MULTICAST ROUTING

SIDDAGANGA INSTITUTE OF TECHNOLOGY

Department of CSE

Prabodh C P

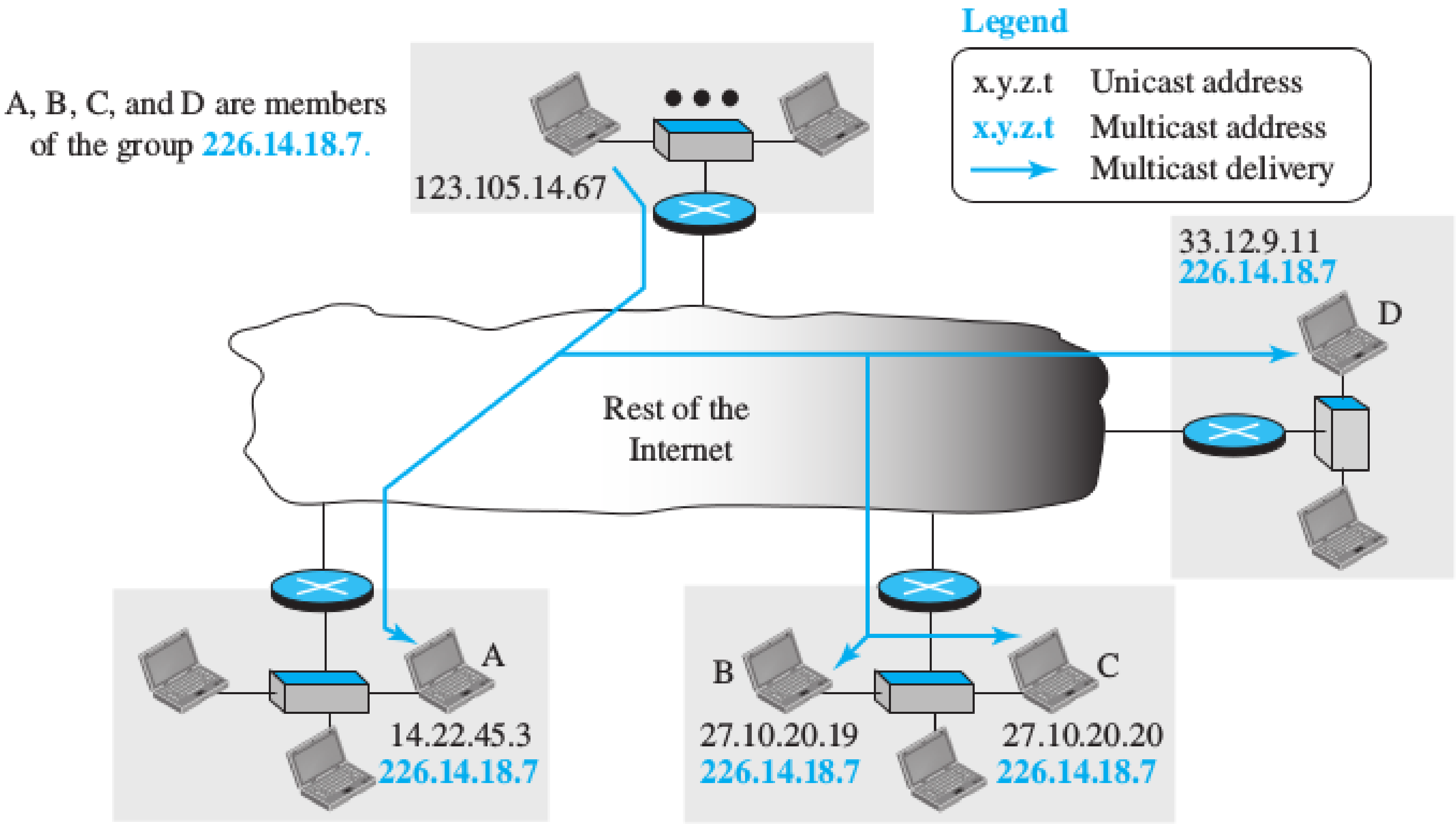
Contents

- MULTICAST ROUTING PROTOCOLS
  - MULTICASTING BASICS
    - Multicast Addresses
    - Delivery at Data-Link Layer
    - Collecting Information about Groups
    - Multicast Forwarding
    - Two Approaches to Multicasting
  - INTRADOMAIN MULTICAST PROTOCOLS
    - Multicast Distance Vector (DVMRP)
    - Multicast Link State (MOSPF)
    - Protocol Independent Multicast (PIM).

Multicast Addresses

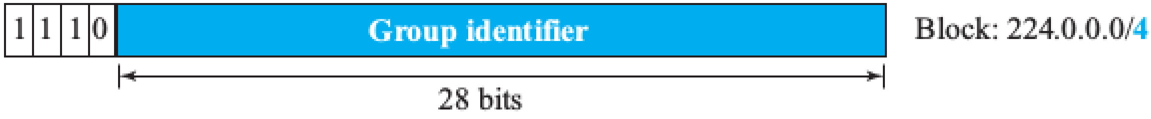
- In multicast communication, the sender is only one, but the receiver is many.
- The destination address of a packet, as described in the Internet Protocol (IP) should be only one.
- A multicast address defines a group of recipients, not a single one.
- In other words, a multicast address is an identifier for a group.
- A host, which is a member of n groups, actually has (n + 1) addresses: one unicast address that is used for source or destination address in unicast communication and n multicast addresses that are used only for destination addresses to receive messages sent to a group.

Need for multicast addresses



Multicast Addresses in IPv4

- A router or a destination host needs to distinguish between a unicast and a multicast datagram.
- Multicast addresses in IPv4 belong to a large block of addresses that are specially designed for this purpose.
- In classful addressing, all of class D was composed of these addresses; classless addressing used the same block, but it was referred to as the block 224.0.0.0/4 (from 224.0.0.0 to 239.255.255.255).



- The number of addresses in the multicast block is huge (**2^{28}**). However, the block is divided into several subblocks, and each subblock is used in a particular multicast application.

Subblocks

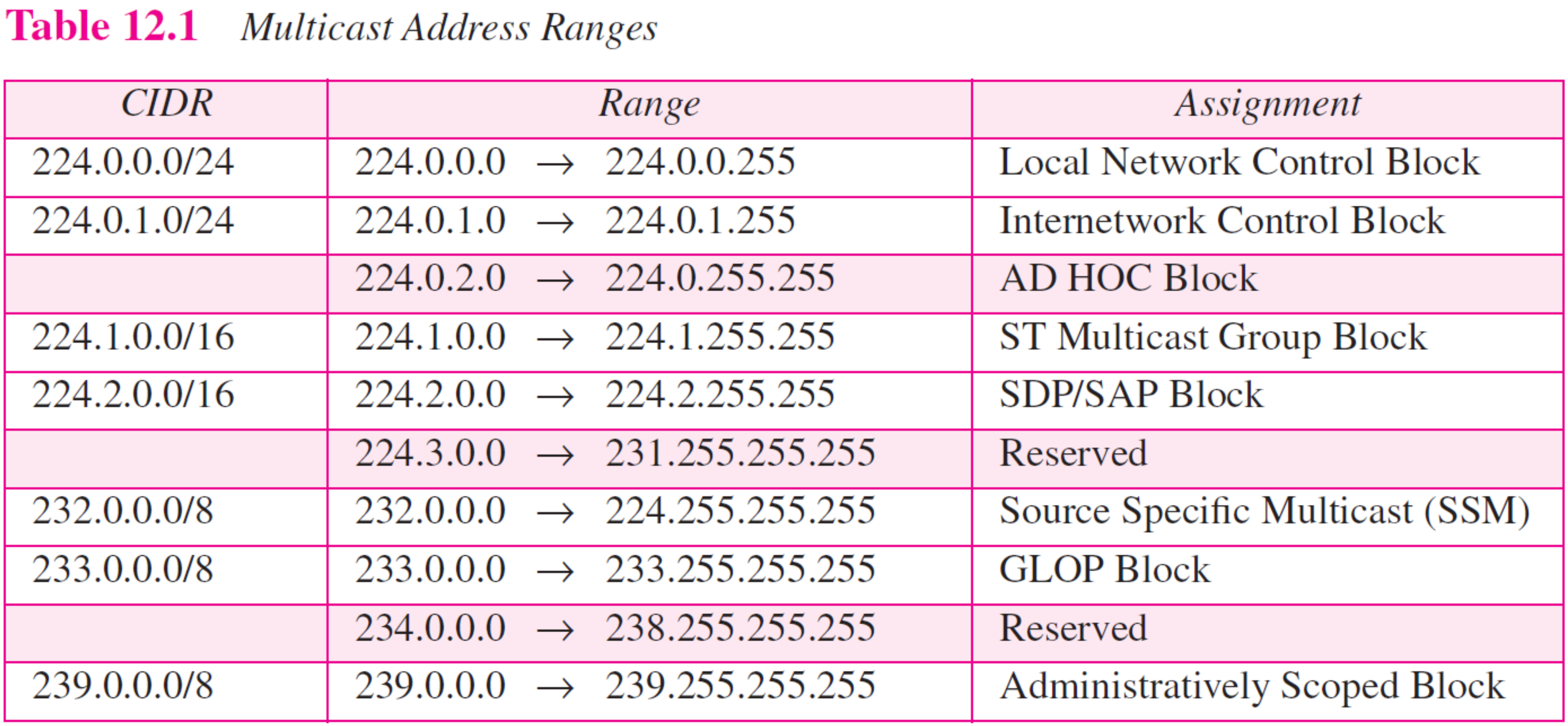


Table 12.1 *Multicast Address Ranges*

CIDR	*Range*	*Assignment*
224.0.0.0/24	224.0.0.0 → 224.0.0.255	Local Network Control Block
224.0.1.0/24	224.0.1.0 → 224.0.1.255	Internetwork Control Block
	224.0.2.0 → 224.0.255.255	AD HOC Block
224.1.0.0/16	224.1.0.0 → 224.1.255.255	ST Multicast Group Block
224.2.0.0/16	224.2.0.0 → 224.2.255.255	SDP/SAP Block
	224.3.0.0 → 231.255.255.255	Reserved
232.0.0.0/8	232.0.0.0 → 224.255.255.255	Source Specific Multicast (SSM)
233.0.0.0/8	233.0.0.0 → 233.255.255.255	GLOP Block
	234.0.0.0 → 238.255.255.255	Reserved
239.0.0.0/8	239.0.0.0 → 239.255.255.255	Administratively Scoped Block

Sub blocks

Local Network Control Block.

The subblock 224.0.0.0/24 is assigned to a multicast routing protocol to be used inside a network, which means that the packet with a destination address in this range cannot be forwarded by a router.

the address 224.0.0.0 is reserved,

the address 224.0.0.1 is used to send datagrams to all hosts and routers inside a network

the address 224.0.0.2 is used to send datagrams to all routers inside a network

Sub blocks

Internetwork Control Block.

The subblock 224.0.1.0/24 is assigned to a multicast routing protocol to be used in the whole Internet, which means that the packet with a destination address in this range can be forwarded by a router.

Source-Specific Multicast (SSM) Block.

The block 232.0.0.0/8 is used for source-specific multicast routing.

Sub blocks

GLOP Block.

The block 233.0.0.0/8 is called the GLOP block.

This block defines a range of addresses that can be used inside an autonomous system (AS).

Each autonomous system is assigned a 16-bit number.

One can insert the AS number as the two middle octets in the block to create a range of 256 multicast addresses (233.x.y.0 to 233.x.y.255), in which x.y is the AS number.

Sub blocks

Administratively Scoped Block.

The block 239.0.0.0/8 is called the Administratively Scoped Block.

The addresses in this block are used in a particular area of the Internet.

The packet whose destination address belongs to this range is not supposed to leave the area.

In other words, an address in this block is restricted to an organization.

Selecting Multicast Address

Limited Group

The administrator can use the AS number (x.y) 256 and choose an address between 239.x.y.0 and 239.x.y.255 (Administratively Scoped Block), that is not used by any other group, as the multicast address for that particular group.

For example, assume college professors need to create group addresses to communicate with their students.

If the AS number that the college belongs to is 23452, which can be written as (91.156) 256 , this gives the college a range of 256 addresses: 233.91.156.0 to 233.91.156.255.

The college administration can grant each professor one of the addresses in the range.

This can then become the group address for the professor to use to send multicast communications to the students. However, the packets cannot go beyond the college AS territory.

Selecting Multicast Address

Larger Group

If the group is spread beyond an AS territory, the previous solution does not work.

The group needs to choose an address from the SSM block (232.0.0.8).

There is no need to get permission to use an address in this block, because the packets in source-specific multicasting are routed based on the group and the source address; they are unique.

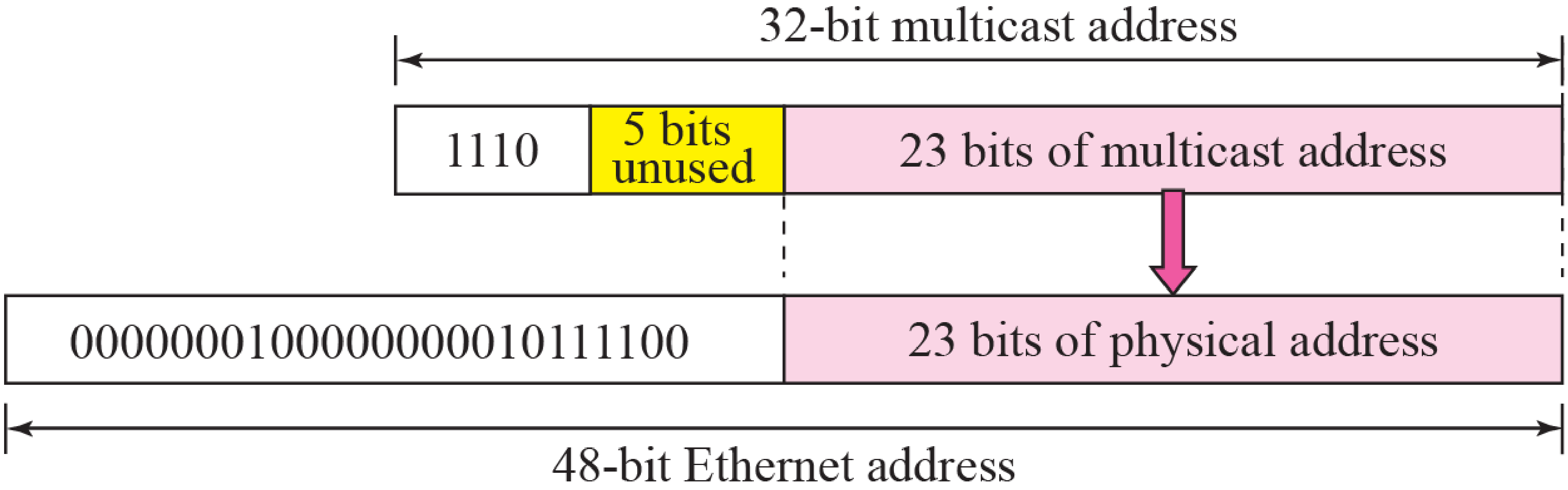
Delivery at Data-Link Layer

- In multicasting, the delivery at the Internet level is done using network-layer multicast addresses .
- Data-link layer multicast addresses are also needed to deliver a multicast packet encapsulated in a frame.
- In the case of unicasting, this task is done by the ARP protocol, but, because the IP packet has a multicast IP address, the ARP protocol cannot find the corresponding MAC (physical) address to forward a multicast packet at the data-link layer.

Network with Multicast Support

- LANs support physical multicast addressing.
- An Ethernet physical address (MAC address) is six octets (48 bits) long.
- If the first 25 bits in an Ethernet address are 00000001 00000000 01011110 0, this identifies a physical multicast address for the TCP/IP protocol.
- The remaining 23 bits can be used to define a group.
- To convert an IP multicast address into an Ethernet address
- The multicast router extracts the least significant 23 bits of a multicast IP address and inserts them into a multicast Ethernet physical address

Mapping class D to Ethernet physical address



Note

An Ethernet multicast physical address is in the range
01:00:5E:00:00:00
to
01:00:5E:7F:FF:FF.

Exercise

Change the multicast IP address **232.43.14.7** to an Ethernet multicast physical address.

Solution

Extract rightmost 23 bits of the IP address in hexadecimal.

the result is **2B:0E:07**.

We add the result of part a to the starting Ethernet multicast address, which is **01:00:5E:00:00:00**

The result is **01:00:5E:2B:0E:07**

Exercise

Change the multicast IP address **238.212.24.9** to an Ethernet multicast physical address.

Solution

Extract rightmost 23 bits of the IP address in hexadecimal.

the result is **54:18:09**.

We add the result of part a to the starting Ethernet multicast address, which is **01:00:5E:00:00:00**

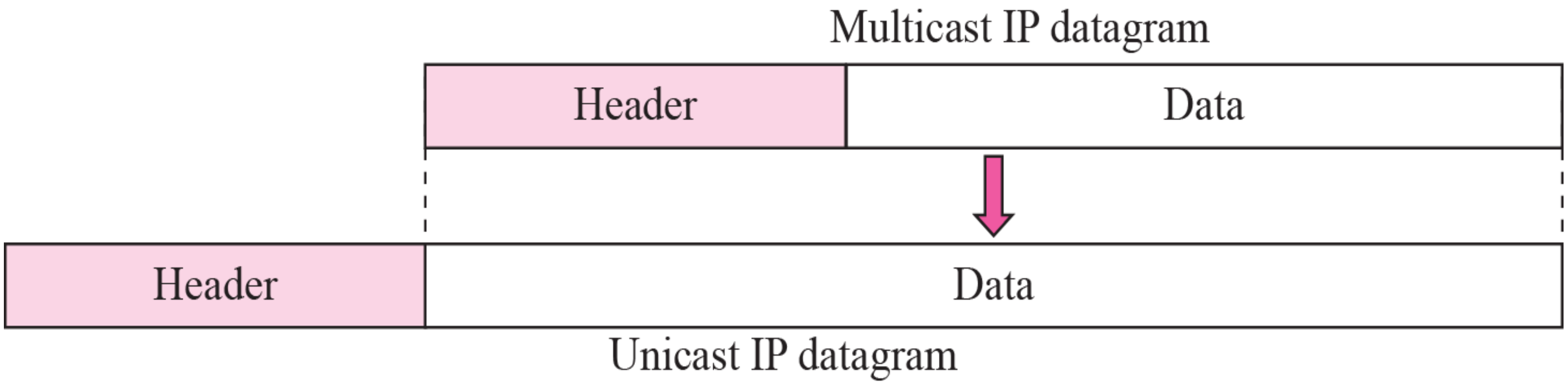
The result is **01:00:5E:54:18:09**

Network with No Multicast Support

Most WANs do not support physical multicast addressing.

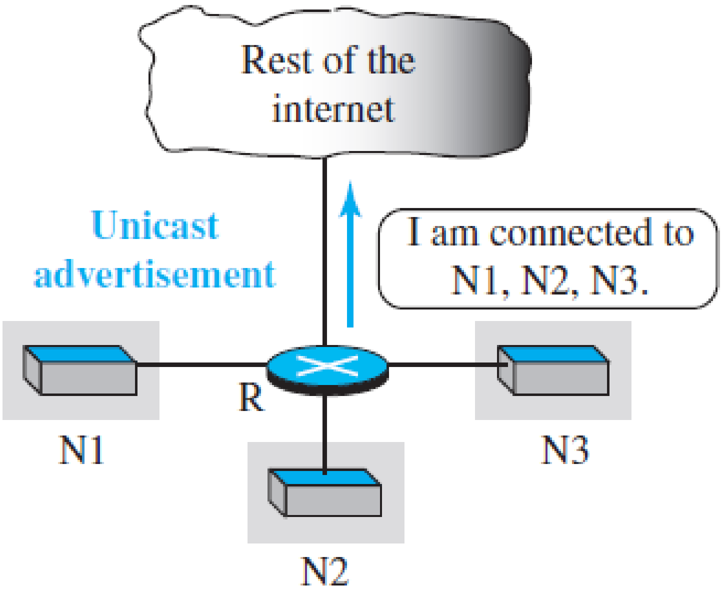
To send a multicast packet through these networks, a process called tunneling is used.

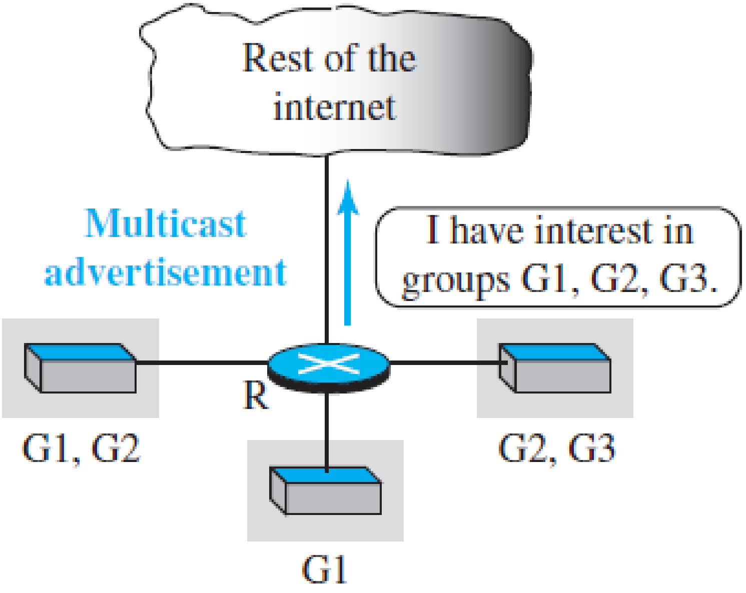
In tunneling, the multicast packet is encapsulated in a unicast packet and sent through the network, where it emerges from the other side as a multicast packet



Collecting Information about Groups

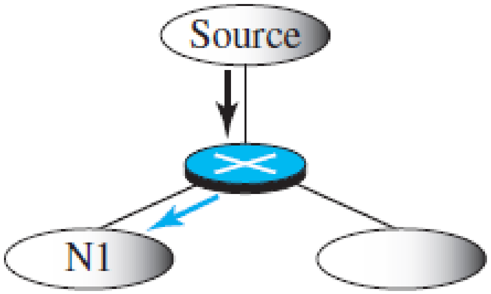
- In Unicast routing v/s In multicast routing. A router needs help to find out which groups are active in each of its interfaces.
- Multicasting we need two protocols:
  - one to collect these pieces of information and the next to propagate them.
- Collecting pieces of information is done by the Internet Group Management Protocol (IGMP),



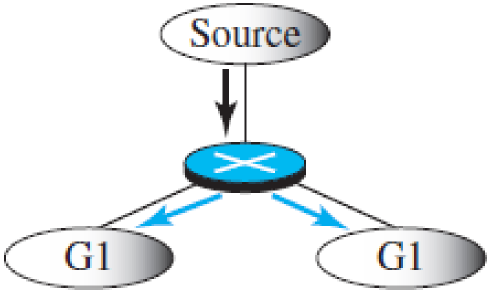


Multicast Forwarding

- Important issue in multicasting is the decision a router needs to make to forward a multicast packet.
- Forwarding in Unicast and multicast communication is different in two aspects:
- In multicast communication, the destination of the packet defines one group, but that group may have more than one member in the internet. To reach all of the destinations, the router may have to send the packet out of more than one interface.

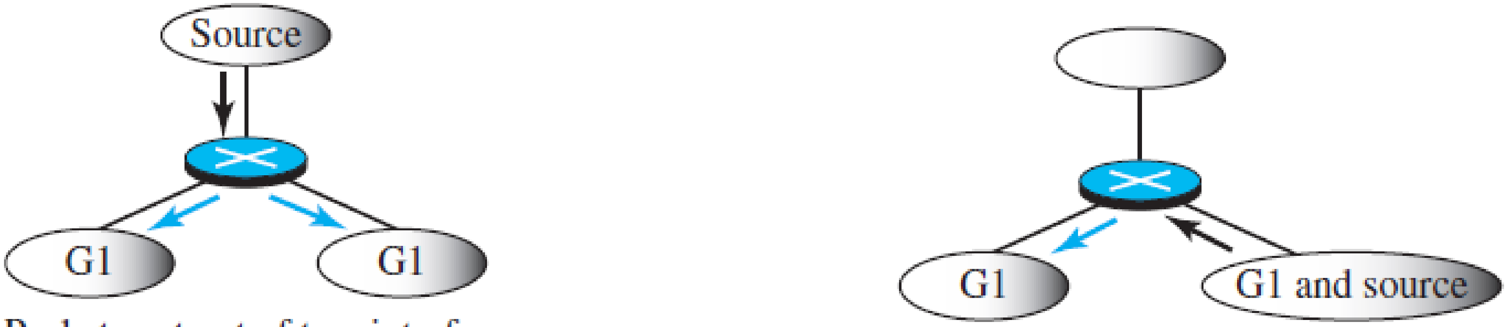


a. Destination in unicasting is one



b. Destination in mulicasting is more than one

- Second , Forwarding decisions,
  - Unicast communication depend only on the destination address of the packet.
  - In multicast communication depend on both the destination and the source address of the packet



a. Packet sent out of two interfaces

b. Packet sent out of one interface

Two Approaches to Multicasting

- In multicast routing, as in Unicast routing.
- Multicast routing decision at each router depends not only on the destination of the packet, but also on the source of the packet.
- Two different approaches
  - Source-based trees
  - Group-shared trees.

Source-Based Tree Approach

- Each router needs to create a separate tree for each source-group combination.
- if there are ***m groups*** and ***n sources*** *in the internet.*
- A router needs to create ($m \times n$) *routing trees.*
- In each tree , the corresponding source is the root, the members of the group are the leaves and the router itself is somewhere on the tree.
- Here each router needs to create and store a huge amount of information about several trees

Group-Shared Tree Approach

- In the group-shared tree approach, we designate a router to act as the phony source for each group.
- The designated router, which is called the **core** router or the **rendezvous** point router, acts as the representative for the group.
- Any source that has a packet to send to a member of that group sends it to the core center (unicast communication) and the core center is responsible for multicasting.
- Group-shared tree approach, only the core router, which has a shortest path tree for each group, is involved in multicasting.
- There are m core routers (one for each group) and each core router has a routing tree, for the total of m trees.

Group-Shared Tree Approach

- A multicast delivery from the source to all group members is divided into two deliveries.
- The first is a unicast delivery from the source to the core router; the second is the delivery from the core router to all group members.
- Note that the first part of the delivery needs to be done using tunneling.
- The multicast packet created by the source needs to be encapsulated in a unicast packet and sent to the core router.
- The core router decapsulates the unicast packet, extracts the multicast packet, and sends it to the group members.
- Although the reduction in number of trees in this approach looks very attractive, this approach has its own overhead

INTRADOMAIN MULTICAST PROTOCOLS

- we discuss three protocols.
- Two are extensions of unicast routing protocols (RIP and OSPF), using the source-based tree approach;
- the third is an independent protocol which is becoming more and more popular.
- It can be used in two modes, employing either the source-based tree approach or the shared-group tree approach.

Multicast Distance Vector (DVMRP)

- The Distance Vector Multicast Routing Protocol (DVMRP) is the extension of the Routing Information Protocol (RIP) which is used in unicast routing. (flood-and-prune)
- It uses the source-based tree approach to multicasting.
- It creates a source-based multicast tree in three steps:
  - The router uses an algorithm called reverse path forwarding (RPF) to simulate creating part of the optimal source-based tree between the source and itself.
  - The router uses an algorithm called reverse path broadcasting (RPB) to create a broadcast (spanning) tree whose root is the router itself and whose leaves are all networks in the internet.
  - The router uses an algorithm called reverse path multicasting (RPM) to create a multicast tree by cutting some branches of the tree that end in networks with no member in the group.

Reverse Path Forwarding (RPF)

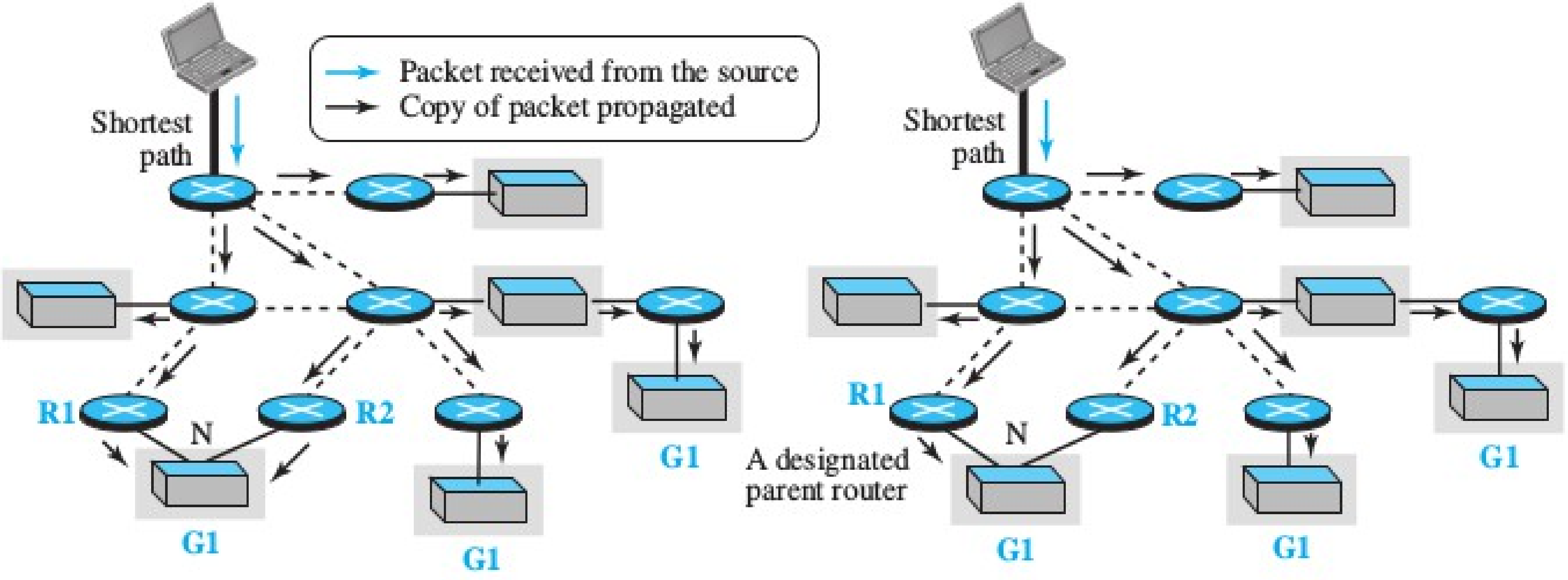
- Router to forward a multicast packet from one specific interface.
- The one which has come through the shortest path from the source to the router.
- How can a router know which interface is in this path if the router does not have a shortest-path tree rooted at the source?
- Solution : The first property of the shortest-path tree.
- the shortest path from A to B is also the shortest path from B to A.

Reverse Path Forwarding (RPF)

- The router does not know the shortest path from the source to itself, but it can find which is the next router in the shortest path from itself to the source (reverse path).
- The router simply consults its unicast forwarding table, pretending that it wants to send a packet to the source; the forwarding table gives the next router and the interface the message that the packet should be sent out in this reverse direction.
- The router uses this information to accept a multicast packet only if it arrives from this interface.

Reverse Path Broadcasting (RPB)

- RPF guarantees that each network receives a copy of the multicast packet but not loops. (Problem of RPF.)
- One router as the parent of a network related to a specific source.
- Several ways that the parent of the network related to a network can be selected;
  - router that has the shortest path to the source
  - router with the smaller IP address
- RPB actually creates a broadcast tree from the graph that has been created by the RPF algorithm.
- RPB has cut those branches of the tree that cause cycles.


Packet received from the source
Copy of packet propagated
Shortest path
R1
R2
N
G1
G1
G1
Shortest path
R1
R2
N
A designated parent router
G1
G1
G1
G1

a. Using RPF, N receives two copies.

b. Using RPB, N receives only one copy.

Reverse Path Multicasting (RPM)

- RPB does not multicast the packet, it broadcasts it.
- This is not efficient. To increase efficiency, the multicast packet must reach only those networks that have active members for that particular group.
- This is called reverse path multicasting (RPM).
- To change the broadcast shortest-path tree to a multicast shortest-path tree, each router needs to prune (make inactive) the interfaces that do not reach a network with active members corresponding to a particular source-group combination.

Pruning

- The designated parent router of each network is responsible for holding the membership information (through IGMP) .
- The router sends a prune message to the upstream router so that it can prune the corresponding interface.
- That is, the upstream router can stop sending multicast message for this group through that interface