


b. Representation

#### Figure 3.29 Example of an AS and its graphical representation in OSPF

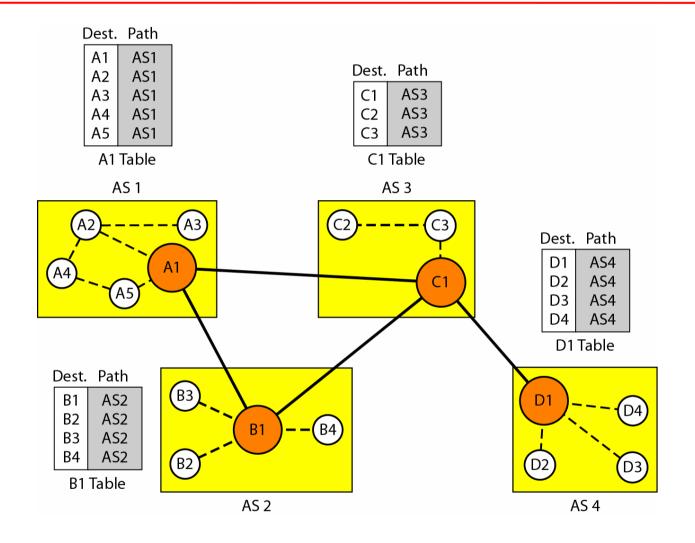


a. Autonomous system



b. Graphical representation

#### Figure 3.30 Initial routing tables in path vector routing



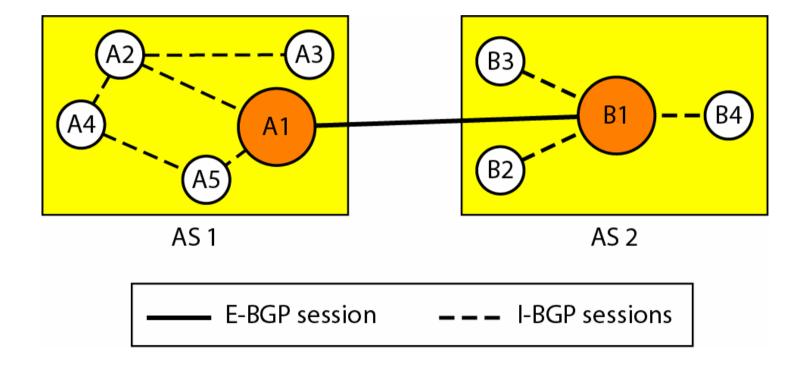
## Figure 3.31 Stabilized tables for three autonomous systems

Dest.	Path	_	Dest.	Path	_	Dest.	
A1	AS1		A1	AS2-AS1		A1	Α
A5	AS1		A5	AS2-AS1		A5	Α
B1  B4	AS1-AS2  AS1-AS2		B1  B4	AS2  AS2		B1  B4	A 
C1  C3	AS1-AS3  AS1-AS3		C1  C3	AS2-AS3  AS2-AS3		C1  C3	A 
D1  D4	AS1-AS2-AS4  AS1-AS2-AS4		D1  D4	AS2-AS3-AS4  AS2-AS3-AS4		D1  D4	A
	A1 Table			B1 Table			(

Dest.	Path
A1	AS3-AS1
A5	AS3-AS1
B1	AS3-AS2
B4	AS3-AS2
C1	AS3
C3	AS3
D1	AS3-AS4
D4	AS3-AS4
	C1 Table

Dest.	Path
A1	AS4-AS3-AS1
A5	AS4-AS3-AS1
B1	AS4-AS3-AS2
B4	AS4-AS3-AS2
C1	AS4-AS3
С3	AS4-AS3
D1	AS4
D4	 AS4
D4	A34
	D1 Table

#### Figure 3.32 Internal and external BGP sessions



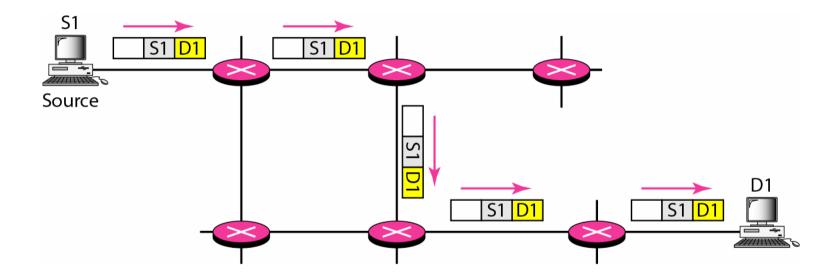
## 3-4 MULTICAST ROUTING PROTOCOLS

In this section, we discuss multicasting and multicast routing protocols.

## Topics discussed in this section:

Unicast, Multicast, and Broadcast Applications Multicast Routing Routing Protocols

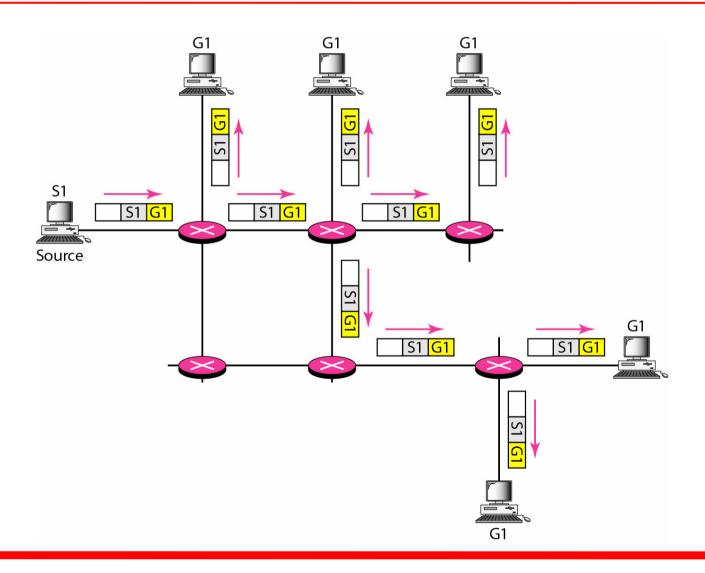
## Figure 3.33 Unicasting





In unicasting, the router forwards the received packet through only one of its interfaces.

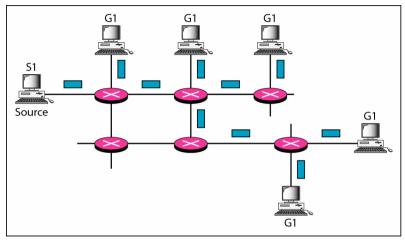
## Figure 3.34 Multicasting



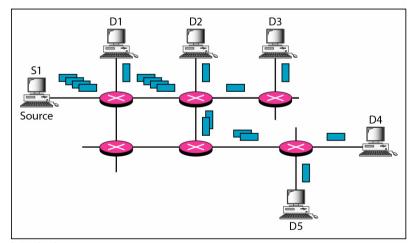


In multicasting, the router may forward the received packet through several of its interfaces.

## Figure 3.35 Multicasting versus multiple unicasting



a. Multicasting



b. Multiple unicasting

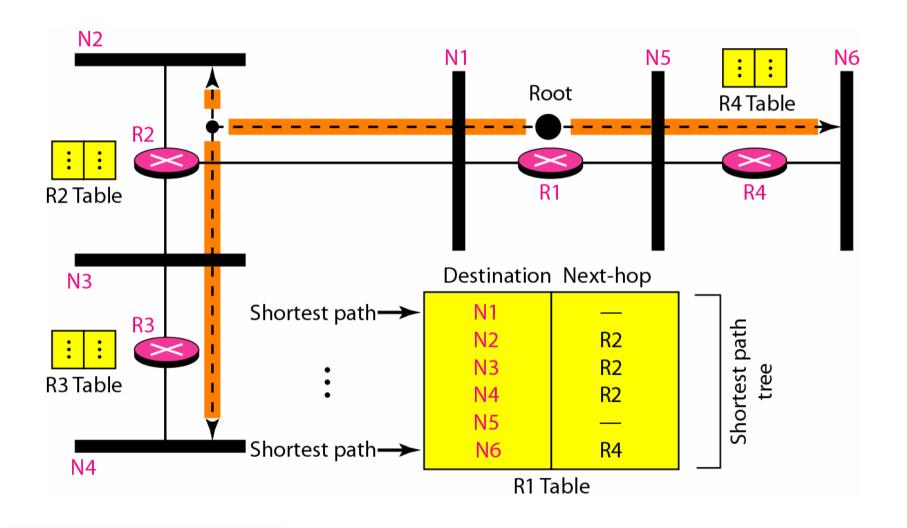


Emulation of multicasting through multiple unicasting is not efficient and may create long delays, particularly with a large group.



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

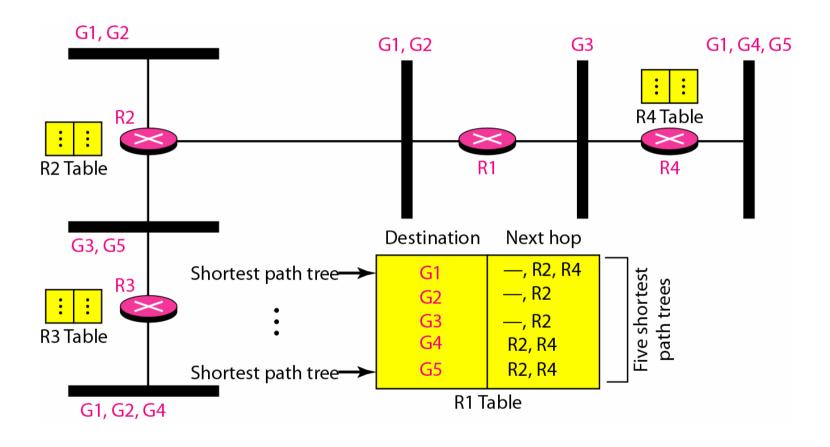
#### Figure 3.36 Shortest path tree in unicast routing





In multicast routing, each involved router needs to construct a shortest path tree for each group.

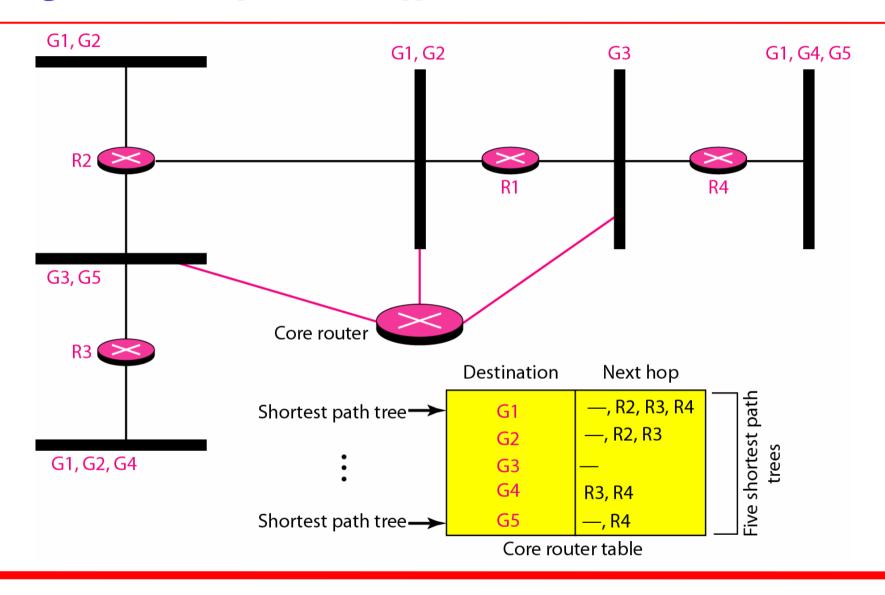
#### Figure 3.37 Source-based tree approach





In the source-based tree approach, each router needs to have one shortest path tree for each group.

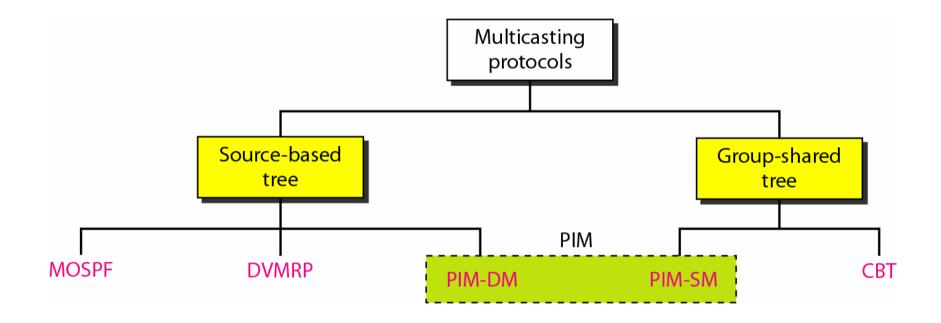
#### Figure 3.38 Group-shared tree approach





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

#### Figure 3.39 Taxonomy of common multicast protocols





# Multicast link state routing uses the source-based tree approach.

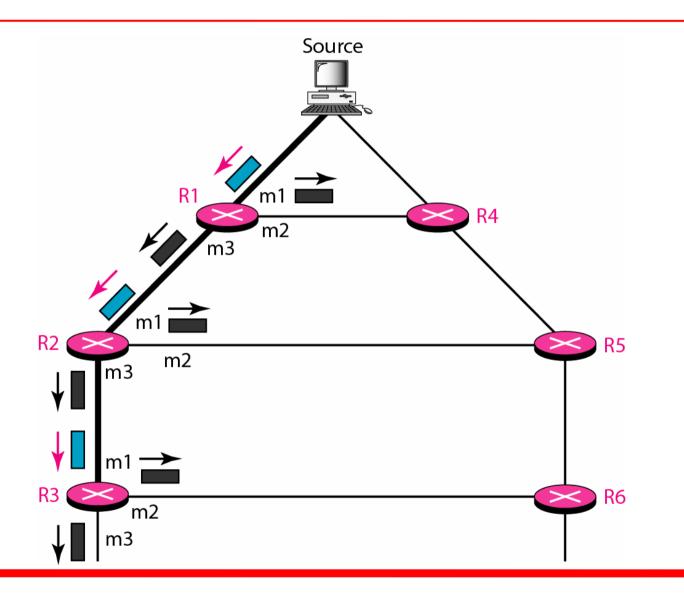


# Flooding broadcasts packets, but creates loops in the systems.

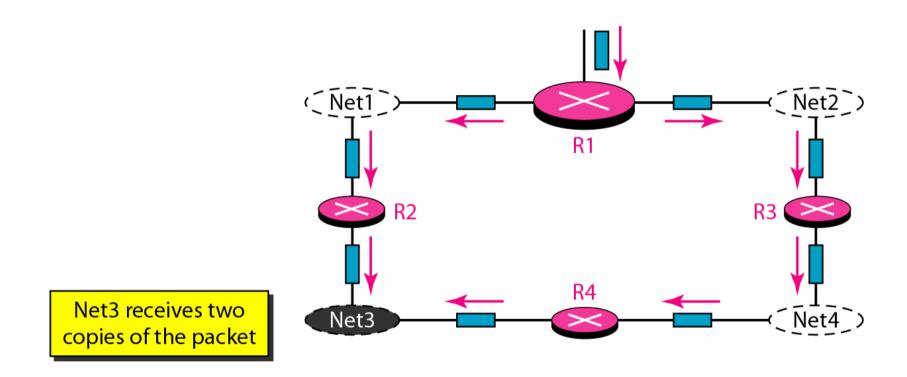


# RPF eliminates the loop in the flooding process.

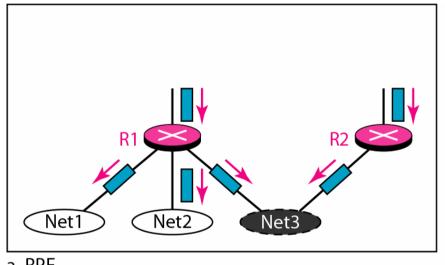
## Figure 3.40 Reverse path forwarding (RPF)

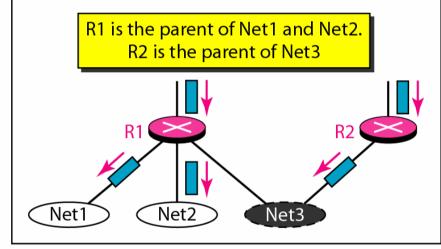


## Figure 3.41 Problem with RPF



## Figure 3.42 RPF Versus RPB





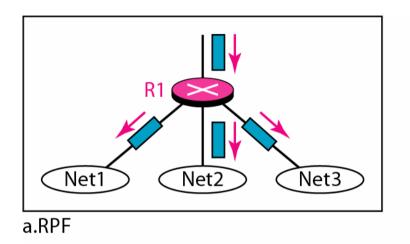
a. RPF

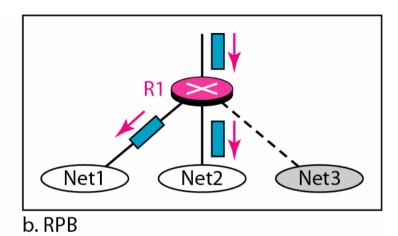
b. RPB

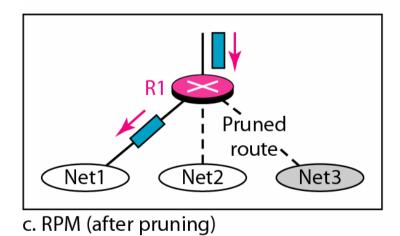


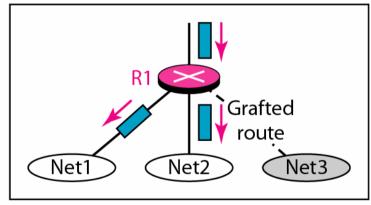
RPB creates a shortest path broadcast tree from the source to each destination. It guarantees that each destination receives one and only one copy of the packet.

#### Figure 3.43 RPF, RPB, and RPM









d. RPM (after grafting)



RPM adds pruning and grafting to RPB to create a multicast shortest path tree that supports dynamic membership changes.

#### Figure 3.44 Group-shared tree with rendezvous router

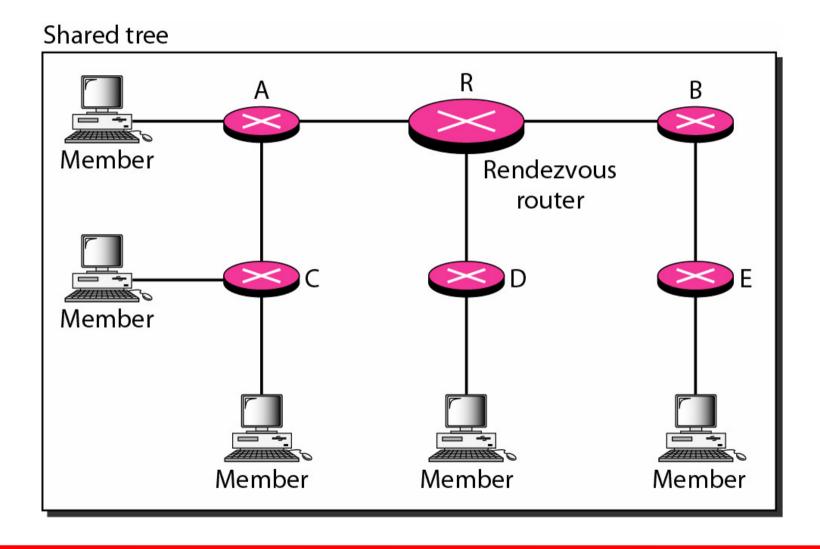
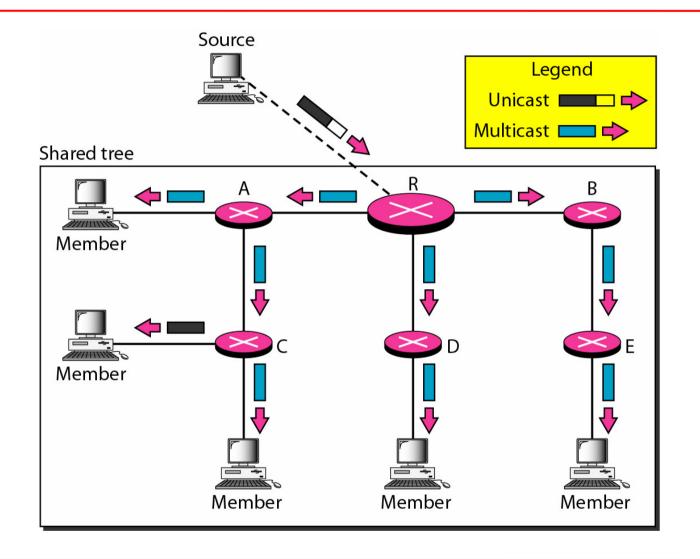


Figure 3.45 Sending a multicast packet to the rendezvous router





In CBT, the source sends the multicast packet (encapsulated in a unicast packet) to the core router. The core router decapsulates the packet and forwards it to all interested interfaces.



# 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, it is independent of the underlying unicast protocol.



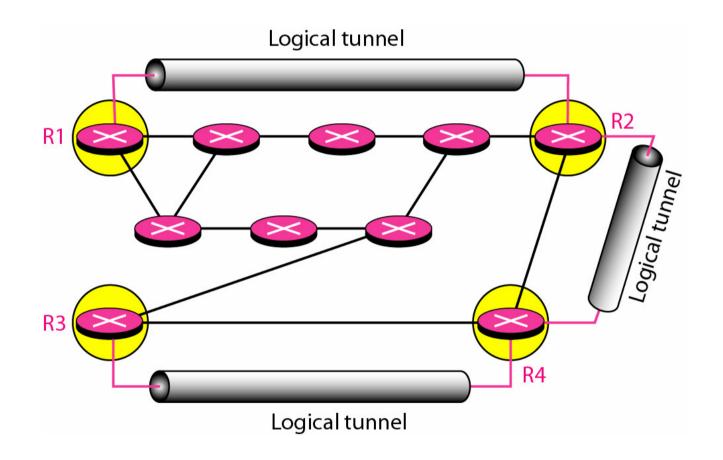
# PIM-SM is used in a sparse multicast environment such as a WAN.





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

## Figure 3.46 Logical tunneling



## Figure 3.47 MBONE

