UNIT - III

Learning Objectives

- Use of Mobility in network
- Discuss about Mobile IP
  - Mobile, Security related issues
- Routing Protocols
- Unicasting Protocols
- IP Multicasting
  - Multicasting routing protocols
  - Address assignment
  - session discovery

Mobile IP

The IP addresses are designed to work with stationary hosts because part of the address defines the network to which the host is attached.

Mobile IP

Mobile IP can be thought of as the cooperation of three major subsystems.

- First, there is a discovery mechanism defined so that mobile computers can determine their new attachment points (new IP addresses) as they move from place to place within the Internet.
- Second, once the mobile computer knows the IP address at its new attachment point, it *registers with an agent representing it at its home network.*
- Lastly, mobile IP defines simple mechanisms to deliver datagrams to the mobile node when it is away from its home network.

 U3.4

Mobile IP

Mobile IP introduces the following new functional entities:

- **Mobile node** — A host or router that changes its point of attachment from one network or subnetwork to another, without changing its IP address. A mobile node can continue to communicate with other Internet nodes at any location using its (constant) IP address.
- **Home agent —** A router on a mobile node's home network which delivers datagrams to departed mobile nodes, and maintains current location information for each.

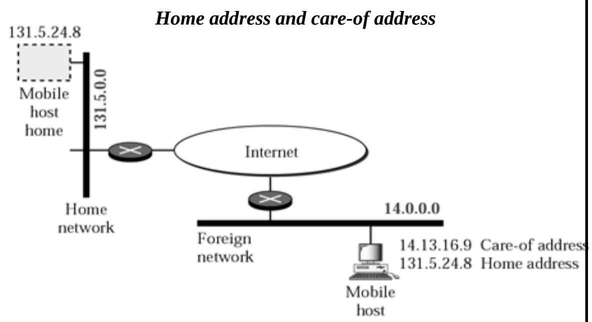
 U3.5

Mobile IP

- **Foreign agent —** A router on a mobile node's visited network which cooperates with the home agent to complete thedelivery of datagrams to the mobile node while it is away from home.
- A mobile node has a home address, which is a long-term IP address on its home network. When away from its home network, a *care-of address is associated with the mobile node and* reflects the mobile node's current point of attachment.
- The mobile node uses its home address as the source address of all IP datagrams it sends, except where otherwise required for certain registration request datagrams.

 U3.6

Mobile IP



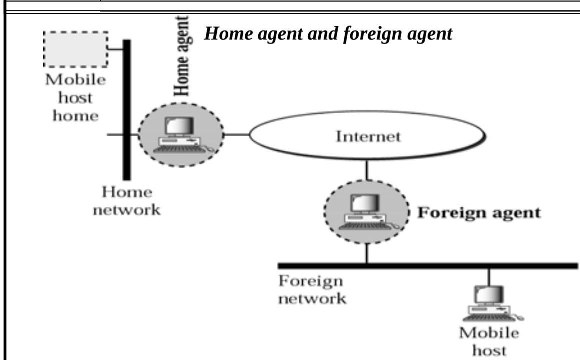
 U3.7

Mobile IP

- *Mobile IP has two addresses for a mobile host: one home address and one care-of address. The home address is permanent; the care-of address changes as the mobile host moves from one network to another.*

 U3.8

Mobile IP



 U3.9

Mobile IP

- *When the mobile host and the foreign agent are the same, the care-of address is called a co-located care-of address.*

 U3.10

Mobile IP

- The following terms are frequently used in connection with mobile IP:
- **Agent advertisement** — Foreign agents advertise their presence by using a special message, which is constructed by attaching a special extension to a router advertisement.
- **Care-of address** — The termination point of a tunnel toward a mobile node, for datagrams forwarded to the mobile node while it is away from home.
- There are two different types of care-of address: a foreign agent care-of address is an address of a foreign agent with which the mobile node is registered; a collocated care-of address is an externally obtained local address which the mobile node has associated with one of its own network interfaces.

 U3.11

Mobile IP

- **Care-of address** — The termination point of a tunnel toward a mobile node, for datagrams forwarded to the mobile node while it is away from home.
- There are two different types of care-of address:
- a foreign agent care-of address is an address of a foreign agent with which the mobile node is registered;
- a collocated care-of address is an externally obtained local address which the mobile node has associated with one of its own network interfaces.

 U3.12

Mobile IP

- **Correspondent node —** A peer with which a mobile node is communicating. A correspondent node may be either mobile or stationary.
- **Foreign network —** Any network other than the mobile node's home network.
- **Home address —** An IP address that is assigned for an extended period of time to a mobile node. It remains unchanged regardless of where the node is attached to the Internet.

Mobile IP

- **Home network —** A network, possibly virtual, having a network prefix matching that of a mobile node's home address. Note that standard IP routing mechanisms will deliver datagrams destined to a mobile node's home address to the mobile node's home network.
- **Link —** A facility or medium over which nodes can communicate at the link layer. A link underlies the network layer.
- **Link-layer address —** The address used to identify an endpoint of some communication over a physical link. Typically, the *link-layer address is an interface's media access control* (MAC) address.
- **Mobility agent** — Either a home agent or a foreign agent**.**

Mobile IP

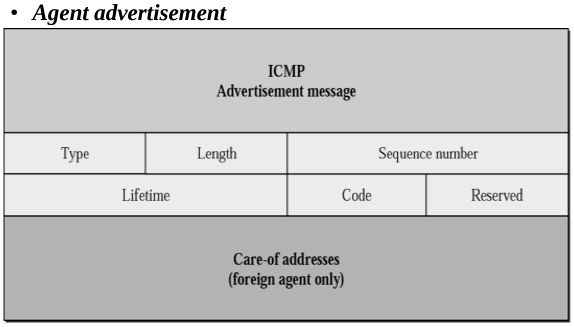
Remote host and mobile host communication

Mobile IP

- *Mobile IP does not use a new packet type for agent advertisement; it uses the router advertisement packet of ICMP, and appends an agent advertisement message.*

Mobile IP

- ***Agent advertisement***



Mobile IP

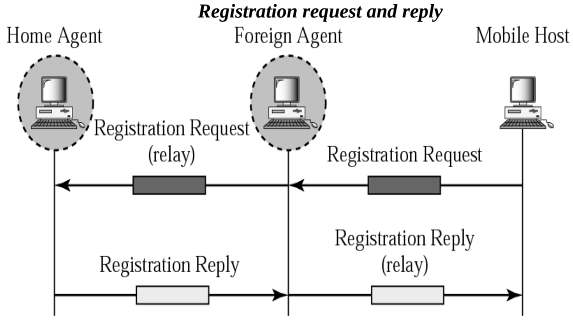
Bit	*Meaning*
0	Registration required. No co-located care-of address.
1	Agent is busy and does not accept registration at this moment.
2	Agent acts as a home agent.
3	Agent acts as a foreign agent.
4	Agent uses minimal encapsulation.
5	Agent uses generic routing encapsulation (GRE).
6	Agent supports header compression.
7	Unused (0).

Mobile IP

- *Mobile IP does not use a new packet type for agent solicitation; it uses the router solicitation packet of ICMP.*

Mobile IP

Registration request and reply



Mobile IP

Registration request format

Type	Flag	Lifetime
Home address		
Home agent address		
Care-of address		
Identification		
Extensions ...		

Mobile IP

Bit	Meaning
0	Mobile host requests that home agent retain its prior care-of address.
1	Mobile host requests that home agent tunnel any broadcast message.
2	Mobile host is using co-located care-of address.
3	Mobile host requests that home agent use minimal encapsulation.
4	Mobile host requests generic routing encapsulation (GRE).
5	Mobile host requests header compression.
6–7	Reserved bits.

Mobile IP

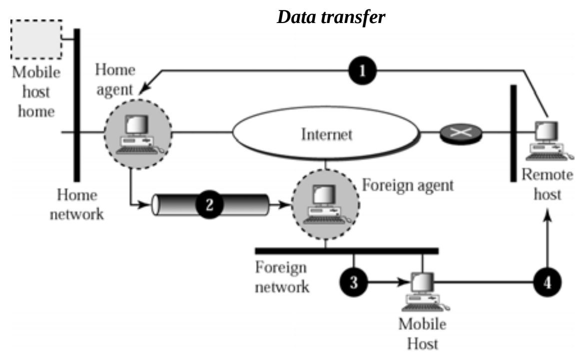
Registration reply format

Type	Code	Lifetime
Home address		
Home agent address		
Identification		
Extensions ...		

Mobile IP

- *A registration request or reply is sent by UDP using the well-known port 434.*

Mobile IP



Mobile IP

- *The movement of the mobile host is transparent to the rest of the Internet.*

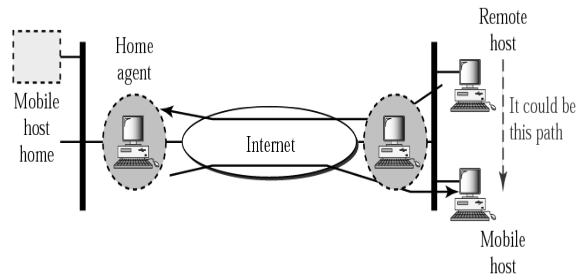
Mobile IP

Inefficiency in Mobile IP

Communication involving mobile IP can be inefficient. A severe case is called double crossing or 2X. A moderate case is called triangle routing or dog-leg routing.

Mobile IP

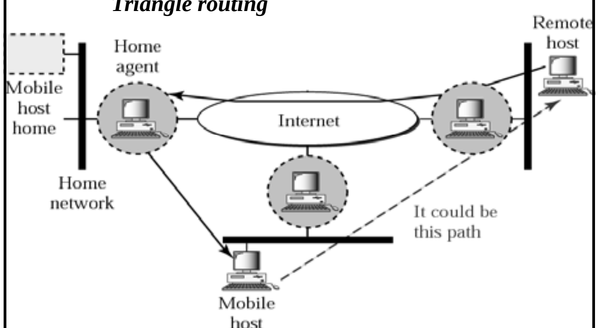
Double crossing



 U3.28

Mobile IP

Triangle routing



 U3.29

Routing Algorithms

The Optimality Principle
Shortest Path Routing
Flooding
Distance Vector Routing
Link State Routing
Hierarchical Routing
Broadcast Routing
Multicast Routing
Routing for Mobile Hosts
Routing in Ad Hoc Networks

 U3.30

Routing Algorithms

- The main function of the network layer is routing packets from the source machine to the destination machine. The algorithms that choose the routes and the data structures that they use are a major area of the network layer design.
- The routing algorithm is that part of the network layer software responsible for deciding which output line an incoming packet should be terminated on.
- If the subnet uses datagrams internally, this decision must be made a new for arriving packets since the best route may have changed since last time.

Routing Algorithms

- If the subnet uses virtual circuits internally, routing decision are made only when a new virtual circuit is being set up. Therefore, data packets just follow the previously established route. This case is sometimes called session routing because a route remains in force for an entire user session.

Routing Algorithms

Routing algorithms can be grouped into two major classes : Non adaptive and adaptive.

Non adaptive algorithms do not base their routing decisions on measurements or estimates of the current traffic and topology. This procedure is sometimes called static routing.

Adaptive algorithms, in contrast, change their routing decisions to reflect changes in the topology, and usually the traffic as well.

Routing Algorithms

List out the advantages and disadvantages of fixed routing.

•The advantages of fixed routing are as follows.
•The routes are always fixed and hence the routing overhead is minimum.
•The routing is dependent on network topology, i.e., static in nature.
•Routing is same for datagram and virtual circuit type of services.

The major disadvantages are:

•Lack of flexibility.
•The system is not robust. In case of link failure or node failure, the system cannot recover.
Congestion may occur on a particular route.

Routing Algorithms

What is flooding? Why flooding technique is not commonly used for routing?

Flooding is one type of non-adaptive routing technique where no network information is used. In case of flooding as each node receives a packet, it is re-transmitted or forwarded to all the links connected to the node (except the link through which the packet has arrived).

Flooding is not commonly used for routing for the following reasons:

- Flooding leads to unbounded number of packets
- May lead to congestion in the network
- A number of copies of the same packet is delivered at the destination node

Routing Algorithms

Define Autonomous Systems.

A routing domain generally is considered a portion of an internet under common administrative authority that is regulated by a particular set of administrative guidelines. Routing domains are also called **autonomous systems**.

Routing Algorithms

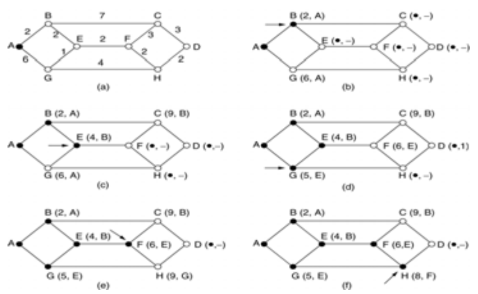
Differentiate between Link State and Distance Vector routing algorithms.

Link-state algorithms (also known as shortest path first algorithms) flood routing information to all nodes in the internetwork. Each router, however, sends only the portion of the routing table that describes the state of its own links. In link-state algorithms, each router builds a picture of the entire network in its routing tables.

Distance vector algorithms (also known as Bellman-Ford algorithms) call for each router to send all or some portion of its routing table, but only to its neighbors. In essence, link-state algorithms send small updates everywhere, while distance vector algorithms send larger updates only to neighboring routers. *Distance vector* algorithms know only about their neighbors.

Shortest Path Routing

The first 5 steps used in computing the shortest path from A to D.



Distance Vector Routing

Distance vector routing algorithms operate by having each router maintain a table (i.e. a vector) giving the best known distance to each destination and which line to use to there. These tables are updated by exchanging information with the neighbors.

The distance vector routing algorithm is sometimes called by other names, most commonly the distribute Bellman-Ford routing algorithm and the Ford-Fulkerson algorithm.

Distance Vector Routing

In distance vector routing, each router maintains a routing table indexed by, and containing one entry for, each router in the subnet. This entry contains two parts : the proffered outgoing line to use for that destination and an estimate of the time or distance to that destination.

The metric used might be number of hops, time delay in milliseconds, total number of packets queued along the path, or something similar.``

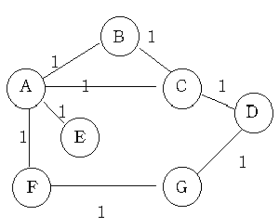
Distance Vector Routing

Distance-Vector Routing

- Each node constructs a one-dimensional array containing the "distances"(costs) to all other nodes and distributes that vector to its immediate neighbors.
- The starting assumption for distance-vector routing is that each node knows the cost of the link to each of its directly connected neighbors.
- A link that is down is assigned an infinite cost.

Distance Vector Routing

Example.



Distance Vector Routing

Information Stored at Node	Distance to Reach Node						
	A	**B**	**C**	**D**	**E**	**F**	**G**
A	0	1	1	�	1	1	�
B	1	0	1	�	�	�	�
C	1	1	0	1	�	�	�
D	�	�	1	0	�	�	1
E	1	�	�	�	0	�	�
F	1	�	�	�	�	0	1
G	�	�	�	1	�	1	0

Table : Initial distances stored at each node(global view).

We can represent each node's knowledge about the distances to all other nodes as a table

Distance Vector Routing

Note that each node only knows the information in one row of the table.

1. Every node sends a message to its directly connected neighbors containing its personal list of distance. (for example, **A** sends its information to its neighbors **B,C,E**, and **F**.)

Distance Vector Routing

2. If any of the recipients of the information from **A** find that **A** is advertising a path shorter than the one they currently know about, they update their list to give the new path length and note that they should send packets for that destination through **A**.

   (node **B**learns from **A** that node **E** can be reached at a cost of 1; **B** also knows it can reach **A** at a cost of 1, so it adds these to get the cost of reaching **E** by means of **A**. **B** records that it can reach **E** at a cost of 2 by going through **A**.)

Distance Vector Routing

3. After every node has exchanged a few updates with its directly connected neighbors, all nodes will know the least-cost path to all the other nodes.
4. In addition to updating their list of distances when they receive updates, the nodes need to keep track of which node told them about the path that they used to calculate the cost, so that they can create their forwarding table.

(for example, **B** knows that it was **A** who said " I can reach **E** in one hop" and so **B** puts an entry in its table that says " To reach **E**, use the link to **A**.)

 U3.46

Distance Vector Routing

Information Stored at Node	Distance to Reach Node						
	A	**B**	**C**	**D**	**E**	**F**	**G**
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

Table: final distances stored at each node (global view).

 U3.47

Distance Vector Routing

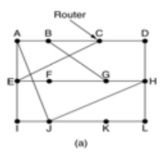
Destination	Cost	NextHop
A	1	A
C	1	C
D	2	C
E	2	A
F	2	A
G	3	A

Table : shows the complete routing table maintained at node B for the network

 U3.48

Distance Vector Routing

(a) A subnet. (b) Input from A, I, H, K, and the new routing table for J.



(a)

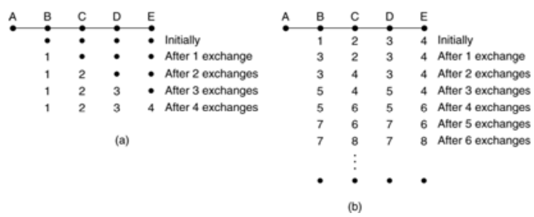
To	A	I	H	K	New estimated delay from J	Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	–
K	24	22	22	0	6	K
L	29	33	9	9	15	K
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6	New routing table for J	

Vectors received from J's four neighbors

(b)

 U3.49

Distance Vector Routing



The count-to-infinity problem.

 U3.50

Link State Routing

Link State Routing

- Every node knows how to reach its directly connected neighbors, and if we make sure that the totality of this knowledge is disseminated to every node, then every node will have enough knowledge of the network to determine correct routes to any destination.

 U3.51

Link State Routing

- **Reliable Flooding** is the process of making sure that all the nodes participating in the routing protocol get a copy of the link-state information from all the other nodes.
- As the term " flooding" suggests, the basic idea is for a node to send its link-state information out on all of its directly connected links, with each node that receives this information forwarding it out on all of its link.
- This process continues until the information has reached all the nodes in the network.

 U3.52

Link State Routing

- **Link State Packet (LSP)** contains the following information**:**
  - The ID of the node that created the LSP;
  - A list of directly connected neighbors of that node, with the cost of the link to each one;
  - A sequence number;
  - A time to live (TTL) for this packet.

 U3.53

Link State Routing

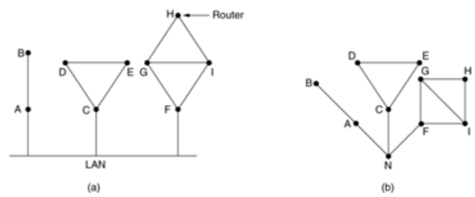
Each router must do the following:

1. Discover its neighbors, learn their network address.
2. Measure the delay or cost to each of its neighbors.
3. Construct a packet telling all it has just learned.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.

 U3.54

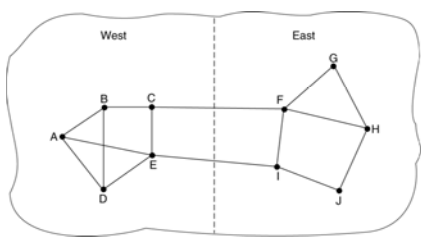
Learning about the Neighbors

Learn about neighbours

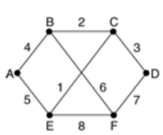


Measuring Line Cost

A subnet in which the East and West parts are connected by two lines.



Building Link State Packets



(a)

Link State Packets

A		B		C		D		E		F	
Seq.		Seq.		Seq.		Seq.		Seq.		Seq.	
Age		Age		Age		Age		Age		Age	
B	4	A	4	B	2	C	3	A	5	B	6
E	5	C	2	D	3	F	7	C	1	D	7
		F	6	E	1			F	8	E	8

(b)

(a) A subnet. (b) The link state packets for this subnet.

Distributing the Link State Packets

The packet buffer for router B in the previous slide

Source	Seq.	Age	Send flags A	Send flags C	Send flags F	ACK flags A	ACK flags C	ACK flags F	Data
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

 U3.58

Hierarchical Routing

- When hierarchical routing is used, the routers are divided into what we call regions, with each router knowing all the details about how to route packets to destinations with in own region, but knowing nothing about the internal structure of other regions.
- When different networks are interconnected, it is natural to regard each one as a separate region in order to free the routers in one network from having to know the topological structure of other ones.

 U3.59

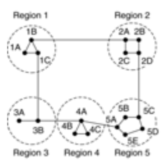
Hierarchical Routing

- For huge networks, a two-level hierarchy may be insufficient, it may be necessary to group the regions into clusters, the clusters into zones, the zones into groups, and so on.

 U3.60

Hierarchical Routing

Hierarchical routing.



(a)

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

(b)

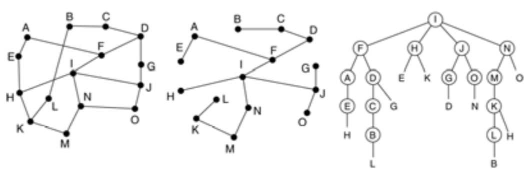
Hierarchical table for 1A

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

(c)

 U3.61

Broadcast Routing



(a) (b) (c)

Reverse path forwarding. (a) A subnet. (b) a Sink tree. (c) The tree built by reverse path forwarding.

 U3.62

Broadcast Routing

- In some applications, hosts need to send messages to many or all other hosts.
- For example, a service distributing weather reports, stock market updates or live radio programs.
- Sending a packet to all destinations simultaneously is called broadcasting.
- Various methods have been proposed for doing it :

 U3.63

Broadcast Routing

•One broadcasting method that requires no special features from the subnet is for the source to simply send a distinct packet to each destinations.

•Not only is the method wasteful of bandwidth, but it also requires the source to have a complete list of all destinations.

•In practice this may be the only possibility, but it is the least desirable of the methods.

Broadcast Routing

- Flooding is another method.
- Although Flooding is ill-suited for ordinary point-to-point communication, for broadcasting it might rate serious consideration.
- The problem with flooding as a broadcast technique is the same problem it has a point-to-point routing algorithms: it generates too many packets and consumes too much bandwidth.

Broadcast Routing

- A third algorithm is multi destination routing.
- If this method is used, each packet contains either a list of destinations or a bit map indicating the desired destinations.
- When a packet arrives at a router, the router checks all the destinations to determine the set of output lines what will be needed.
- The router regenerates a new copy of the packet for each output line to be used and includes in each packet only those destinations that are to use the line.

Broadcast Routing

•Fourth broadcast algorithm makes explicit use of the sink tree for the router initiating the broadcast- or any other convenient spanning tree for that matter.

•A spanning subtree is a subset of the subnet that includes all the routers but contains no loops.

•If each router knows which of its lines belong to the spanning tree lines except the one copy of an incoming broadcast packet onto all the spanning tree lines except the one is arrived on.

•This method makes excellent use of bandwidth, generating the absolute minimum number of packets necessary to do the job.

 U3.67

Broadcast Routing

•Our last broadcast algorithm is an attempt to approximate the behavior of the previous one.

•The idea is called, reverse path forwarding, is remarkably simple once it has been pointed out..

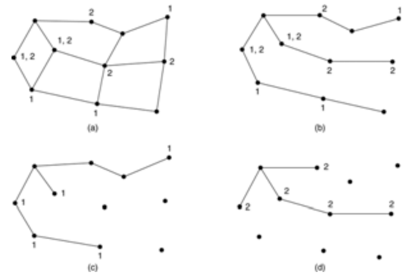
•When a broadcast packet arrives at a router, the router checks to see if the packet arrived on the line that is normally used for sending broadcast packets to the source of the broadcast.

•If so, there is an excellent chance that the broadcast packet itself followed the best route from the router and is therefore the first copy to arrive the router.

•This being the case, the router forwards copies of it onto all lines except the one it arrived on.

 U3.68

Multicast Routing



(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.

 U3.69

Routing Algorithms

- Introduction
- Routing Protocols
- Unicast Routing Protocols
- Multicast Routing protocols

 U3.70

Routing Algorithms

Unicast Routing Protocols: RIP, OSPF, and BGP

1. intra and inter domain routing
2. distance vector routing and RIP
3. link state routing and OSPF
4. path vector routing and BGP

 U3.71

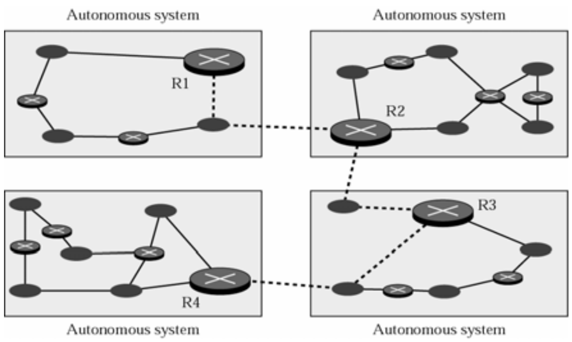
Routing Algorithms

Intra and Inter Domain Routing Protocols

- Routing inside an autonomous system is referred to as intradomain routing.
- Routing between autonomous systems is referred to as interdomain routing.

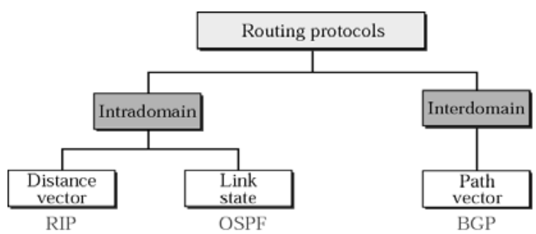
 U3.72

Routing Algorithms



 U3.73

Routing Algorithms



 U3.74

Routing Algorithms

Distance Vector Routing

In distance vector routing, the least cost route between any two nodes is the route with minimum distance. In this protocol each node maintains a vector (table) of minimum distances to every node

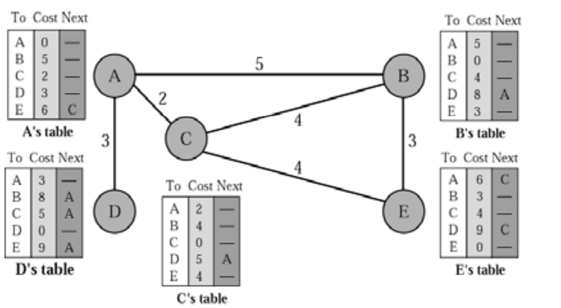
 U3.75

Routing Algorithms

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

Routing Algorithms

Distance vector routing tables



A's table

To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

B's table

To	Cost	Next
A	5	—
B	0	—
C	4	—
D	8	A
E	3	—

D's table

To	Cost	Next
A	3	—
B	8	A
C	5	A
D	0	—
E	9	A

C's table

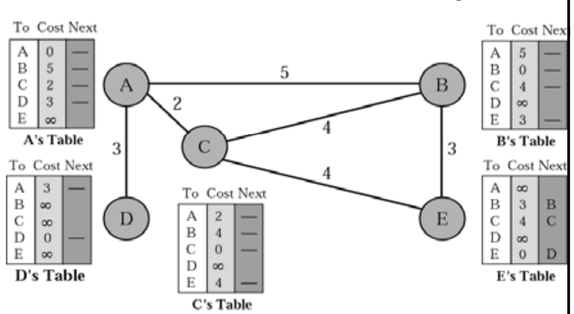
To	Cost	Next
A	2	—
B	4	—
C	0	—
D	5	A
E	4	—

E's table

To	Cost	Next
A	6	C
B	3	—
C	4	—
D	9	C
E	0	—

Routing Algorithms

Initialization of tables in distance vector routing



A's Table

To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	∞	

B's Table

To	Cost	Next
A	5	—
B	0	—
C	4	—
D	∞	
E	3	—

D's Table

To	Cost	Next
A	3	—
B	∞	
C	∞	
D	0	—
E	∞	

C's Table

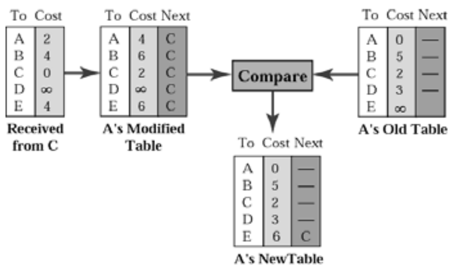
To	Cost	Next
A	2	—
B	4	—
C	0	—
D	∞	
E	4	—

E's Table

To	Cost	Next
A	∞	
B	3	B
C	4	C
D	∞	
E	0	D

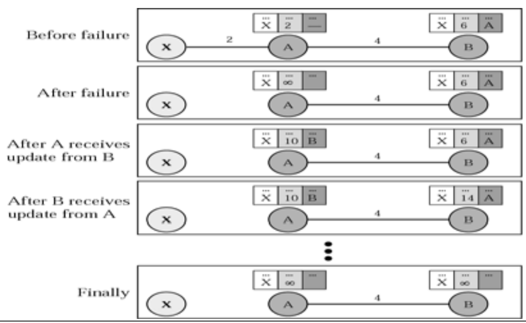
Routing Algorithms

Updating in distance vector routing



Routing Algorithms

Two-node instability



Routing Protocol

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.

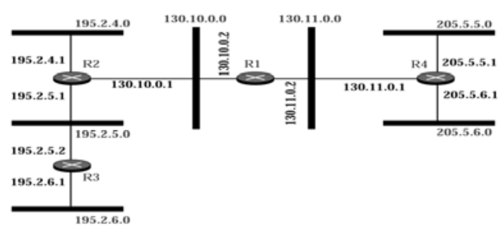
Routing Protocol

RIP uses the services of UDP on well-known port 520.

 U3.82

Routing Protocol

Example of a domain using RIP



Dest.	Hop	Next
130.10.0.0	1	——
130.11.0.0	1	——
195.2.4.0	2	130.10.0.1
195.2.5.0	2	130.10.0.1
195.2.6.0	3	130.10.0.1
205.5.5.0	2	130.11.0.1
205.5.6.0	2	130.11.0.1

R1 Table

Dest.	Hop	Next
130.10.0.0	1	——
130.11.0.0	2	130.10.0.2
195.2.4.0	1	——
195.2.5.0	1	——
195.2.6.0	2	195.2.5.2
205.5.5.0	3	130.10.0.2
205.5.6.0	3	130.10.0.2

R2 Table

Dest.	Hop	Next
130.10.0.0	2	195.2.5.1
130.11.0.0	3	195.2.5.1
195.2.4.0	2	195.2.5.1
195.2.5.0	1	——
195.2.6.0	1	——
205.5.5.0	4	195.2.5.1
205.5.6.0	4	195.2.5.1

R3 Table

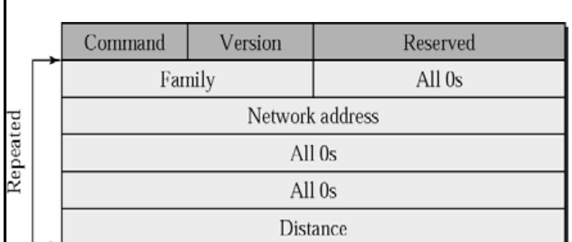
Dest.	Hop	Next
130.10.0.0	2	130.11.0.2
130.11.0.0	1	——
195.2.4.0	3	130.11.0.2
195.2.5.0	3	130.11.0.2
195.2.6.0	4	130.11.0.2
205.5.5.0	1	——
205.5.6.0	1	——

R4 Table

 U3.83

Routing Protocol

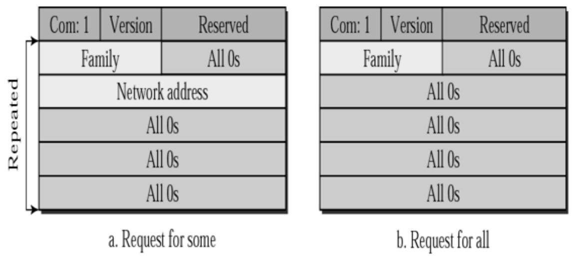
RIP message format



 U3.84

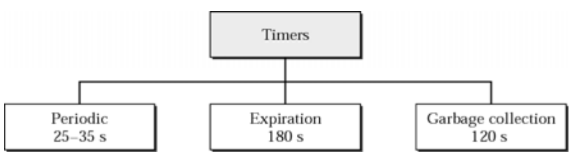
Routing Protocol

Request messages



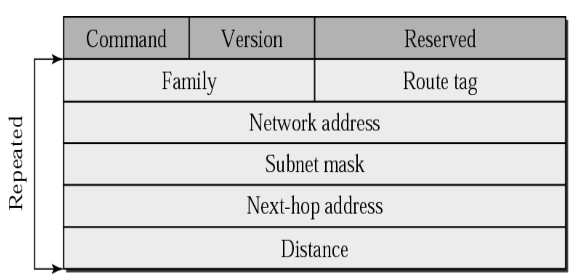
Routing Protocol

RIP timers



Routing Protocol

RIP version 2 format

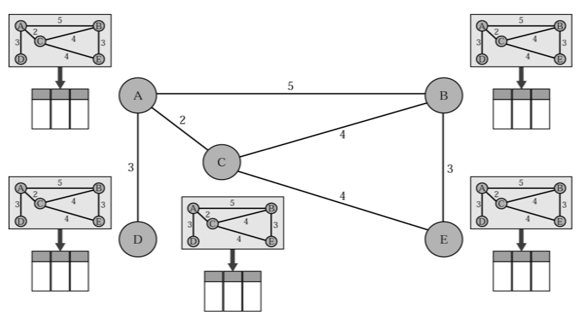


Routing Algorithms

Link State Routing

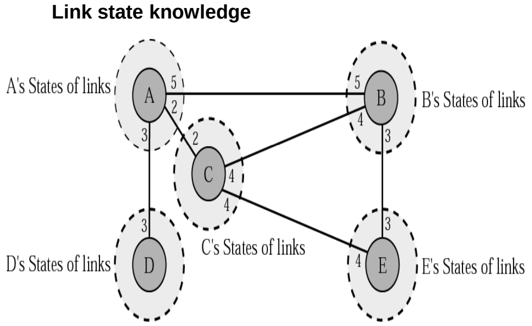
In link state routing, if each node in the domain has the entire topology of the domain, the node can use Dijkstra's algorithm to build a routing table.

Routing Algorithms



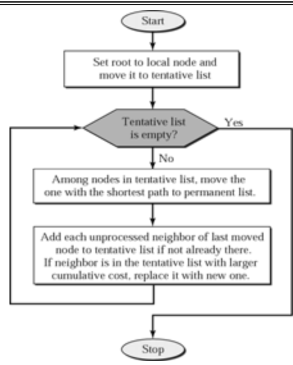
Routing Algorithms

Link state knowledge



Routing Algorithms

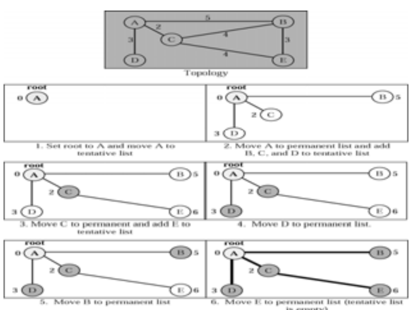
Dijkstra algorithm



 U3.91

Routing Algorithms

Example of formation of shortest path tree



 U3.92

Routing Algorithms

Routing table for node A

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

 U3.93

Routing Protocol

OSPF

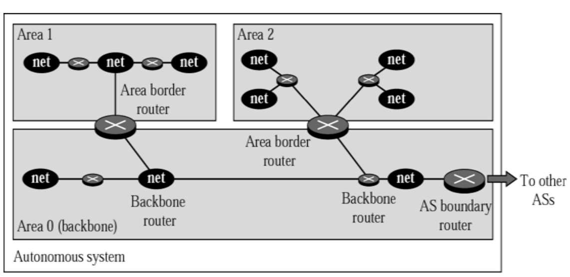
The Open Shortest Path First (OSPF) protocol is an intra domain routing protocol based on link state routing. Its domain is also an autonomous system.

Routing Protocol

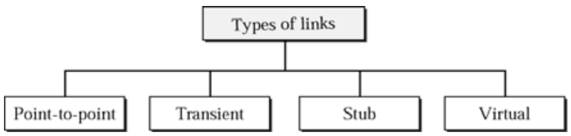
OSPF packets are encapsulated in IP datagrams.

Routing Protocol

Areas in an autonomous system

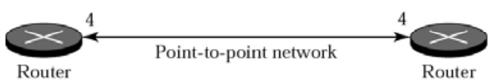


Routing Protocol



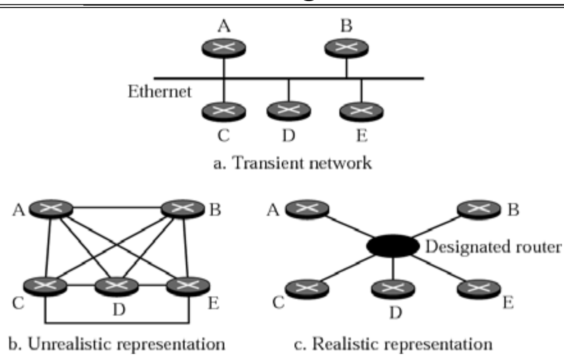
 U3.97

Routing Protocol



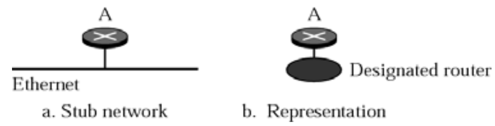
 U3.98

Routing Protocol

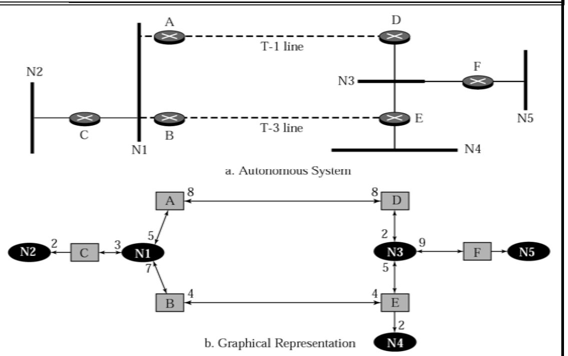


 U3.99

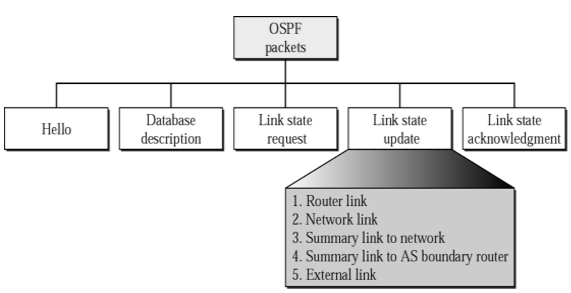
Routing Protocol



Routing Protocol



Routing Protocol



Routing Protocol

OSPF common header

0 – 7	8 – 15	16 – 31
Version	Type	Message length
Source router IP address		
Area Identification		
Checksum		Authentication type
Authentication (32 bits)		

Routing Protocol

Link state update packet

OSPF common header 24 bytes Type: 4
Number of link state advertisements
Link state advertisement Any combination of five different kinds (network link, router link, summary link to network, summary to boundary router, or external link)

Repeated

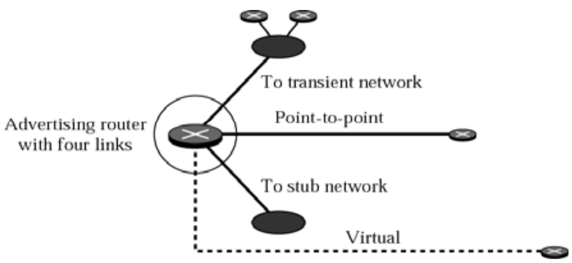
Routing Protocol

LSA general header

Link state age	Reserved	E	T	Link state type
Link state ID				
Advertising router				
Link state sequence number				
Link state checksum	Length			

Routing Protocol

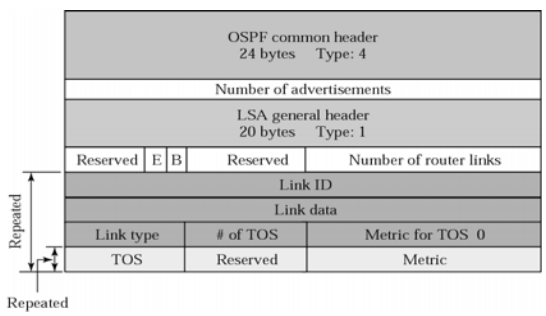
Router link



 U3.106

Routing Protocol

Router link LSA



 U3.107

Routing Protocol

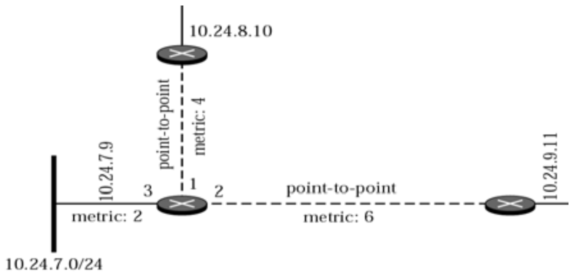
Link types, link identification, and link data

Link Type	*Link Identification*	*Link Data*
Type 1: Point-to-point	Address of neighbor router	Interface number
Type 2: Transient	Address of designated router	Router address
Type 3: Stub	Network address	Network mask
Type 4: Virtual	Address of neighbor router	Router address

 U3.108

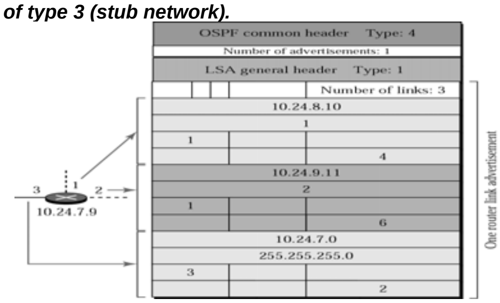
Routing Protocol

Example ***Give the router link LSA sent by router 10.24.7.9***



Routing Protocol

This router has three links: two of type 1 (point-to-point) and one of type 3 (stub network).

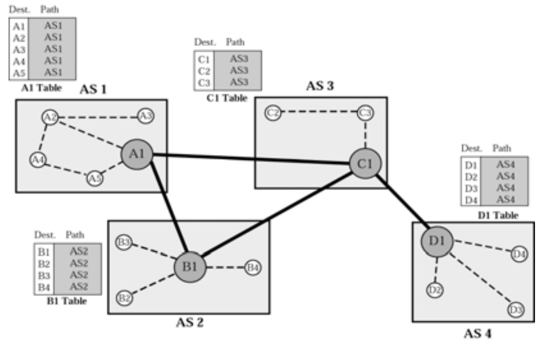


Routing Algorithms

Path Vector Routing

Path vector routing is similar to distance vector routing. There is at least one node, called the speaker node, in each AS that creates a routing table and advertises it to speaker nodes in the neighboring ASs..

Routing Algorithms



 U3.112

Routing Algorithms

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

A1 Table

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

 U3.113

Routing Protocol

Border Gateway Protocol

Border Gateway Protocol (BGP) is an inter domain routing protocol using path vector routing. It first appeared in 1989 and has gone through four versions.

 U3.114

Routing Protocol

- The Border Gateway Protocol (BGP) is an inter-autonomous system routing protocol.
- An autonomous system (AS) is a network or group of networks under a common administration and with common routing policies. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP), which are different ASes.
- The only requirement is that each AS have at least one router that is able to run BGP and that this router connect to at least one other AS's BGP router.

 U3.115

Routing Protocol

BGP Route Information Management Functions Conceptually, the overall activity of route information management can be considered to encompass four main tasks:

Route Storage: Each BGP stores information about how to reach networks in a set of special databases. It also uses databases to hold routing information received from other devices.

Route Update: When a BGP device receives an Update from one of its peers, it must decide how to use this information. Special techniques are applied to determine when and how to use the information received from peers to properly update the device's knowledge of routes.

 U3.116

Routing Protocol

Route Selection: Each BGP uses the information in its route databases to select good routes to each network on the internetwork.

Route Advertisement: Each BGP speaker regularly tells its peers what it knows about various networks and methods to reach them. This is called route advertisement and is accomplished using BGP Update messages.

 U3.117

Routing Protocol

BGP supports classless addressing and CIDR.

 U3.118

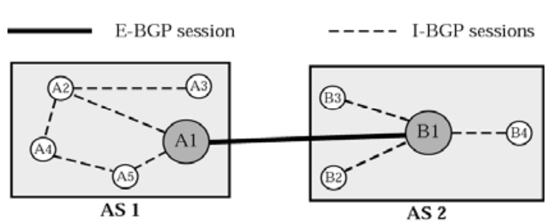
Routing Protocol

BGP uses the services of TCP
on port 179.

 U3.119

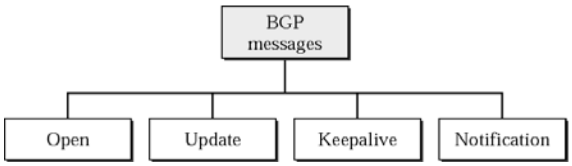
Routing Protocol

Internal and external BGP sessions



 U3.120

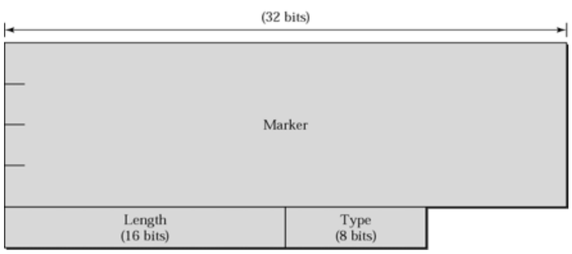
Routing Protocol



 U3.121

Routing Protocol

BGP packet header



 U3.122

BGP

Fields in the fixed header

MARKER: The 16-octect MARKER field contains a value that both sides agree to use to mark the beginning of the message. This is basically used for synchronization. In the initial message it contains all 1's and if the peers agree to use authentication mechanism, the marker can contain the authentication information.

LENGTH: The 2-octect LENGTH field Specifies the Total message length measured in octets. The minimum message size is 19 octets (i.e. only fixed header), and the maximum allowable length is 4096 octets.

 U3.123

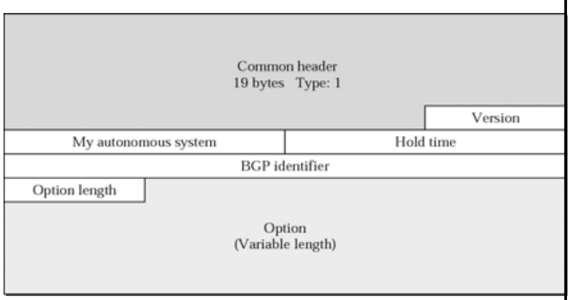
BGP

TYPE: 1-octet field contains one of the 4 values of the message type listed below:

Type Code	Message Type	Description
1	OPEN	Initialize communication
2	UPDATE	Advertise or withdraw routes
3	NOTIFICATION	Response to an Incorrect message
4	KEEPALIVE	Actively test peer Connectivity

Routing Protocol

Open message



Routing Protocol

Open message

This is the first message send after the BGP peers establishes a TCP connection. Both of the peers send OPEN message to declare their autonomous system number and other operating parameters.

Routing Protocol

Fields in the message header has been explained below:

Version: It identifies the protocol version used.

Autonomous System Number: Gives the autonomous system of the sender's system.

Hold Time: it specifies maximum time receiver should wait for a message from sender. The receiver implements a timer using this value. The value is reset each time a message arrives; if timer expires it assumes that sender is not available.

Routing Protocol

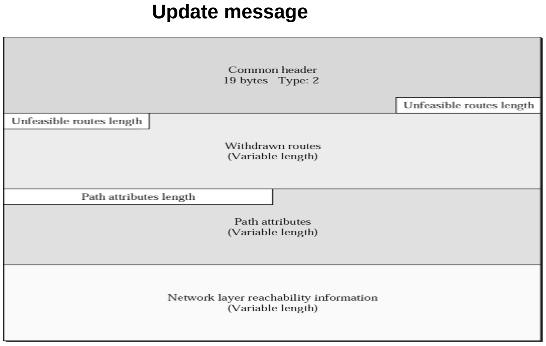
BGP identifier: It is a 32-bit value that uniquely identifies the sender. It is the IP address and the router must choose one of its IP addresses to use with all the BGP peers.

Parameter Length: If Optional parameters are specified then this fields contains the length of optional parameters, in octets.

Optional Parameters: It contains a list of parameters. Authentication is also a kind of parameter in BGP. It's done in this way so that the BGP peers can choose the authentication method without making it a part of BGP fixed header.

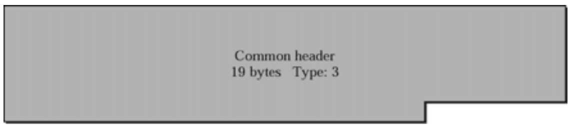
Routing Protocol

Update message



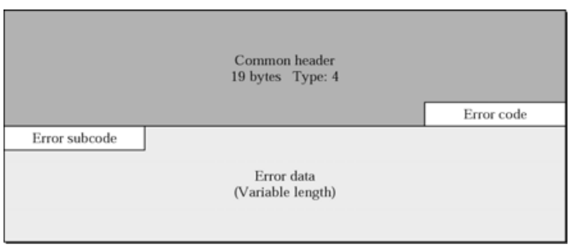
Routing Protocol

Keepalive message



Routing Protocol

Notification message



Routing Protocol

Notification message

Error Code	Meaning
1	Error in Message header
2	Error in OPEN Message
3	Error in UPDATE Message
4	Hold Timer Expired
5	Finite State machine Error
6	Cease (terminate connection)

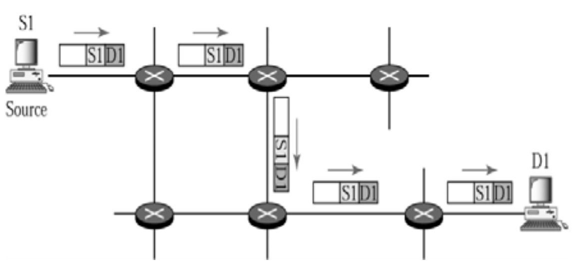
Routing Protocol

A message can be unicast, multicast, or broadcast. Let us clarify these terms as they relate to the Internet.

 U3.133

Routing Protocol

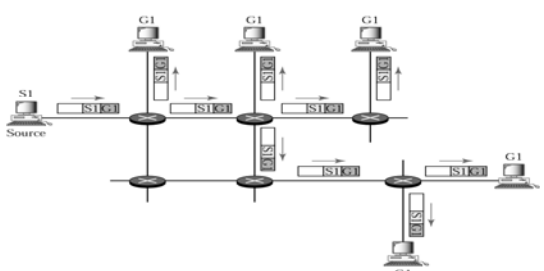
Unicast :- the router forwards the received packet through only one of its interfaces



 U3.134

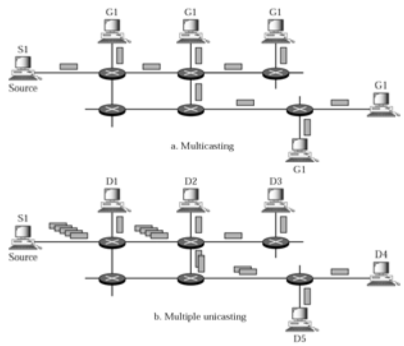
Routing Protocol

Multiicast :- *the router may forward the received packet through several of its interfaces*



 U3.135

Routing Protocol



 U3.136

Routing Protocol

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

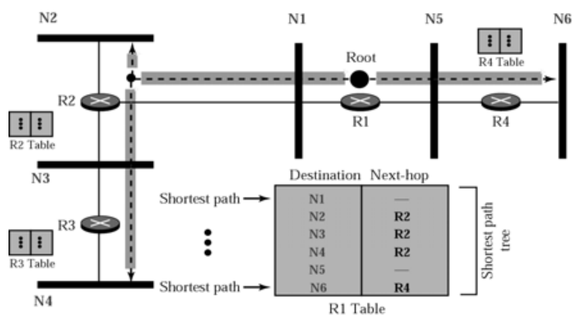
 U3.137

Routing Protocol

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

 U3.138

Routing Protocol



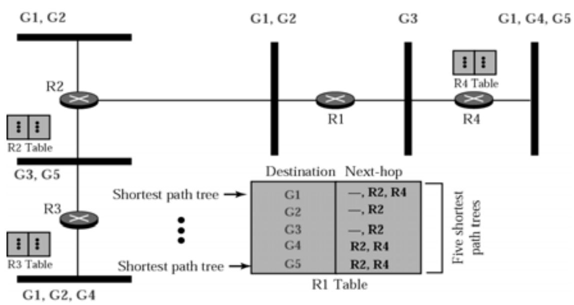
Routing Protocol

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

Routing Protocol

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

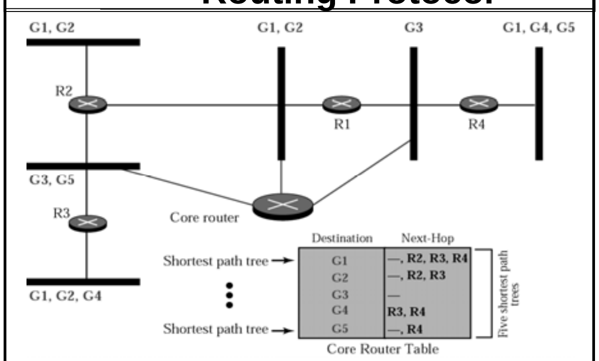
Routing Protocol



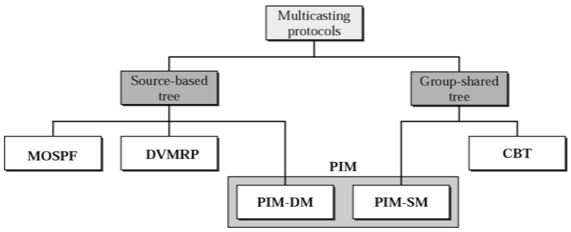
Routing Protocol

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

Routing Protocol



Routing Protocol



 U3.145

Routing Protocol

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

 U3.146

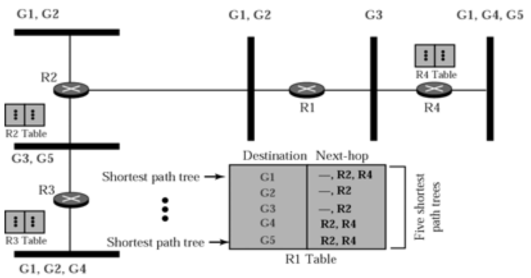
Routing Protocol

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

 U3.147

Routing Protocol

Source-based tree approach



 U3.148

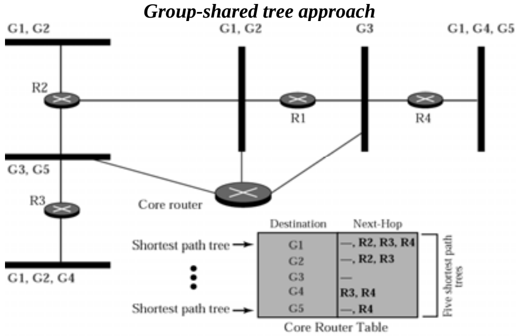
Routing Protocol

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

 U3.149

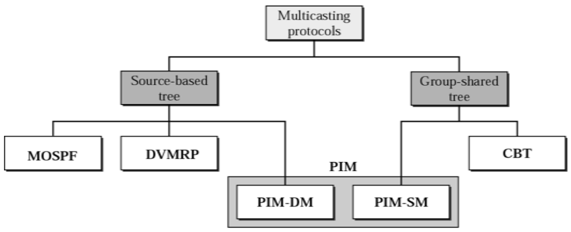
Routing Protocol

Group-shared tree approach



 U3.150

Routing Protocol



Routing Protocol

- Several algorithms have been proposed for building multicast trees through which the multicast packets can be delivered to the destination nodes.
- These algorithms can be potentially used in implementing the multicast routing protocols: -
  - Flooding
  - Spanning Trees
  - Reverse Path Forwarding (RPF)
  - Truncated Reverse Path Forwarding (TRPF)
  - Steiner Trees (ST), and
  - Core-Based Trees (CBT).

Flooding

- The Flooding algorithm which has been already used in protocols such as OSPF is the simplest technique for delivering the multicast datagrams to the routers of an internetwork.
- In this algorithm, when a router receives a multicast packet it will first check whether it has seen this particular packet earlier or this is the first time that this packet has reached this router.
- If this is the first time, the router will forward the packet on all interfaces, except the one from which the packet has been received.

Flooding

- Otherwise, the router will simply discard the packet. This way we make sure that all routers in the internetwork will receive at least one copy of the packet.
- Although this algorithm is pretty simple, it has some major disadvantages. The flooding algorithm generates a large number of duplicated packets and waste the network bandwidth.
- Furthermore, since each router needs to keep track of the packets it hasreceived in order to find out whether this is the first time that a particular packet has been seen or not, it needs to maintain a distinct entry in its table for each recently seen packet.
- Therefore, the Flooding algorithm makes inefficient use of router memory resources.

 U3.154

Spanning Trees

- A better algorithm than Flooding is the Spanning Tree algorithm. This algorithm which has been already used by IEEE-802 MAC bridges is powerful and easy to implement.
- In this algorithm, a subset of internetwork links are selected to define a tree structure (loop-less graph) such that there is only one active path between any two routers.
- Since this tree spans to all nodes in the internetwork it is called spanning tree.
- Whenever a router receives a multicast packet, it forwards the packet on all the links which belong to the spanning tree except the one on which the packet has arrived, guaranteeing that the multicast packet reaches all the routers in the internetwork.

 U3.155

Spanning Trees

- Obviously, the only information a router needs to keep is a boolean variable per network interface indicating whether the link belongs to the spanning tree or not. We use a small network with five nodes and six links to show different trees.
- For simplicity sake, we do not differentiate between hosts and routers, subnets and links.
- We also assume that links are symmetric and their costs are shown next to the link
- The spanning tree algorithm has two drawbacks:
  - It centralizes all the traffic on a small set of links and
  - it does not consider the group membership.

 U3.156

Reverse Path Broadcasting (RPB)

- The RPB algorithm which is currently being used in the MBone (Multicast Backbone), is a modification of the Spanning Tree algorithm.
- In this algorithm, instead of building a network-wide spanning tree, an implicit spanning tree is constructed for each source.
- Based on this algorithm whenever a router receives a multicast packet on link "L" and from source "S", the router will check and see if the link L belongs to the shortest path toward S.
- If this is the case the packet is forwarded on all inks except L. Otherwise, the packet is discarded.

 U3.157

Truncated Reverse Path Broadcasting (TRPB)

- The TRPB algorithm has been proposed to overcome some of the limitations of the RPB algorithm. We earlier mentioned that by using IGMP protocol, a router can determine whether members of a given multicast group are present on the router subnetwork or not.
- If this sub network is a leaf sub network (it doesn't have any other router connected to it) the router will truncate the spanning tree.
- It should be noted here that TRPB similar to RPB won't forward the message to a neighbor router if the local router is not on the shortest path from the neighbor router to the source node.

 U3.158

Truncated Reverse Path Broadcasting (TRPB)

- Although, multicast group membership is used in the TRPB algorithm and the leaf subnets are truncated from the spanning trees but, it does not eliminate unnecessary traffics on non-leaf sub networks which do not have group member.

 U3.159

Reverse Path Multicasting (RPM)

- The RPM algorithm (also known as RPB with prunes) is an enhancement to the RPB and TRPB algorithms. RPM constructs a delivery tree that spans only:
- *1) sub networks with group members, and*
- *2) routers and sub networks along the shortest path to Sub networks with group members*
- The RPM tree can be pruned such that the multicast packets are forwarded along links which lead to members of the destination group.

 U3.160

Reverse Path Multicasting (RPM)

- For a given pair of (source, group) the first multicast packet is forwarded based on the TRPB algorithm. The routers which do not have any downstream router in the TRPB tree are called leaf routers.
- If a leaf router receives a multicast packet for a(source, group) pair and it does not have any group member on its subnetworks, it will send a "prune" message to the router from which it has received the multicast packet.
- The prune message indicates that the multicast packets of that particular (source, group) pair should not be forwarded on the link from which the prune message has been received. It is important to note that prune messages are only sent one hop back towards the source.

 U3.161

Reverse Path Multicasting (RPM)

- The upstream router is required to record the prune information in its memory.
- On the other hand, if the upstream router does not have any local recipient and receives prune messages from all of its children in the TRPB tree, the upstream router will send a prune message itself to its parent in the RPB tree indicating that the multicast packets for the (source, group) pair need not be forwarded to it.

 U3.162

Core-Based Trees (CBT)

- The latest algorithm proposed for constructing multicast deliver trees is called Core-Based Tree (CBT) algorithm. Unlike other algorithms discussed earlier, CBT creates a single delivery tree for each group.
- In other words, the tree used for forwarding multicast messages of a particular group, is a single tree regardless of the location of the source node.
- A single router, or a set of routers, are chosen to be the "core" router of a delivery tree. All messages to a particular group are forwarded as unicast messages toward the core router until they reach a router which belongs to the corresponding delivery tree.
- Then, the packet is forwarded to all ongoing interfaces which are part of the delivery tree except the incoming interface.

 U3.163

Routing Protocol

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

 U3.164

Routing Protocol

Flooding broadcasts packets, but creates loops in the systems.

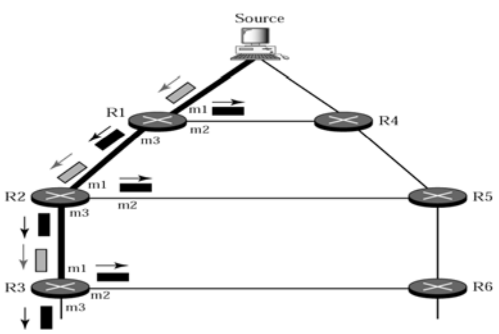
 U3.165

Routing Protocol

RPF eliminates the loop in the flooding process.

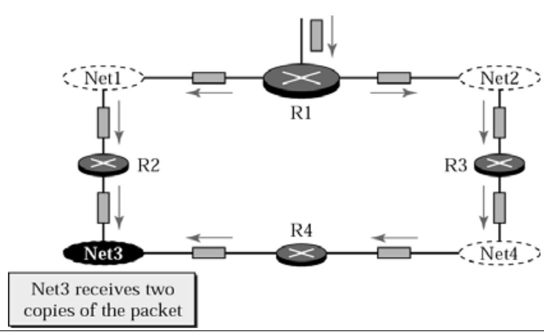
Routing Protocol

RPF



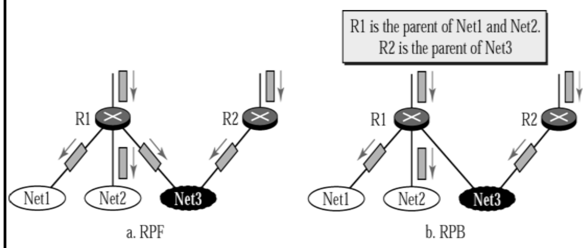
Routing Protocol

Problem with RPF



Routing Protocol

RPF versus RPB



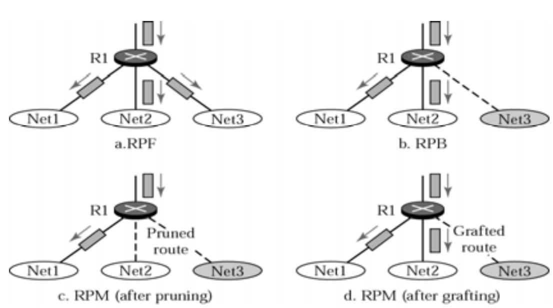
Routing Protocol

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.

Routing Protocol

RPF, RPB, and RPM



Routing Protocol

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

 U3.172

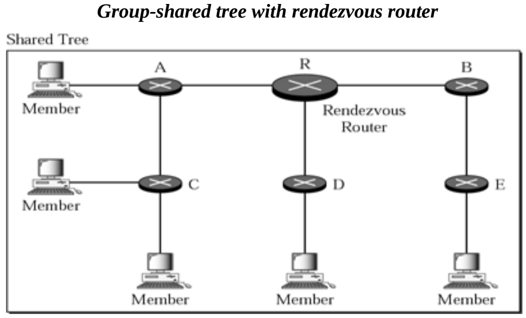
Routing Protocol

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 (center router or rendezvous router) is chosen for each region.

 U3.173

Routing Protocol

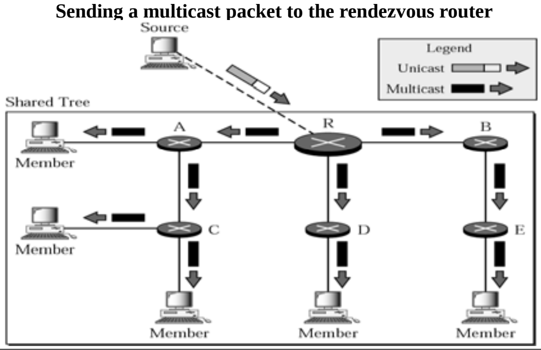
Group-shared tree with rendezvous router



 U3.174

Routing Protocol

Sending a multicast packet to the rendezvous router



 U3.175

Routing Protocol

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.

 U3.176

Multicast Routing Protocols

- Multicast Routing Protocol (DVMRP),
- Multicast Extensions to OSPF (MOSPF) protocol,
- Protocol Independent Multicast- Dense Mode (PIM-DM) protocol)
- Protocol Independent Multicast - Sparse Mode (PIM-SM)

 U3.177

Multicast Routing Protocols

- The Distance Vector Multicast Routing Protocol (DVMRP) which was originally defined in RFC 1075 was driven from Routing Information Protocol (RIP) with the difference being that RIP forwards the unicast packets based on the information about the next-hop toward a destination,
- while DVMRP constructs delivery trees based on the information on the previous-hop back to the source.

 U3.178

Multicast Routing Protocols

- The earlier version of this distance-vector routing algorithm constructs delivery trees based on TRPB algorithm. Later on, DVMRP was enhanced to use RPM.
- Standardization of the latest version of DVMRP is being conducted by the Internet Engineering Task Force (IETF) Inter-Domain Multicast Routing (IDMR) working group.

 U3.179

Multicast Routing Protocols

- Furthermore, a new type of messages is used to quickly **"graft" back a** previously pruned branch of a delivery tree in case a new host on that branch joins the multicast group.
- Similar to prune messages which are forwarded hop by hop, graft messages are sent back one hop at a time until they reach a node which is on the multicast delivery tree. Similar to RPM, DVMRP still implements the flooding of packets periodically.

 U3.180

Multicast Routing Protocols

- DVMRP as mentioned earlier implements the RPM algorithm.
- The first packet of multicast messages sent from a particular source to a particular multicast group is flooded across the internetwork.
- Then, prune messages are used to truncate the branches which do not lead to a group member.

 U3.181

Multicast Routing Protocols

- MOSPF uses the group membership information obtained through IGMP and with the help of OSPF database builds multicast delivery trees.
- These trees are shortest-path trees constructed (on demand) for each (source, group) pair.
- Although MOSPF does not support tunnels it can coexist and interoperate with non-MOSPF routers.

 U3.182

Multicast Routing Protocols

- The Protocol Independent Multicast (PIM) routing protocols are being developed by the Inter-Domain Multicast Routing (IDMR) working group of the IETF.
- IDMR is planned to develop a set of multicast routing protocols which independent of any particular unicast routing protocol can provide scalable Internet-wide multicast routing.
- Of course, PIM requires the existence of a unicast routing protocol.

 U3.183

Multicast Routing Protocols

- The major proposed (and used) multicast protocols perform well if group members are densely packed and bandwidth is not a problem.
- However, the fact that DVMRP periodically floods the network and the fact that MOSPF sends group membership information over the links, make these protocols not efficient in cases where group members are sparsely distributed among regions and the bandwidth is not plentiful.

 U3.184

Multicast Routing Protocols

- To address these issues, PIM contains two protocols:
- PIM - Dense Mode (PIM-DM) which is more efficient when the group members are densely distributed, and
- PIM - Sparse Mode (PIM-SM) which performs better in cases where group members are sparsely distributed.
- Although these two algorithms belong to PIM and they share similar control messages, they are essentially two different protocols.

 U3.185

Routing Protocol

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).

 U3.186

Routing Protocol

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

Routing Protocol

- *PIM-DM uses RPF and pruning/grafting strategies to handle multicasting.*

  However, it is independent from the underlying unicast protocol.

Routing Protocol

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

Routing Protocol

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

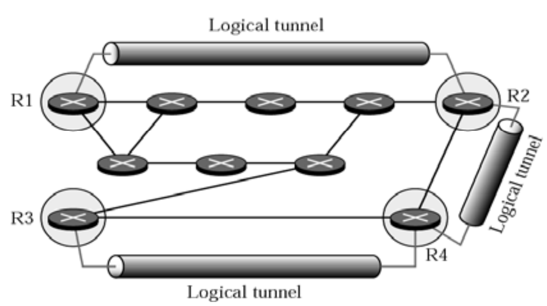
.

Routing Protocol

A multicast router may not find another multicast router in the neighborhood to forward the multicast packet. A solution for this problem is tunneling. We make a multicast backbone (MBONE) out of these isolated routers using the concept of tunneling.

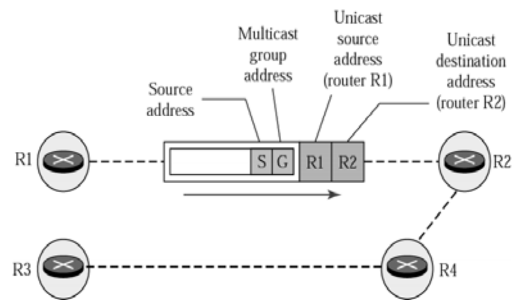
Routing Protocol

Logical tunneling



Routing Protocol

MBONE



 U3.193

Summary

- Routing inside an autonomous system is referred to as intradomain routing.
- Routing between autonomous systems is referred to as interdomain routing.
- In distance vector routing, each node shares its routing table with its immediate neighbors periodically and when there is a change.

 U3.194

Summary

- In multicast routing, each involved router needs to construct a shortest path tree for each group
- In the source-based tree approach, each router needs to have one shortest path tree for each group.
- In the group-shared tree approach, only the core router, which has a shortest path tree for each group, is involved in multicasting.
- The Flooding algorithm which has been already used in protocols such as OSPF is the simplest technique for delivering the multicast datagrams to the routers of an internetwork.
- RPB creates a shortest path broadcast tree from the source to each destination.

 U3.195

Short Questions

1. Why Care-of address use in Mobile IP?
2. Explain Reverse Path Multicasting.
3. How can we secure Mobile IP?
4. What are the different types of intra-domain and inter-domain routing protocols?
5. What are the security related issues in Mobile IP?
6. What are the different phases include in communication between Remote host and Mobile host?
7. Explain the term Triangle Routing and Double Crossing in the Mobile IP. What are the solutions?
8. What do you mean by session discovery?
9. Explain PIM.
10. Discuss RIP and OSPF.

 U3.196

Long Questions

1. Why Care-of address use in Mobile IP?
2. Differentiate between DVMRP and CBT routing protocols.
3. Explain the term Triangle Routing and Double Crossing in the Mobile IP. What are the solutions?
4. Differentiate between MOSPF and PIM routing protocols
5. Explain Reverse Path Multicasting.
6. Comparison between Source-Based Tree and Group-Based Tree in router multicasting.
7. Explain the architecture of Mobile IP. How care-of-address used in between Home Agent and Foreign Agent?
8. Difference between Unicast and Multicast routing protocols.

 U3.197

References

1. W. ER. Stevens, "TCP/IP illustrated, Volume 1: The protocols", Addison Wesley, 1994.
2. G. R. Wright, "TCP/IP illustrated volume 2. The Implementation", Addison Wesley,1995.
3. Forouzan, "TCP/IP Protocol Suite", Tata Mc Grew Hill, 4th Ed., 2009.
4. William Stalling, "Cryptography and Network Security", Pearson Publication.

 U3.198