

Module IV

Network Layer:

Delivery, Forwarding, and Routing

22-1 DELIVERY

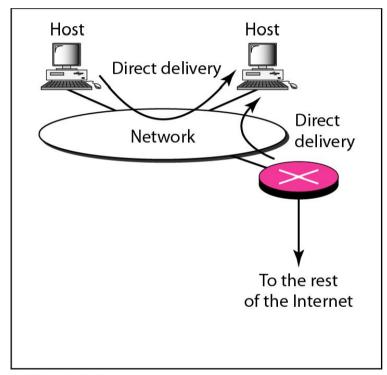
The network layer supervises the handling of the packets by the underlying physical networks. We define this handling as the delivery of a packet..

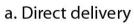
Topics discussed in this section:

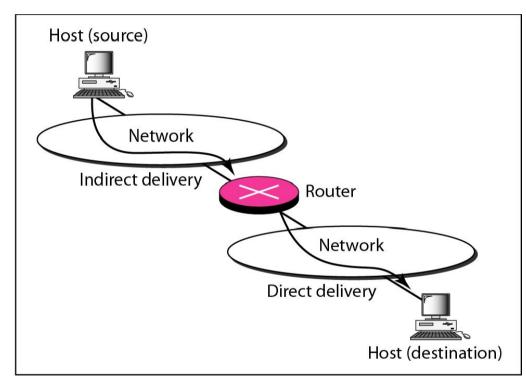
Direct Versus Indirect Delivery

Figure 22.1 Direct and indirect

delivery







b. Indirect and direct delivery

22-2 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 22.2 Route method versus next-hop

method

a. Routing tables	s based on route		b. Routing tables	based on next hop		
Destination	Route	Routing table	Destination	Next hop		
Host B	R1, R2, host B	for host A	Host B	R1		
Destination	Route	Routing table	Destination	Next hop		
Host B	R2, host B	for R1	Host B	R2		
Destination	Route	Routing table	Destination	Next hop		
Host B	Host B	for R2	Host B			
Host A				Host B		
	R1		R2			
Network Network						

Figure 22.3 Host-specific versus network-specific method

Routing table for host S based on host-specific method

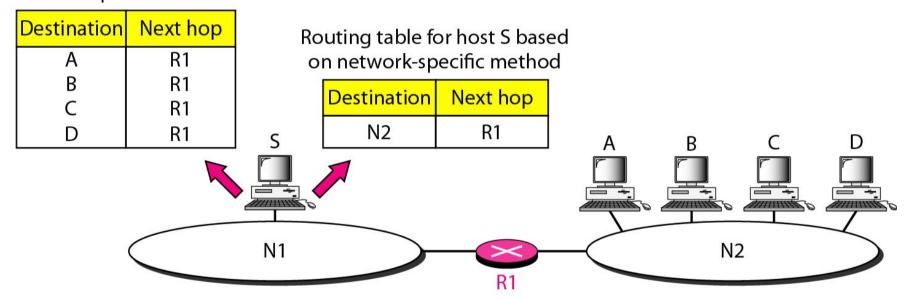


Figure 22.4 Default

method

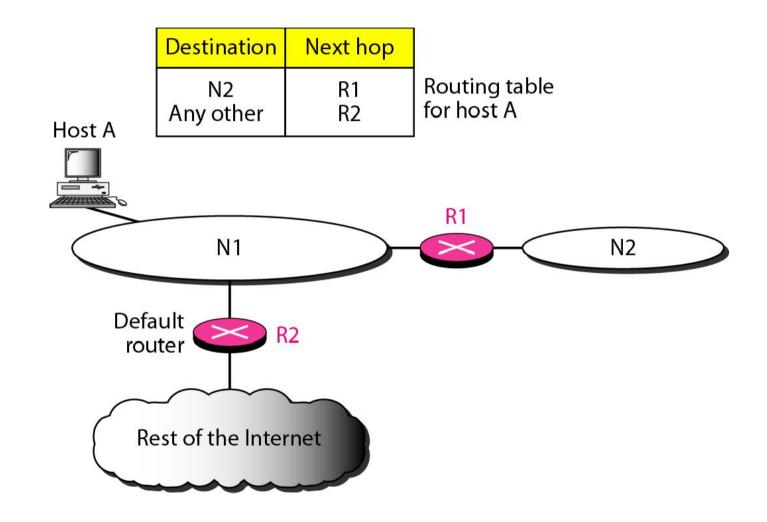
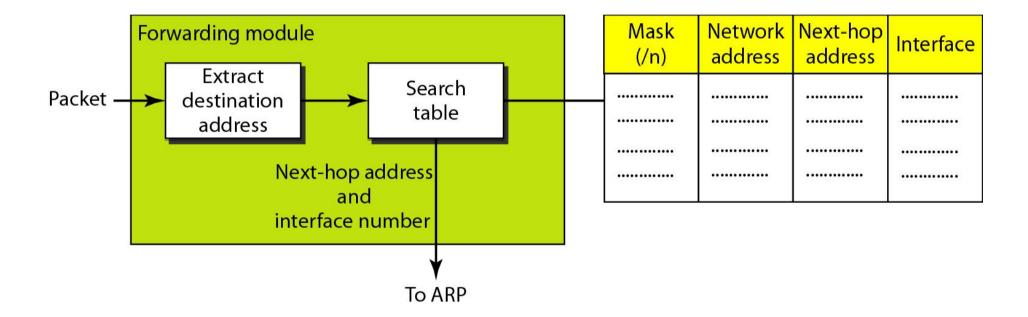


Figure 22.5 Simplified forwarding module in classless address





Note

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

table.



Make a routing table forrouterR1, using the configuration in Figure 22.6.

Solution

Table 22.1 shows the corresponding table.

Figure 22.6 Configuration for Example 22.1

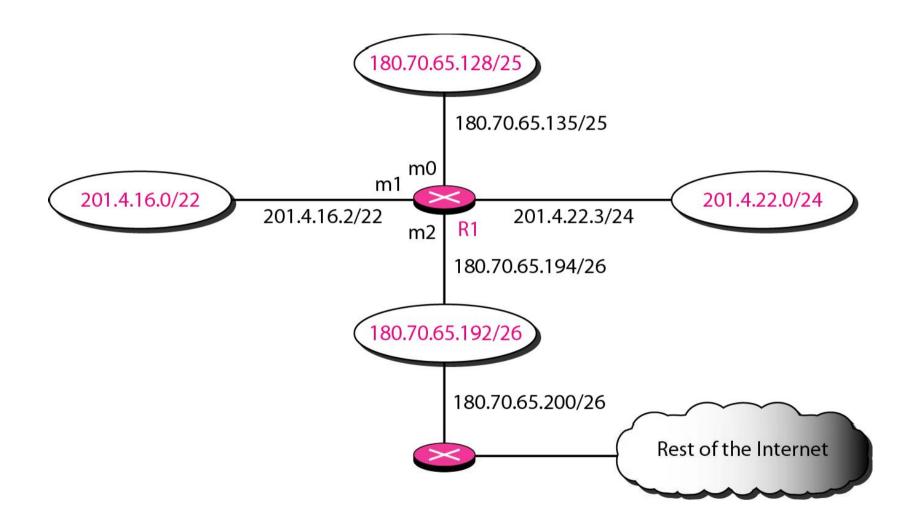


Table 22.1 Routing table for router R1 in Figure 22.6

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



Show the forwarding process if a packet arrives at R1 in Figure 22.6 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.



Show the forwarding process if a packet arrives at R1 in Figure 22.6 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 22.14 address (row 2).



Example 22.3 (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.



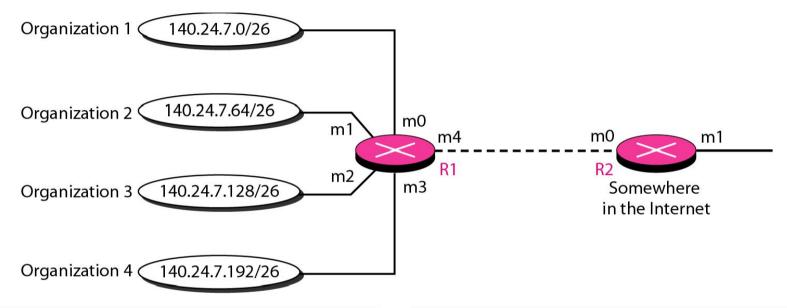
Show the forwarding process if a packet arrives at R1 in Figure 22.6 with the destination address 18.24.32.78.

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 22.7 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	

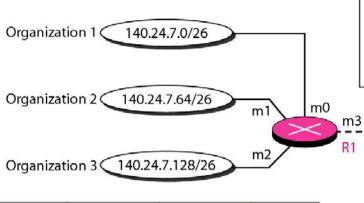
Mask	Network address	Next-hop address	Interface
/24	140.24.7.0		m0
/0	0.0.0.0	Default	m1

Routing table for R2

Routing table for R1

Figure 22.8 Longest mask

matching



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
/0	0.0.0.0	Default	m3

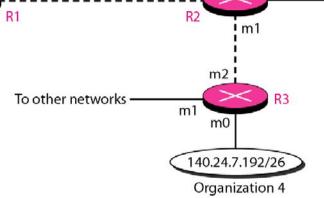
Routing table for R1

Routing table for R2

Mask	Network address	Next-hop address	Interface	
/26	140.24.7.192		m1	
/24	140.24.7.0		m0	
/??	???????	?????????	m1	
/0	0.0.0.0	Default	m2	

m0

m2



Mask	Network address	Next-hop address	Interface
/26	140.24.7.192	h 	m0
/??	???????	777777777	m1
/0	0.0.0.0	Default	m2

Routing table for R3

Example 22.5

an example of hierarchical routing, us consider Figure 22.9. A regional ISP is granted 16,384 addresses starting from 120.14.64.0. The regional ISP has decided to divide this block 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 22.5 (continued)

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

The third local ISP has divided its block into 16 bhooksassigned each block to a small organization. Each small organization has 256 addresses, and themask 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 22.9 Hierarchical routing with ISPs

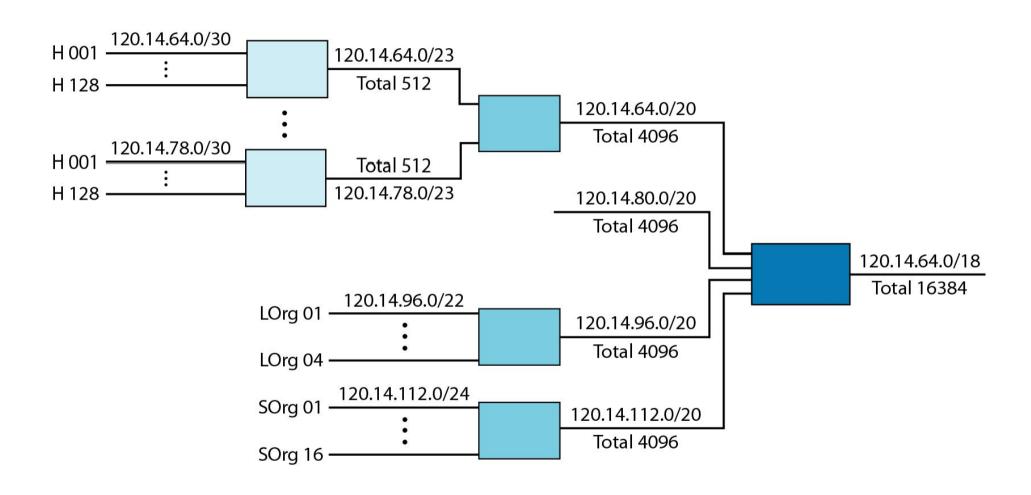


Figure 22.10 Common fields in a routing table

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



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 22.6 (continued)

\$ netstat -rn							
Kernel IP routing	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 22.6 (continued)

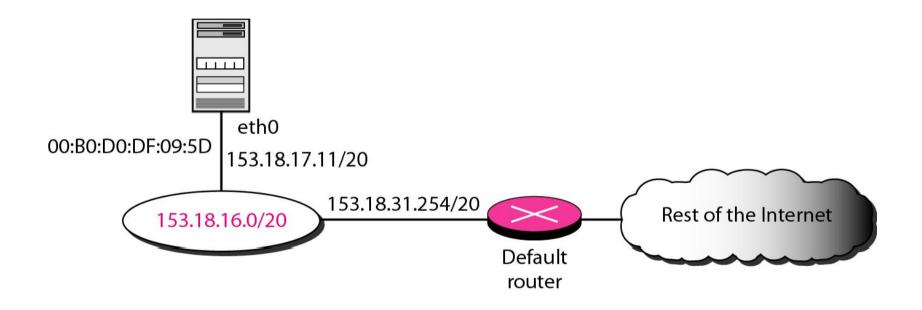
More information about the IP address and physical address of the server can be found by using the ifconfig command on the given interface (eth0).

\$ 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 22.11 Configuration of the server for Example 22.6



22-3 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 22.12 Autonomous

systems

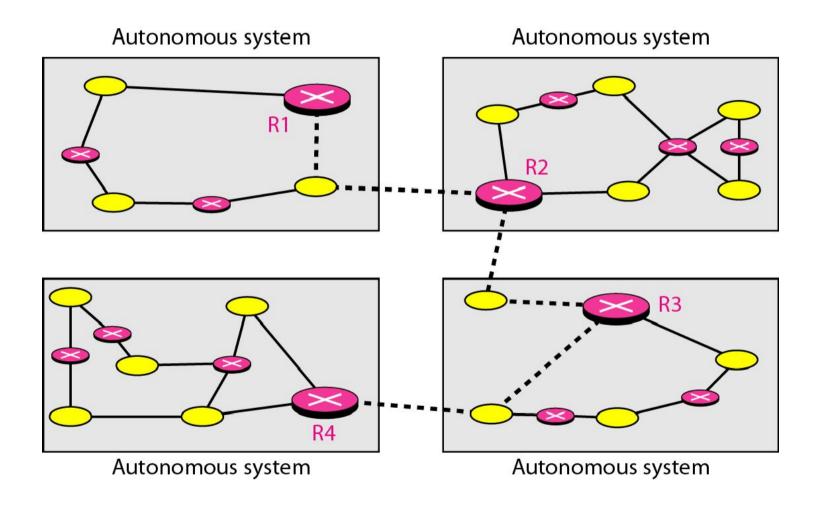


Figure 22.13 Popular routing

protocols

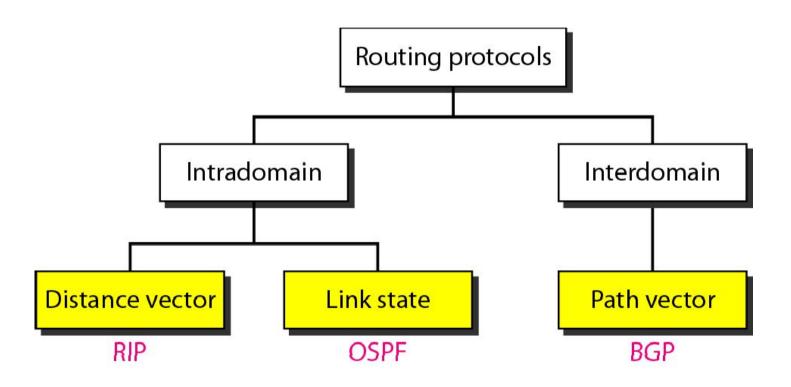


Figure 22.14 Distance vector routing

tables

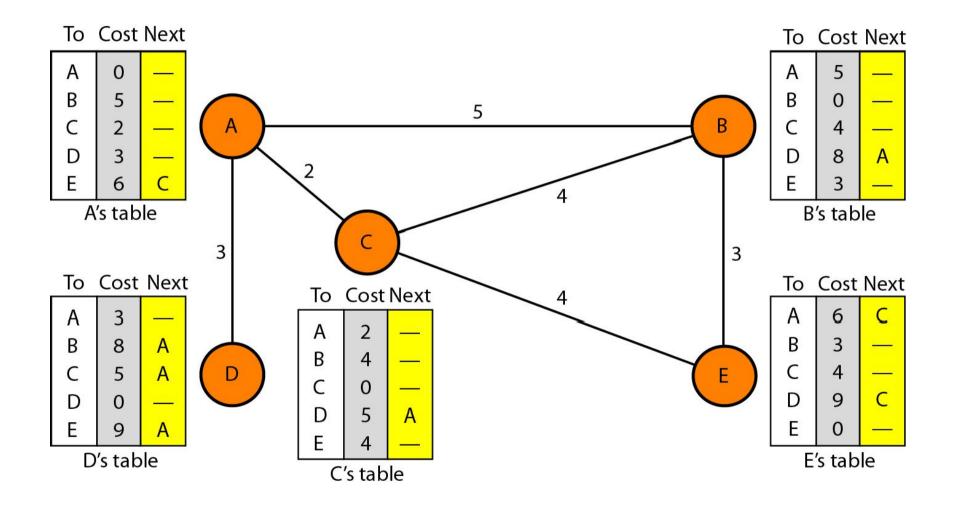
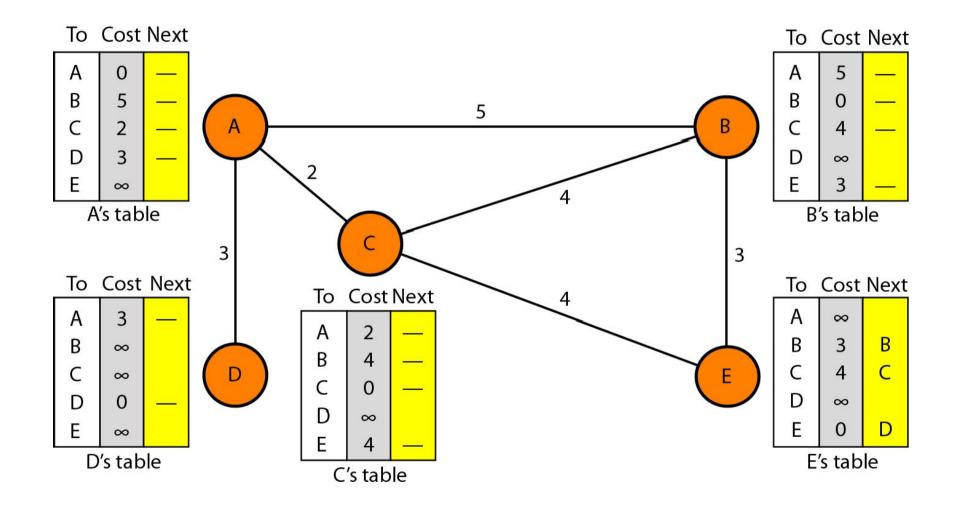


Figure 22.15 Initialization of tables in distance vector routing





Note

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

Figure 22.16 Updating in distance vector routing

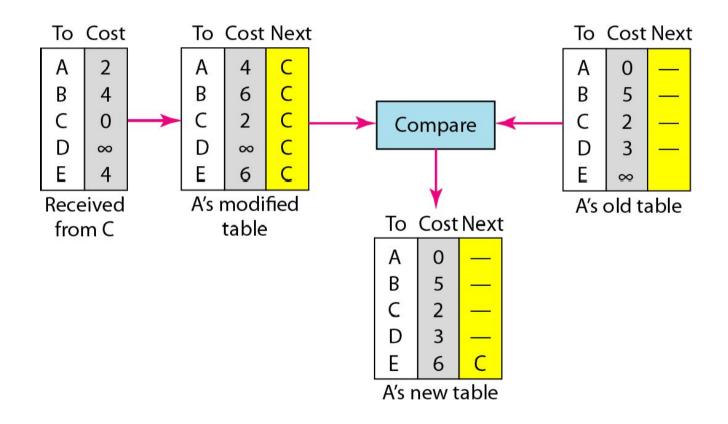


Figure 22.17 Two-node

instability

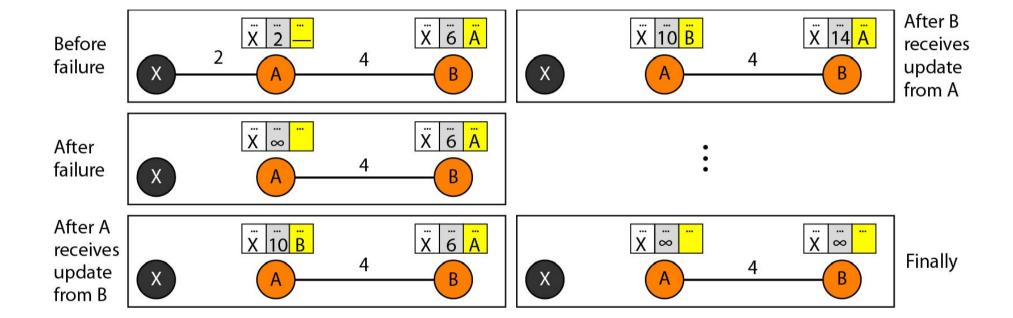


Figure 22.18 Three-node

instability

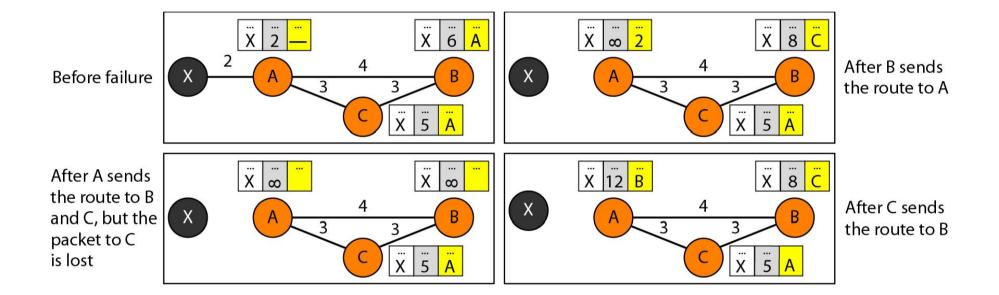


Figure 22.19 Example of a domain using RIP

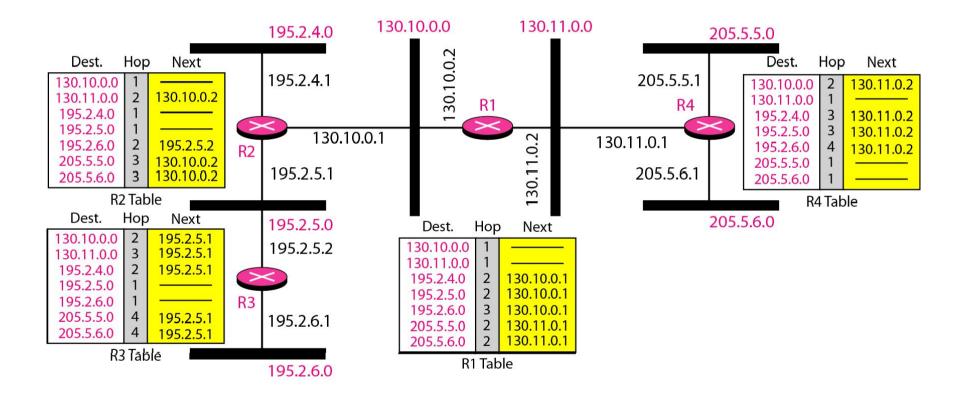


Figure 22.20 Concept of link state

routing

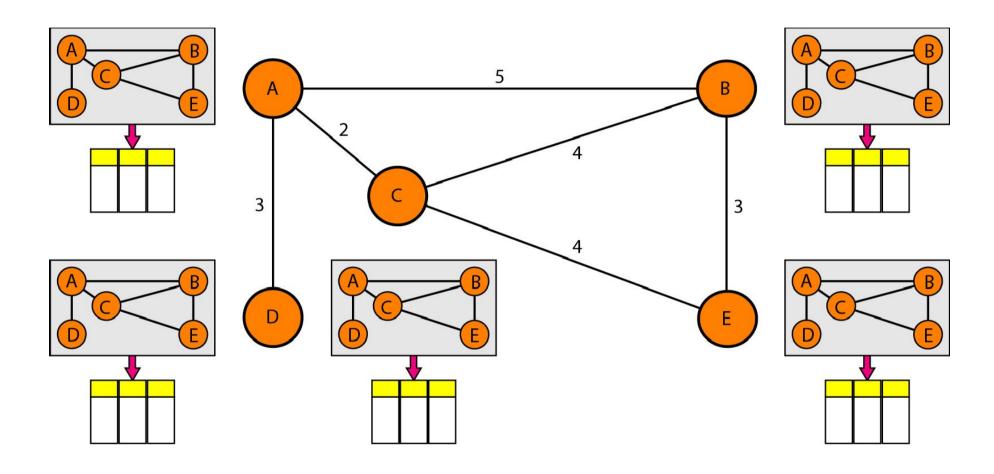


Figure 22.21 Link state

knowledge

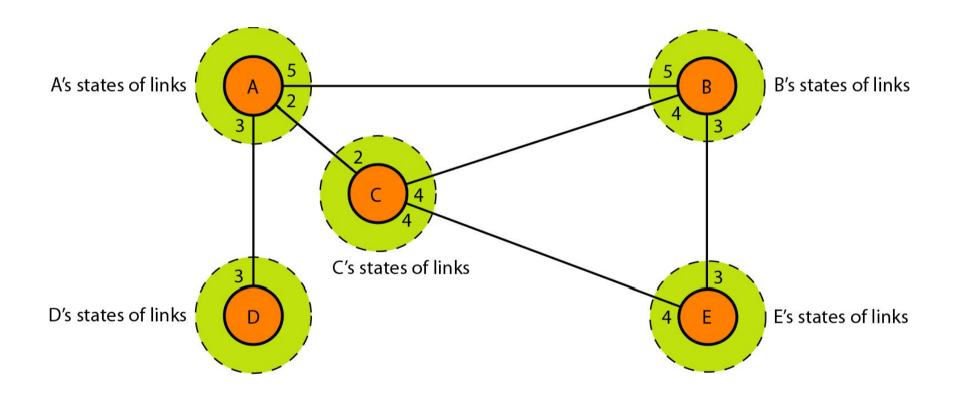


Figure 22.22 Dijkstra

algorithm

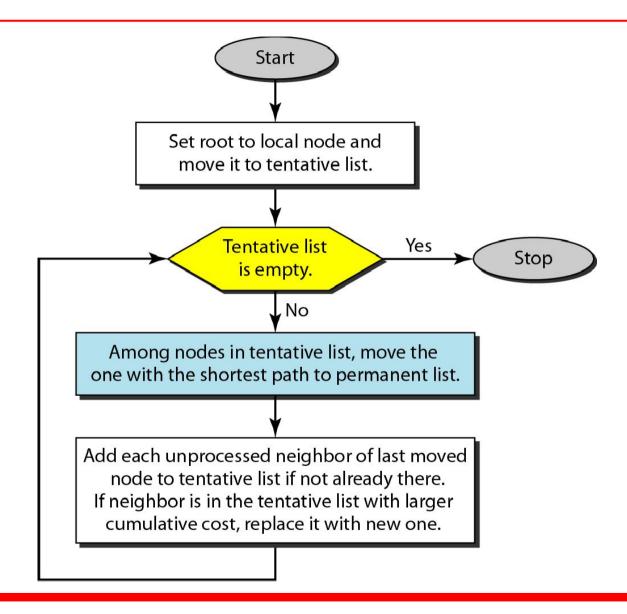


Figure 22.23 Example of formation of shortest path

tree

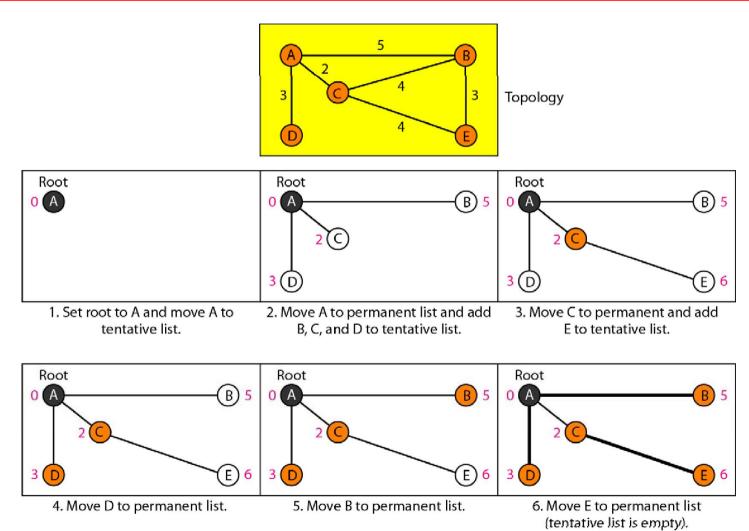


 Table 22.2Routing table for node A

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

Figure 22.24 Areas in an autonomous

system

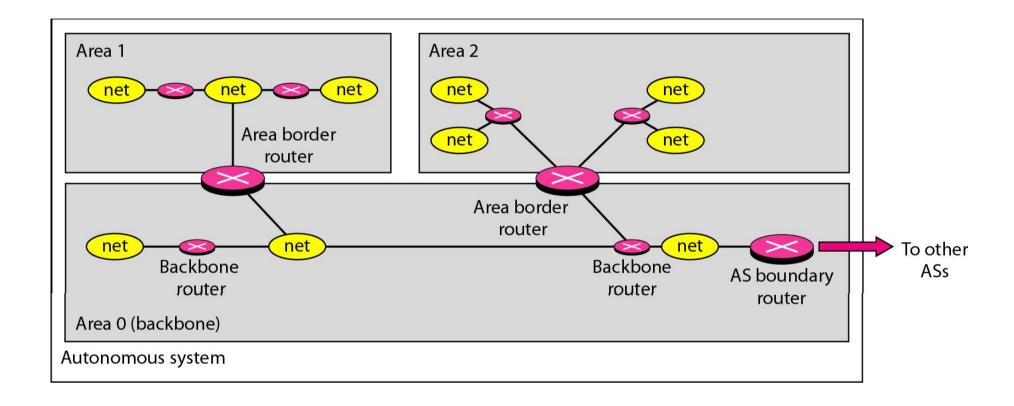


Figure 22.25 Types of

links

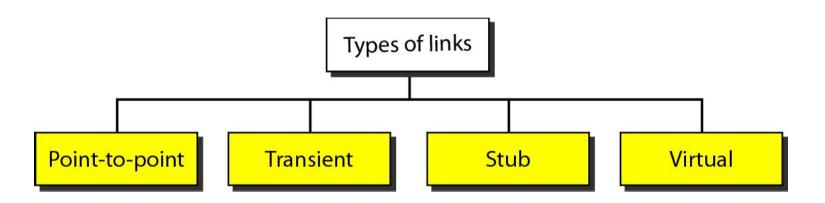


Figure 22.26 Point-to-point

link

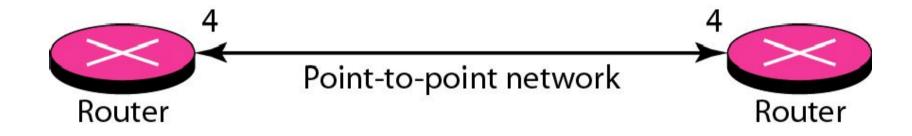
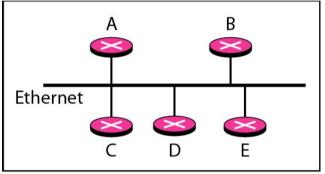
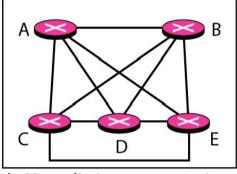


Figure 22.27 Transient

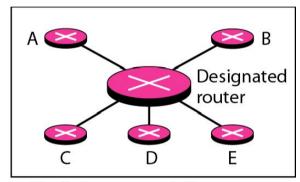
link



a. Transient network



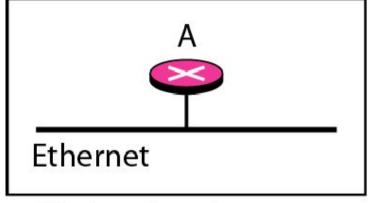
b. Unrealistic representation



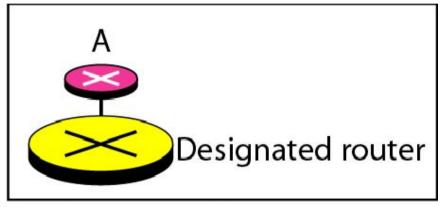
c. Realistic representation

Figure 22.28 Stub

link

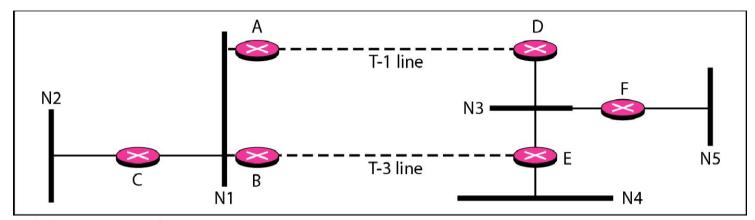


a. Stub network

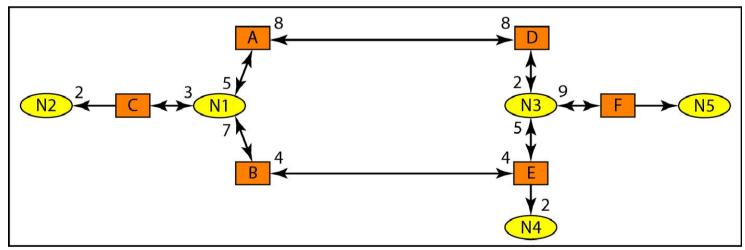


b. Representation

Figure 22.29 Example of an AS and its graphical representation in OSPF



a. Autonomous system



b. Graphical representation

Figure 22.30 Initial routing tables in path vector

routing

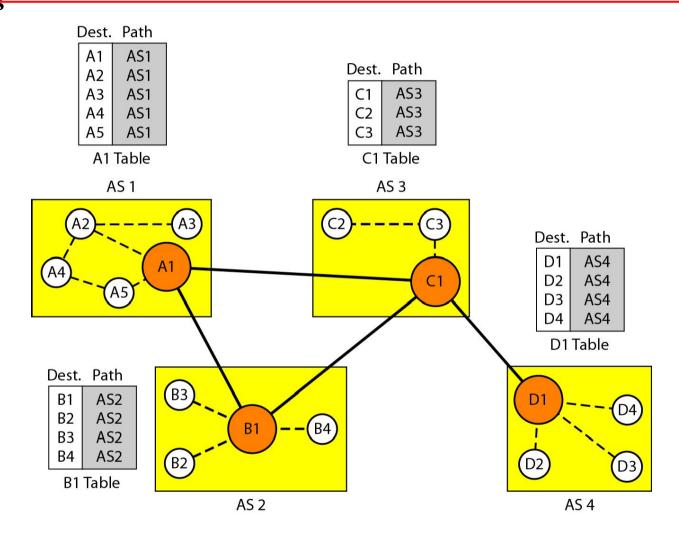


Figure 22.31 Stabilized tables for three autonomous

systems

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

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

D1 Table

Figure 22.32 Internal and external BGP

sessions

