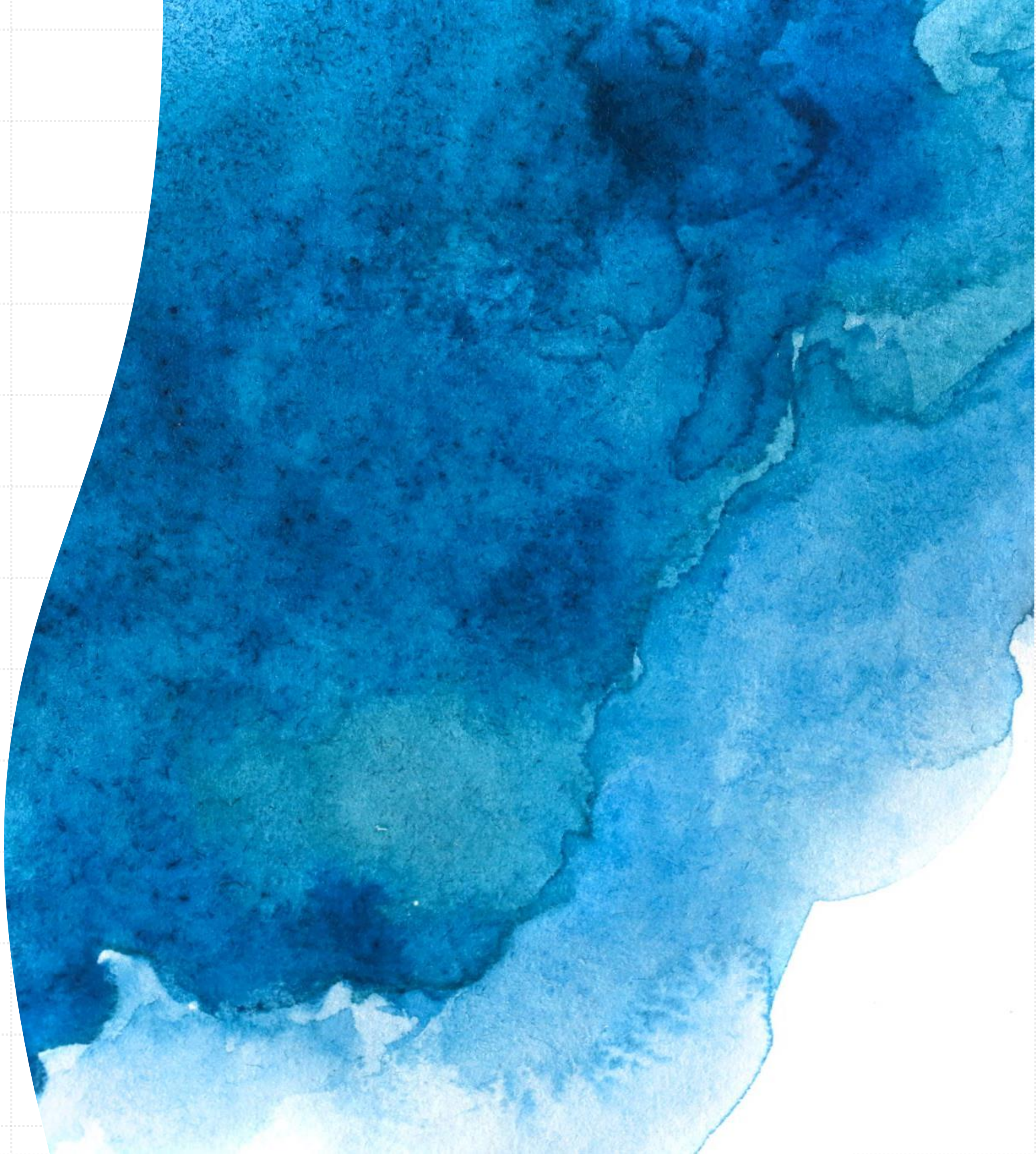
# Multicasting

Internetworking with TCP/IP

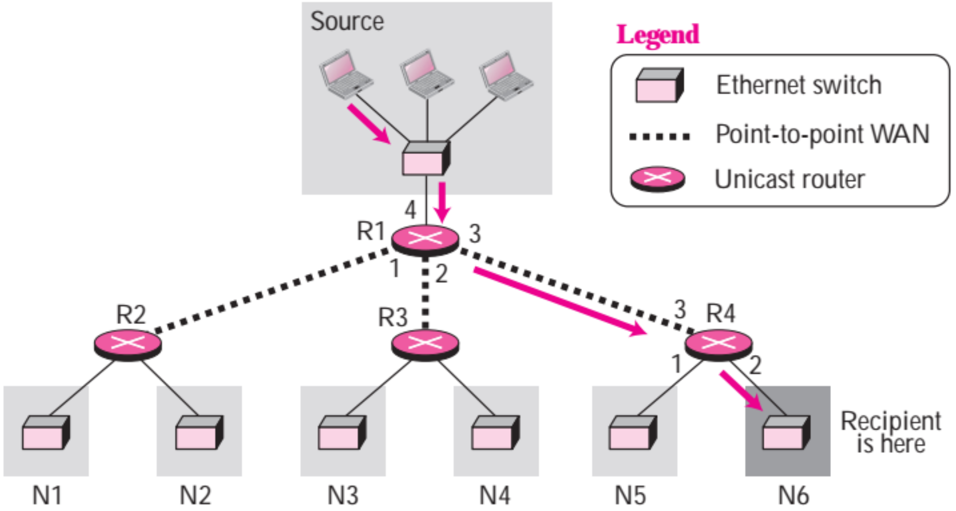
Ref: TCP/IP Protocol Suite

*Chapter 12: Multicasting and Multicast Routing Protocols*



# Unicasting

- One source, one destination (relationship between source and destination: one to one)
- Each router tries to forward the packet to one and only one of its interfaces

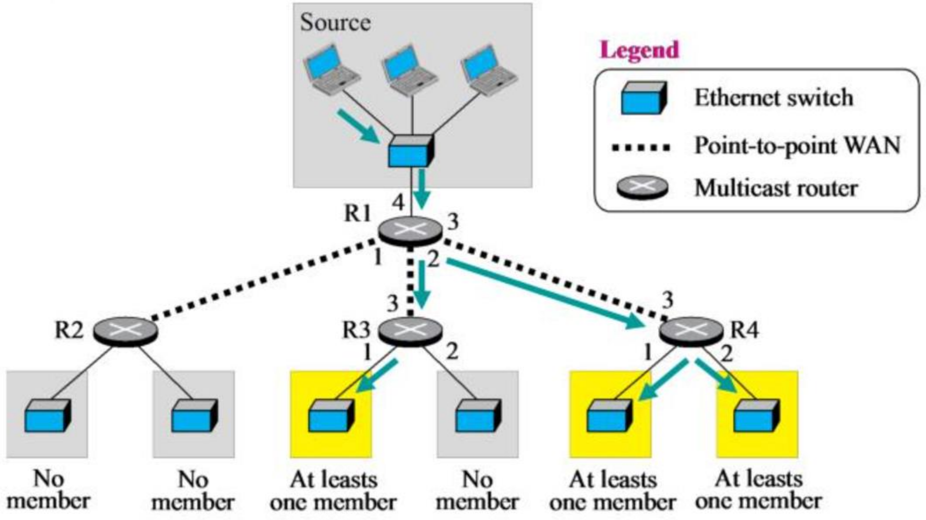


- Router R1: forward the packet only through interface 3;
- Router R4: forward the packet only through interface 2;
- When the packet arrives to N6, the delivery to the destination host is the responsibility of the network;
- *it is either broadcasted to all hosts or the smart Ethernet switch delivers it only to the destination host*

# Multicasting

- One source, and a group of destinations (relationship between source and destination: one to many)
- The source address is a unicast address - destination address is a group address: a group of one or more destination networks in which *there is at least one member of the group that is interested in receiving the multicast datagram.*
- The group address defines the members of the group.
- A multicast router may have to send out copies

of the same datagram through more than one interface.



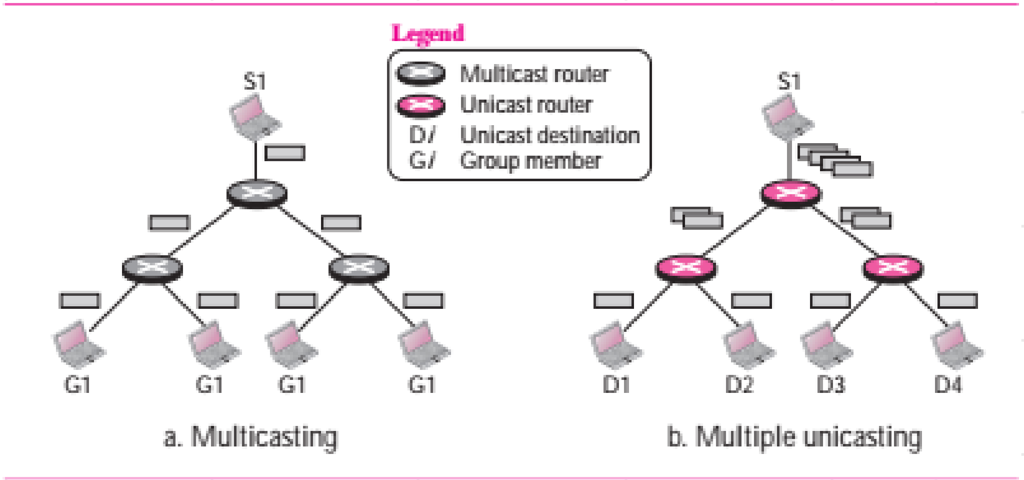
# Multicasting versus Multiple Unicasting

Multicasting

- starts with a single packet from the source that is duplicated by the routers.
- The destination address in each packet is the same for all duplicates.
- only one single copy of the packet travels between any two routers

Multiple unicasting:

- several packets starts from the source.
- For ex. If there are four destinations, the source sends
- 4 packets, each with a different unicast destination address.
- there may be multiple copies traveling between two routers



# Emulation of Multicasting with Unicasting

Why do we need multicasting

- Multicasting is more efficient than multiple unicasting – it requires less bandwidth than multiple unicasting.
- In multiple unicasting, the packets are created by the source with a relative delay between packets.
- If there are 1,000 destinations, the delay between the first and the last packet may be unacceptable.
- In multicasting, there is no delay because only one packet is created by the source

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

# Multicast Applications

- Access to Distributed Databases
  - Information is stored in more than one database.
  - The user does not know the location of the information
  - A request is multicast to all the database locations-location that has information responds.
- Information Dissemination
  - If the nature of the information is same, businesses can multicast messages to rich many customers
- Dissemination of News
  - One single message can be sent to those interested in particular topic.
- Teleconferencing
  - involves multicasting
  - Individuals attending a conference all need to receive the same information at the same

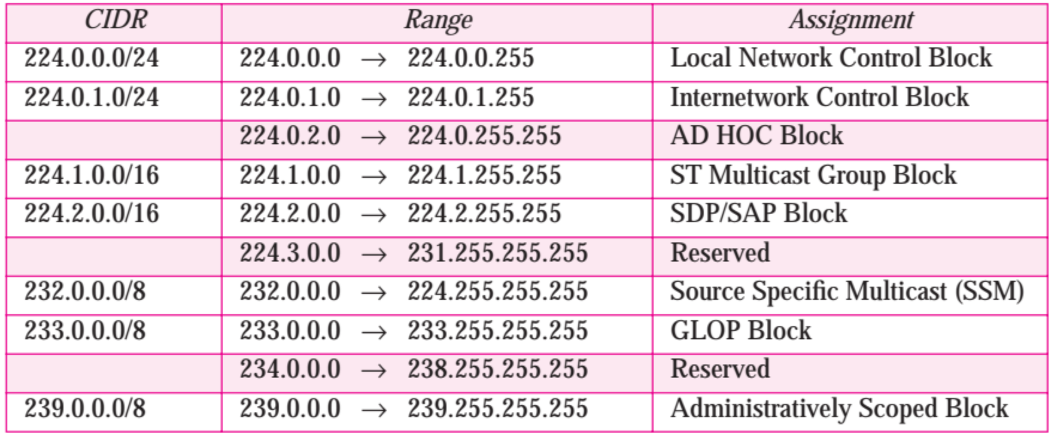
# Broadcasting

- The relationship between the source and the destination is one to all.
- Only one source, but all of the other hosts are the destinations.
- Internet does not explicitly support broadcasting because of the huge amount of traffic it would create and because of the bandwidth it would need.

# Multicast Addresses

- In classful addressing, multicast addresses occupied the only single block in Class D.
- In classless addressing, the same block has been used for this purpose.
- Multicast Address: a destination address for a group of hosts that have joined a multicast group.
- A packet that uses a multicast address as a destination can reach all members of the group unless there are some filtering restrictions by the receiver.
- The block assigned for multicasting is 224.0.0.0/24

**Table 12.1** *Multicast Address Ranges*



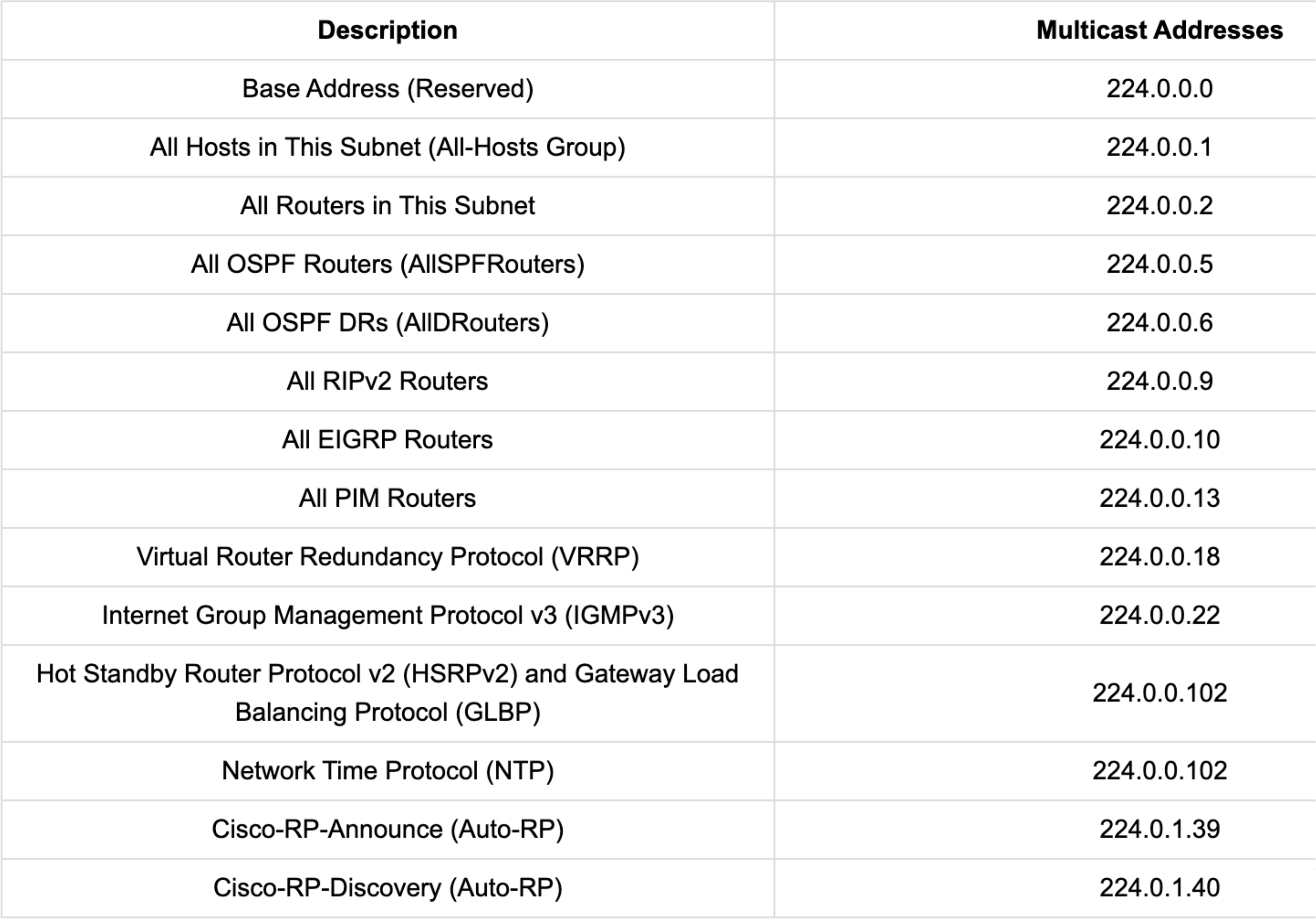
| *CIDR* | *Range* | *Assignment* |
|---|---|---|
| 224.0.0.0/24 | 224.0.0.0 → 224.0.0.255 | Local Network Control Block |
| 224.0.1.0/24 | 224.0.1.0 → 224.0.1.255 | Internetwork Control Block |
| | 224.0.2.0 → 224.0.255.255 | AD HOC Block |
| 224.1.0.0/16 | 224.1.0.0 → 224.1.255.255 | ST Multicast Group 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 |

# Multicast Addresses

- Local Network Control Block:
  - First block (224.0.0.0 – 224.0.0.255) – addresses are used for protocol control traffic
  - Not used for general multicast communication
  - The IP packets with the destination address in this range need to have the value of TTL set to 1.
  - The packet remains in the network, meaning two or more networks can use the same address simultaneously.
- Internetwork Control Block:
  - Block 224.0.1.0/24
  - Addresses in this block are used for protocol control traffic
  - IP packets with one of these addresses as the destination can be forwarded by a router through the whole Internet

# Multicast Addresses

- **some of the well-known multicast addresses from the local network and internetwork control blocks**



| Description | Multicast Addresses |
|---|---|
| Base Address (Reserved) | 224.0.0.0 |
| All Hosts in This Subnet (All-Hosts Group) | 224.0.0.1 |
| All Routers in This Subnet | 224.0.0.2 |
| All OSPF Routers (AllSPFRouters) | 224.0.0.5 |
| All OSPF DRs (AllDRouters) | 224.0.0.6 |
| All RIPv2 Routers | 224.0.0.9 |
| All EIGRP Routers | 224.0.0.10 |
| All PIM Routers | 224.0.0.13 |
| Virtual Router Redundancy Protocol (VRRP) | 224.0.0.18 |
| Internet Group Management Protocol v3 (IGMPv3) | 224.0.0.22 |
| Hot Standby Router Protocol v2 (HSRPv2) and Gateway Load Balancing Protocol (GLBP) | 224.0.0.102 |
| Network Time Protocol (NTP) | 224.0.0.102 |
| Cisco-RP-Announce (Auto-RP) | 224.0.1.39 |
| Cisco-RP-Discovery (Auto-RP) | 224.0.1.40 |

# Multicast Addresses

**AD-HOC Block:**

- Block – 224.0.2.0 to 224.0.255.255
- Historically, addresses in this range have been assigned to applications that do not that don't fit either of the previously described purposes
- These addresses are **globally routed**

**ST Multicast Group Protocol:**

- Block 224.1.0.0/16 – allocated for the Internet Stream protocol (ST)
- ST protocol is an experimental resource reservation protocol intended to provide end-to-end real-time guarantees.
- It allows applications to build multi-destination simplex data streams with a desired Qos.

# Multicast Addresses

## Administratively Scoped Block (RFC 2365)

- **(239.0.0.0/8)**
- This address block is confined to a single local group or organisation.
- These addresses will not be assigned by the IANA to other protocols or groups.
- Network administrators can use this range within their domain without conflicting with others anywhere on the Internet.
- The packet whose destination address belongs to this range is not supposed to leave the area.

# Selecting Multicast Addresses

- Not an easy task – the selection of an address depends on the type of application.

**Limited Group:**

- Administrators can use the AS number (x.y) and choose an address between 239.x.y.0 and 239.x.y. 255 that is not used by any other group.
- For example: *a college AS number is 91.156, so the college administration can assign 239.91.156.47 – a group address assigned to the college professor*.
- The Packets can not go beyond the college AS territory.

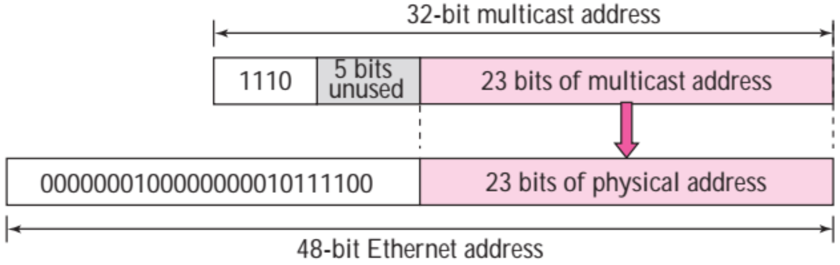
**Larger Group:**

- If the group is spread beyond AS territory, the previous solution does not work.
- The group needs to choose an address from the SSM block (232.0.0.0/8)

# Delivery of Multicast Packets at the Data Link Layer

- ARP can not find the corresponding MAC(physical) address to forward the packet at DLL as IP Packets have multicast IP addresses.

- Network with Multicast Support:
  - Most LANs including ethernet support physical multicast addressing.



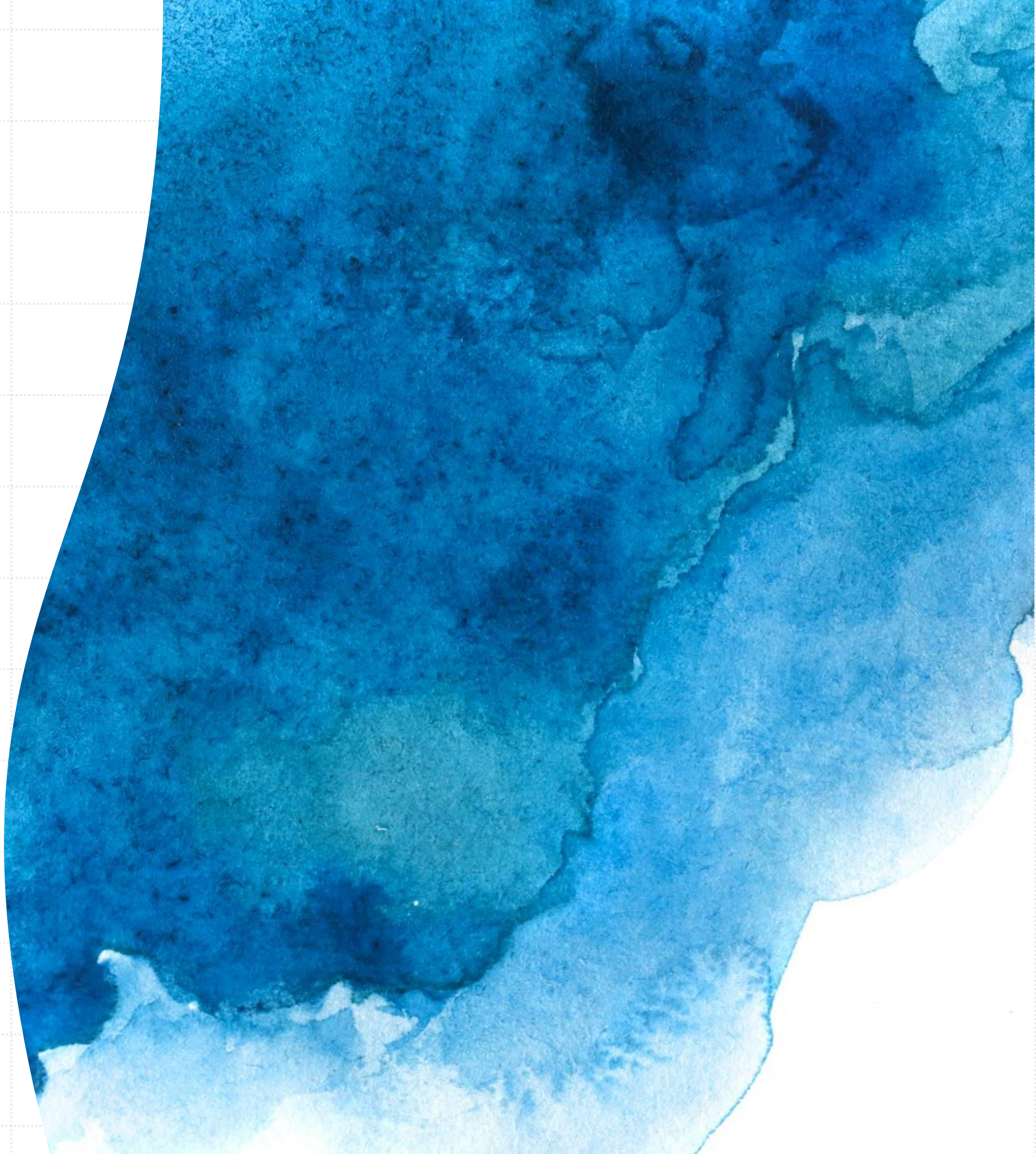
To convert an IP multicast address into an ethernet address, the multicast router extracts the LSB (23) and inserts them into a multicasr ethernet physical address.

# Delivery of Multicast Packets at Data Link Layer

.Network with No Multicast Support:

- Most WANs do not support physical multicast addressing
- Tunneling is used to send multicast packets through these networks
- Tunneling: a packet is encapsulated in a unicast packet and sent through the network.

# IGMP protocol



# Introduction to IGMP

- Multicast communication means that a sender sends a message to a group of recipients that are members of the same group.
- Each multicast router needs to know the list of groups that have at least one loyal member related to each interface.
- Collection of this type of information is done at two levels: locally and Globally
- The first task is done by IGMP (Internet Group Management Protocol);
- The second task is done by multicast routing protocols

# Introduction to IGMP

- IGMP is not a multicast routing protocol; it is a protocol that manages group membership.
- IGMP protocol allows the multicast routers to create and update a list of loyal members related to each router interface.
- IGMP is responsible for collecting information about group members in a network. i.e. , the IGMP protocol gives the multicast routers information about the membership status of the routers connected to the network.
- It helps the multicast routers create and update a list of loyal members related to each router interface.

# Introduction to IGMP

- IGMP has three versions.
- Versions 1 and 2 provide what is called as any-source multicast (ASM), which means that group members receive a multicast message no matter where it comes from.
- Version 3: provide SSM (Source Specific Multicast) – recipient can choose to receive multicast messages coming from a list of predefined sources.

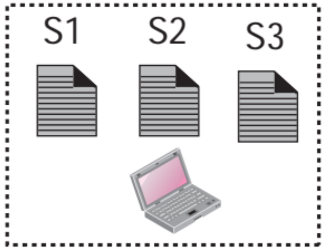
# IGMP Messages

Two types of messages:

- Membership query message
- Sent by a router to find active group members in the network
  - Can be used in three different formats: general, group-specific, group and source - specific
  - General query message: router probes each neighbour to report the whole list of its group membership (interest in any multicast group) For ex.- "Who is in your multicast group?"
  - Group-specific query message: the router probes each neighbour to report if it is still interested in a specific multicast group. For ex.- "Are you still interested in multicast group X?"
  - Source- Specific message: used to check if a specific router is still interested in a multicast group X when the data is sourced from a specific source S. For ex. - "Are you still interested in multicast group X from source S?"
- Membership report message

# IGMP Protocol Applied to the Host

- Management of a group starts with the process (running application programs) on a host connected to an interface.
- Each process (associated with a socket) has a record for each multicast group from which the socket receives a multicast messages.
- include – only these source addresses
- Exclude: all but… (socket will not accept the message from these states)

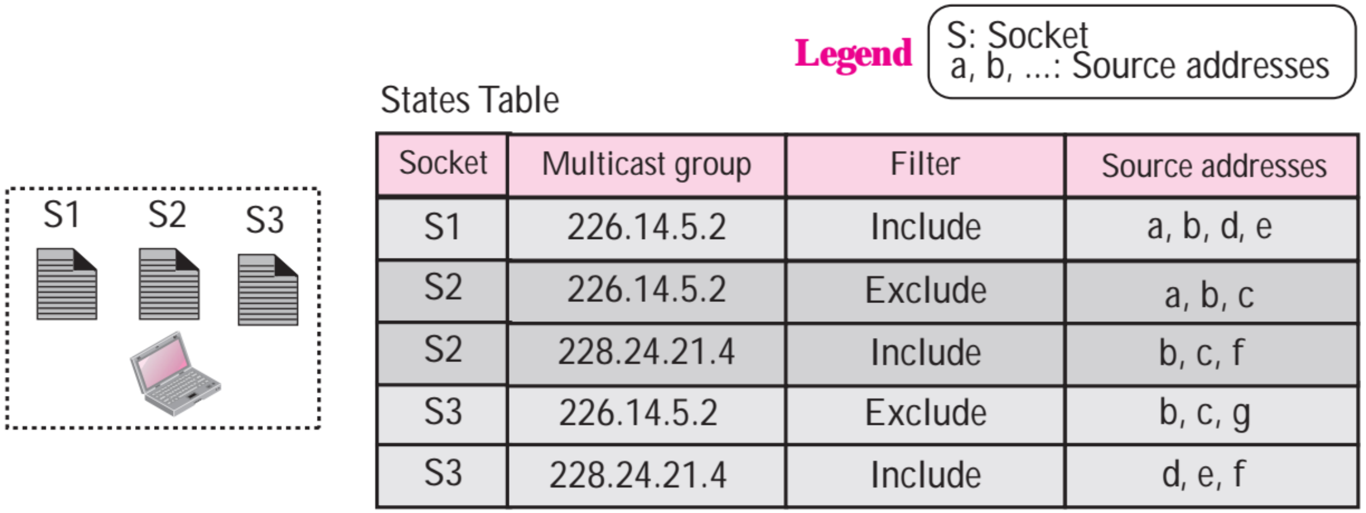


Legend
S: Socket
a, b, ….: Source addresses

States Table

| Socket | Multicast group | Filter | Source addresses |
|---|---|---|---|
| S1 | 226.14.5.2 | Include | a, b, d, e |
| S2 | 226.14.5.2 | Exclude | a, b, c |
| S2 | 228.24.21.4 | Include | b, c, f |
| S3 | 226.14.5.2 | Exclude | b, c, g |
| S3 | 228.24.21.4 | Include | d, e, f |

# IGMP Protocol Applied to the Host

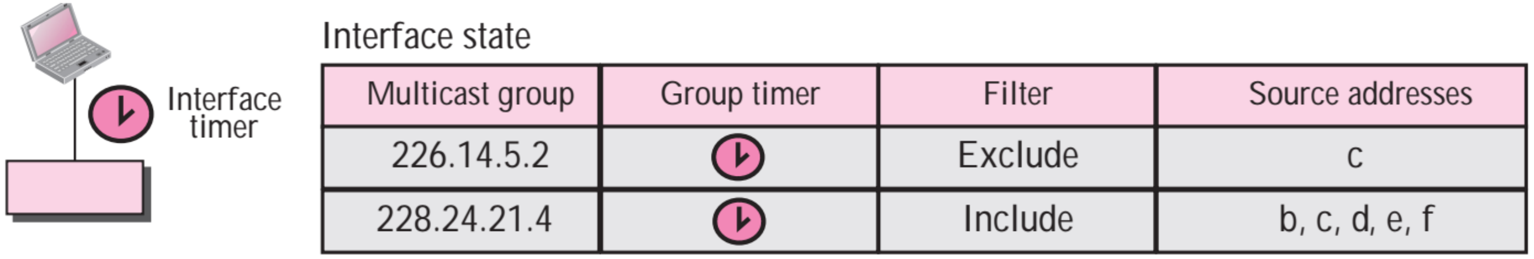


Legend: S: Socket; a, b, ...: Source addresses

States Table

| Socket | Multicast group | Filter | Source addresses |
|---|---|---|---|
| S1 | 226.14.5.2 | Include | a, b, d, e |
| S2 | 226.14.5.2 | Exclude | a, b, c |
| S2 | 228.24.21.4 | Include | b, c, f |
| S3 | 226.14.5.2 | Exclude | b, c, g |
| S3 | 228.24.21.4 | Include | d, e, f |

- There is some overlap in the socket records – two or more sockets may have a record with the same multicast group.
- So, we need to remove the overlap and combine the record. - only two records with different multicast address.

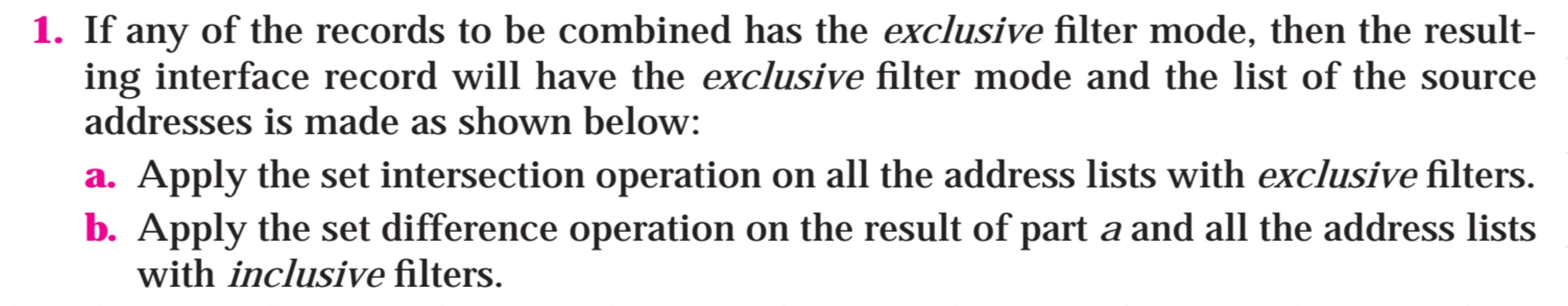


Interface state

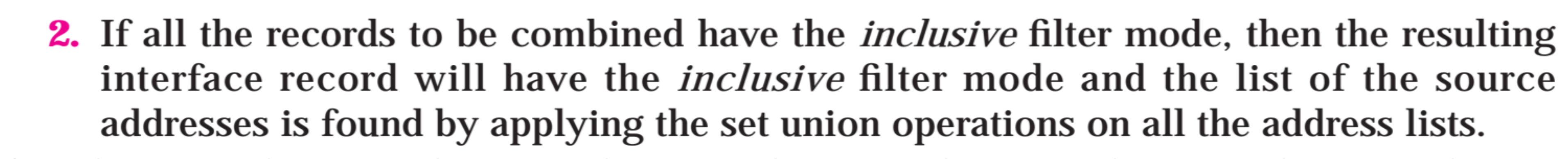
| Multicast group | Group timer | Filter | Source addresses |
|---|---|---|---|
| 226.14.5.2 | 🕒 | Exclude | c |
| 228.24.21.4 | 🕒 | Include | b, c, d, e, f |

# IGMP Protocol Applied to the Host

- If a record with the same multicast group has two or more different list of resources, the following two rules need to be followed:

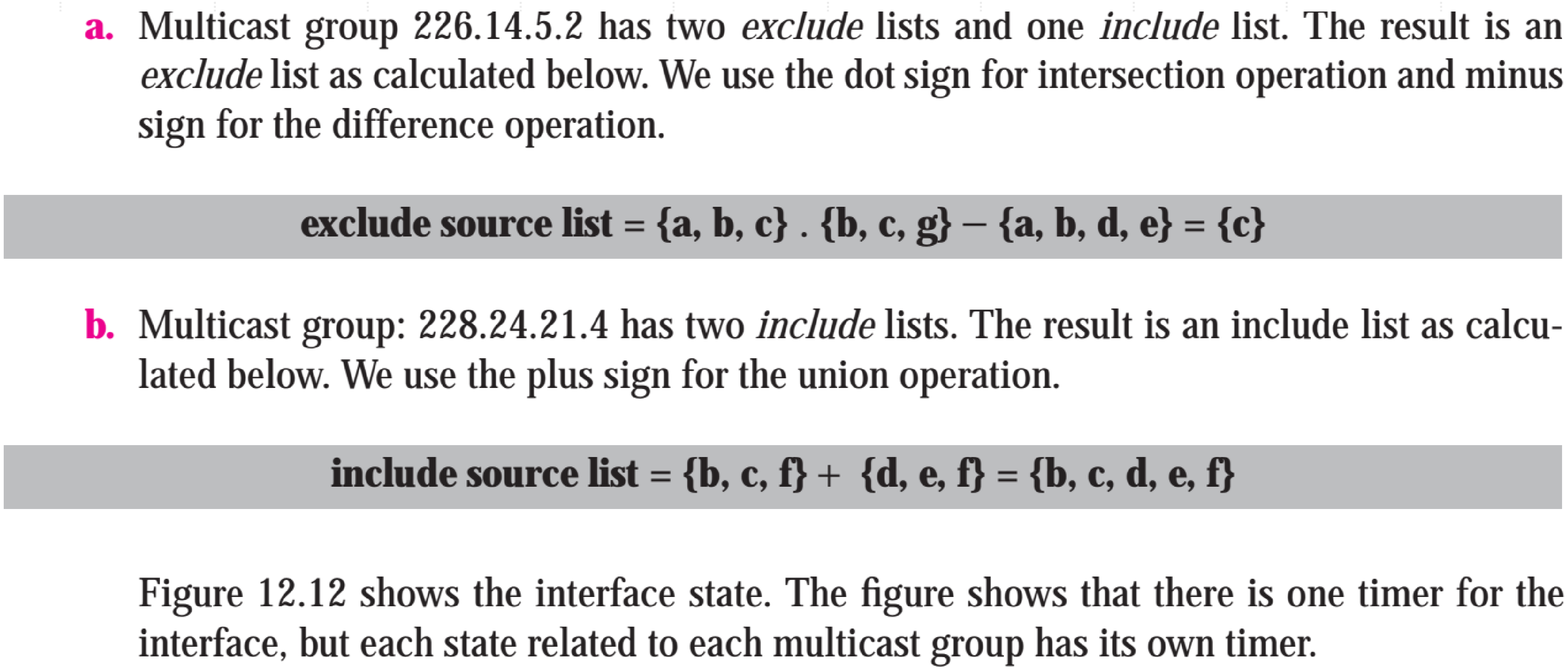


1. If any of the records to be combined has the *exclusive* filter mode, then the resulting interface record will have the *exclusive* filter mode and the list of the source addresses is made as shown below:
    a. Apply the set intersection operation on all the address lists with *exclusive* filters.
    b. Apply the set difference operation on the result of part *a* and all the address lists with *inclusive* filters.



2. If all the records to be combined have the *inclusive* filter mode, then the resulting interface record will have the *inclusive* filter mode and the list of the source addresses is found by applying the set union operations on all the address lists.

# IGMP Protocol Applied to the Host



**a.** Multicast group 226.14.5.2 has two *exclude* lists and one *include* list. The result is an *exclude* list as calculated below. We use the dot sign for intersection operation and minus sign for the difference operation.

**exclude source list** = {a, b, c} . {b, c, g} − {a, b, d, e} = {c}

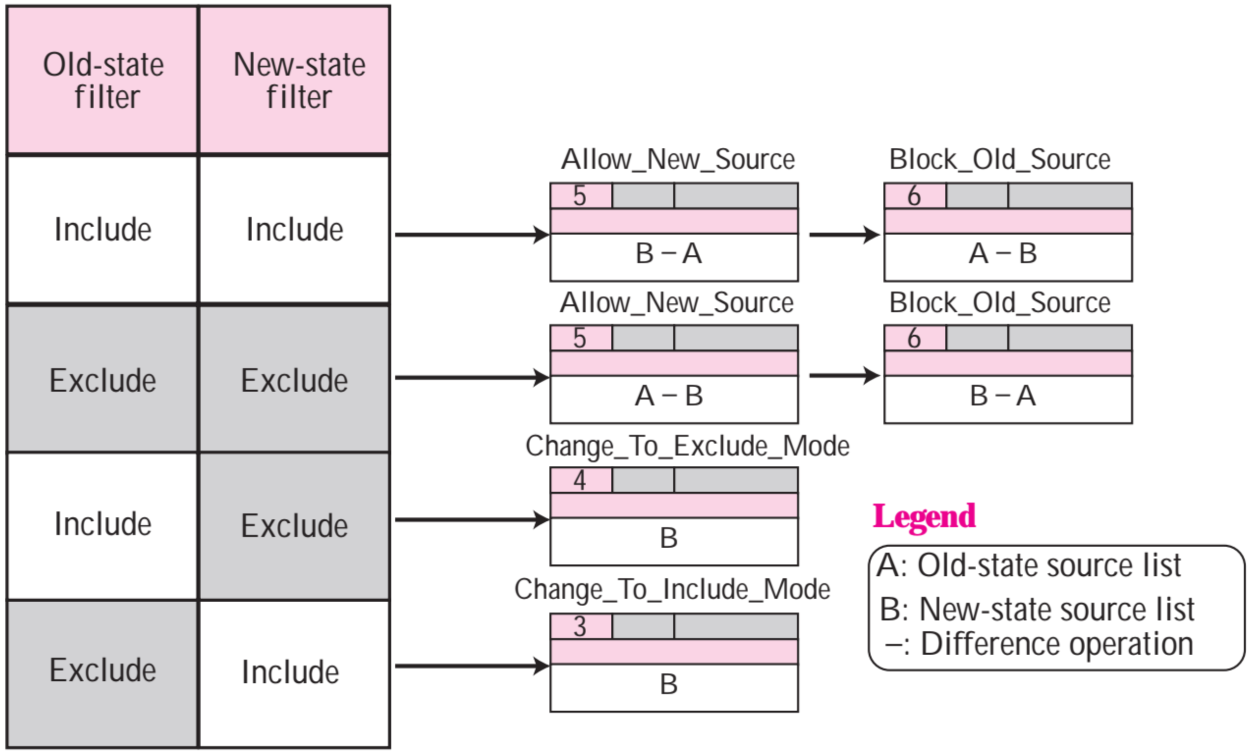
**b.** Multicast group: 228.24.21.4 has two *include* lists. The result is an include list as calculated below. We use the plus sign for the union operation.

**include source list** = {b, c, f} + {d, e, f} = {b, c, d, e, f}

Figure 12.12 shows the interface state. The figure shows that there is one timer for the interface, but each state related to each multicast group has its own timer.

# Sending Change-State reports

- If there is any change in the interface state, the host needs to immediately send a membership report message for that group, using the appropriate group record(s)



| Old-state filter | New-state filter |
|---|---|
| Include | Include |
| Exclude | Exclude |
| Include | Exclude |
| Exclude | Include |

**Legend**

A: Old-state source list
B: New-state source list
−: Difference operation

# Receiving Query Reports

- When a host receives a query, it does not respond immediately; it delays the response by a random amount of time calculated from the value of the Max Resp Code field.

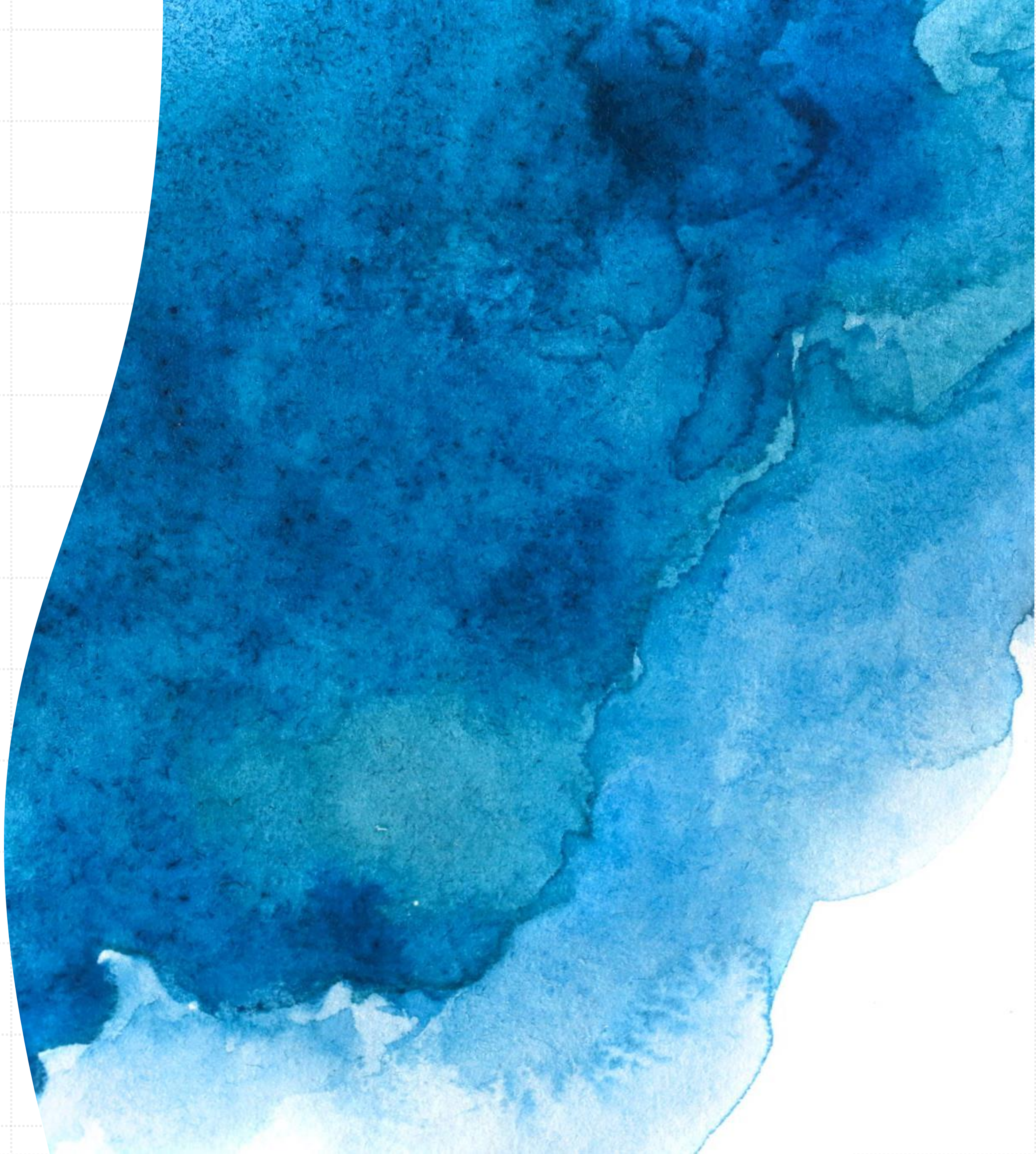
The action of the host depends on the type of the query received, as shown below:

1. If the received query is a general query, the host reset the interface timer (see Figure 12.12) to the calculated delay value. This means if there is any previous delayed response, it is cancelled.

2. If the received query is a group-specific query, then the corresponding group time (see Figure 12.12) is reset to the shorter value of the remaining time for the timer or the calculated delay. If a timer is not running, its remaining time is considered to be infinity.

3. If the received query is a group-and-source-specific query, then the action is the same as the previous case. In addition, the list of sources is recorded for the delayed response.

# Multicast Routing Protocols



# Multicast Routing

- Optimal Routing – a process of finding the shortest path tree – root of the tree: source and leaves: potential destinations
- The number of trees and the formation of trees in unicast and multicast routing is different
- Unicast Routing:
  - Each line of the routing table is a shortest path - next hop entry corresponding to the destination is the start of the shortest path.
  - The whole routing table is a shortest path tree.

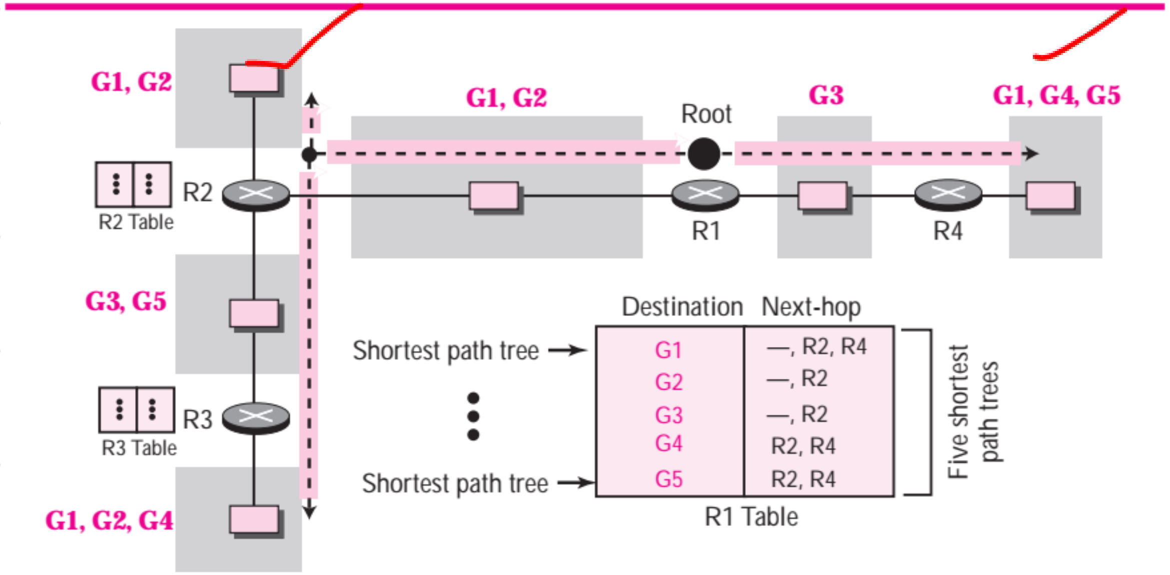
# Multicast Routing

- The situation is different when a router receives a multicast packet.
- A multicast packet may have destinations in more than one network.
- Forwarding a single packet to members of a group requires a shortest path tree.
- N group – need n shortest-path trees.
- Approaches used to solve this problem are:
  - Source-based trees ✓
  - Group-shared trees

# Source-based Tree

- Each router needs to have one shortest path tree for each group.
- The shortest path tree for a group defines the next hop for each network that has loyal members for that group.

**Figure 12.19** *Source-based tree approach*



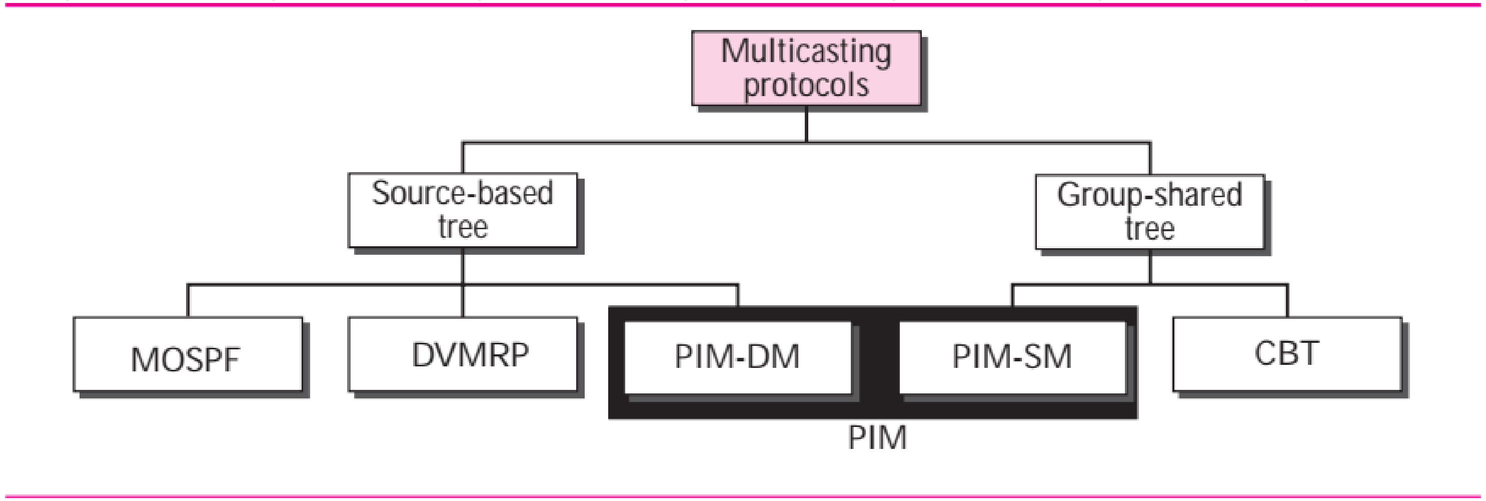
| Destination | Next-hop |
|---|---|
| G1 | —, R2, R4 |
| G2 | —, R2 |
| G3 | —, R2 |
| G4 | R2, R4 |
| G5 | R2, R4 |

R1 Table

# Group-Shared Tree

- Only one designated router, called the centre core, rendezvous router, takes the responsibility of distributing multicast traffic.
- Core has m shortest path trees in its routing table. The rest of the routers in the domain have none.
- If a router receives a multicast packet, it encapsulates the packet in a unicast packet and sends it to the core router.
- The core router removes the multicast packet from its capsule and consults its routing table to route the packet

# Routing Protocols



# Multicast Link State Routing: MOSPF

- a direct extension of unicast routing and uses a source-based tree approach. (each router creates a shortest path tree using Dijkstra's Algorithm)
- A node needs to revise the interpretation of the state.
- A node advertises every group that has any loyal member on the link.
- The meaning of state here is "what groups are active on this link"
- Each router running IGMP solicits the hosts on the link to find out the membership status.
-

# Multicast Link State Routing: MOSPF

- When a router receives all these LSPs, it creates n (n is the number of groups) topologies, from which n shortest path trees are made using Dijkstra algo.
- Each router has a routing table representing as many shortest path trees as groups.
- Problem: Time and space are needed to create and save the shortest path trees.
- Solution: create only when needed.
- When a router receives a packet with a multicast destination address, it runs the Dijkstra algorithm to calculate the shortest path for that group. (**On-Demand Calculation)**
- **Caching for Optimisation:**
  - Once calculated, the tree can be stored in cache memory for future use by the same source and group pair, optimising performance.

# Multicast Distance Vector (DVMRP)

- Unicast distance vector routing is simple; extending it to support multicast routing is complicated.
- When a router receives a multicast packet, it forwards the packet as though it is consulting a routing table.
- Destroys the routing table when the work is done.

**Operation of Multicast Distance Vector Routing:**

- Instead of transmitting routing tables, multicast distance vector routing creates tables from scratch using information from unicast distance vector tables.
- It employs source-based trees for routing, where routers forward multicast packets based on these dynamic tree structures.

# Multicast Distance Vector (DVMRP)

**Evanescent Nature of Shortest Path Trees:**

- The routing tables in multicast distance vector routing are evanescent—they are transient and destroyed after forwarding a packet.

**Decision-Making Strategies:**

- Multicast distance vector algorithm employs four decision-making strategies.
- Each strategy builds upon its predecessor to improve routing efficiency and address limitations encountered in the previous strategies.
  - Flooding
  - Reverse Path Forwarding ✓
  - Reverse Path Broadcasting
  - Reverse Path Multicasting

# Flooding

*Upon receiving a packet, the router sends it out from every interface except the one it received it from.*

**Outcome:**

- Ensures every network with active members receives the packet, fulfilling multicasting's initial goal

**Drawbacks:**

- Networks without active members also receive the packet, resembling a broadcast rather than a true multicast.
- Creates loops where packets may re-enter the router and get forwarded multiple times.

**Loop Prevention:**

- Some flooding protocols retain a packet copy briefly and discard duplicates to prevent loops.
- The next strategy, reverse path forwarding, corrects this defect

# Reverse Path Forwarding(RPF)

RPF is an enhancement over basic flooding to prevent loops in multicast routing.

- Ensures only one copy of a packet is forwarded, dropping others to avoid redundancy and potential loops.

**Path Selection:**

- Upon receiving a multicast packet, the router extracts the source address (unicast address).
- Consults its unicast routing table to determine the next hop towards the source address as if it were sending a unicast packet.
- **Shortest Path Verification:**
- If the incoming interface matches the shortest path indicated in the routing table for the source address, the packet is considered to have travelled the shortest path.
- In unicast distance vector protocols, the shortest path is reciprocal; thus, the same path used from A to B is shortest from B to A.

# Reverse Path Forwarding(RPF)

**Loop Prevention:**

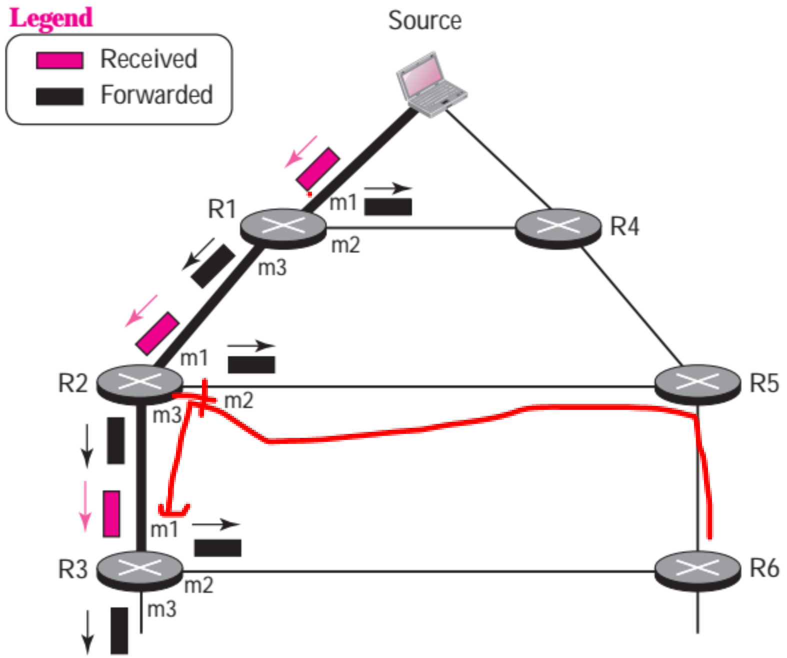
The router forwards the multicast packet only if it arrived via the shortest path indicated in the unicast routing table.

If the packet returns to the router from a different path, it indicates a loop and is discarded.

**Effectiveness:**

- **Guaranteed Loop Prevention:**
  - RPF ensures loops are prevented by consistently forwarding packets along the shortest path identified through the unicast routing table.
  - Maintains efficient multicast packet delivery by avoiding unnecessary duplication and network congestion caused by loops.

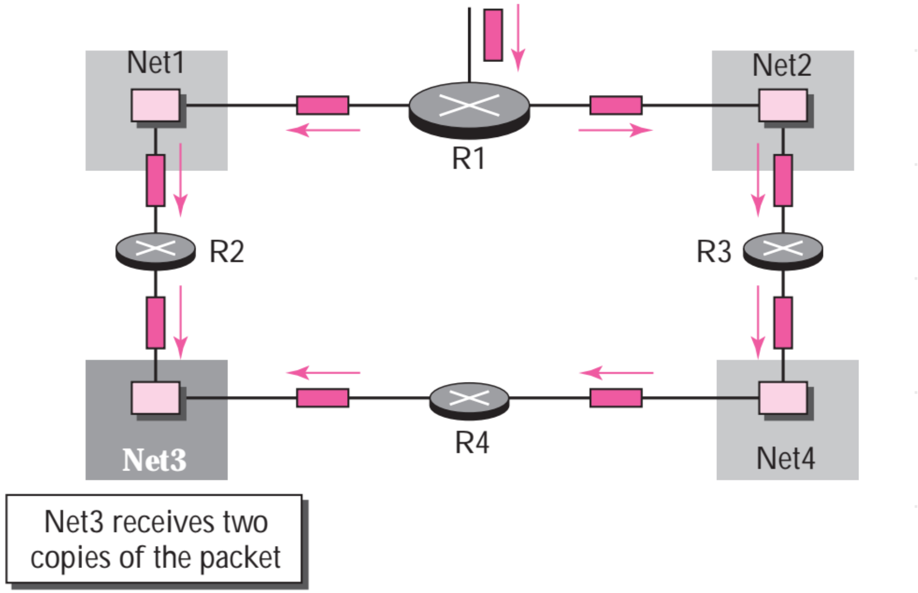
# Reverse Path Forwarding(RPF)



- When R1 receives a packet from a source – consults its routing table – finds that shortest path from R1 to the source is through m1.
- If a copy of the packet is arrived through m2, then discarded? Because m2 does not define the shortest path from R1 to the source.
- Suppose a copy arrives at R3 interface m1, via R6, R5, R2. Is that copy forwarded?
- Scenario never happens because when the packet comes at R2 from R5– discarded because not gone through the shortest path

# Reverse Path Broadcasting (RPB)

- RPF guarantees that each network receives a copy of the multicast packet without the formation of loops.
- However, RPF does not guarantee that each network gets only one copy;
- A network may receive two or more copies.

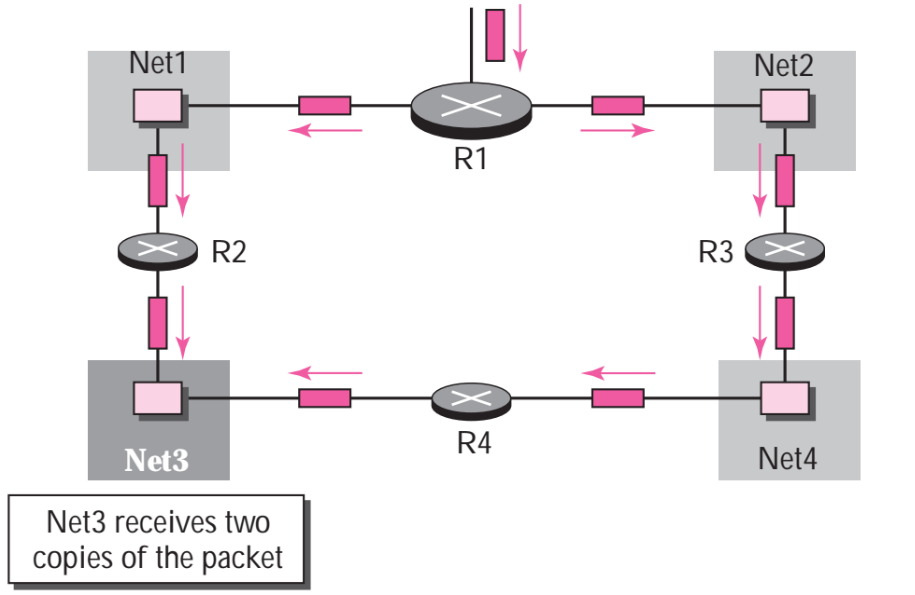


Net3 receives two copies of the packet

- The reason is that RPF is not based on the destination address (a group address); forwarding is based on the source address

# Reverse Path Broadcasting (RPB)

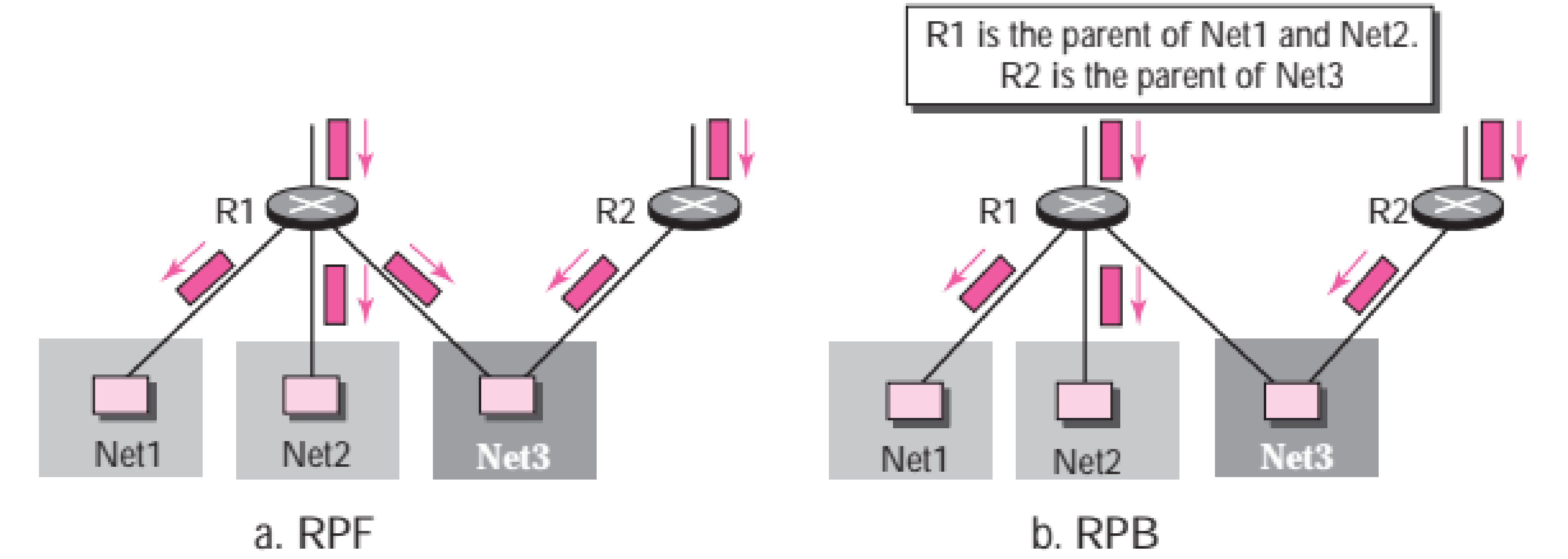
- Net3 has two parents R2 and R4.
- To remove duplication, only one parent router for each network.
- Restrictions should be made: *a network can only receive packets from a particular source through a designated router.*



Net3 receives two copies of the packet

# Reverse Path Broadcasting (RPB)

**Figure 12.24** *RPF versus RPB*



a. RPF

b. RPB

- For each source, the router sends the packet only out of those interfaces for which it is the designated parent.
- RPB guarantees that the packet reaches every n/w and every network receives only one copy.

# Reverse Path Broadcasting (RPB)

- How is the designated router parent determined?

- Routers send update packets to each other.

- They can easily determine which router in the neighbourhood has the shortest path to the destination (when interpreting the source as the destination)

- If more than one router qualifies, the router with the smallest IP address is selected.

# Reverse Path Multicasting

- RPB is not efficient as it broadcasts the packet.
- So, the multicast packet must reach only those networks that have active members from that particular group – reverse path multicasting.

- To convert broadcasting to multicasting, two procedures are used:
- Pruning ✓
- Grafting ✓

# Reverse Path Multicasting – Pruning

- The designated parent router of each network is responsible for holding the membership information.
- This is done through **the IGMP protocol**.
- The process starts:
  - When a router connected to a network finds no interest in a multicast packet.
  - The router sends a prune message to the upstream router to prune the corresponding interface – the upstream router can stop sending multicast messages for this group through that interface.

*If this router receives prune messages from all downstream routers, it, in turn, sends a prune message to its upstream router*

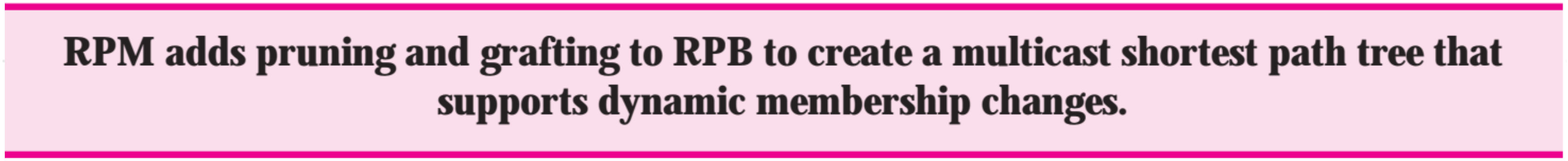
# Reverse Path Multicasting – Grafting

*What if a leaf router (a router at the bottom of the tree) has sent a prune message but suddenly realizes, through IGMP, that one of its networks is again interested in receiving the multicast packet?*

Solution:

- It can send a graft message.
- The graft message forces the upstream router to resume sending the multicast message

# Reverse Path Multicasting



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

# Core-based Tree (CBT) Protocol

- A group-based tree protocol - uses a core as the root of the tree.
- Autonomous systems are divided into regions, and a core is chosen for each router.

- Formation of the Tree
- Sending Multicast Packets
- Selecting the Rendezvous Router (not to be discussed)

# Core-based Tree (CBT) Protocol

- Rendezvous Point (RP) selection initiates the process.
- Each router is informed of the unicast address of the selected RP.

**Joining the Group**

- Routers with interest send a unicast join message (similar to a grafting message) to join the group.
- The message travels through routers between the sender and the RP.
- Intermediate routers extract the sender's unicast address and arrival interface, forwarding the message.

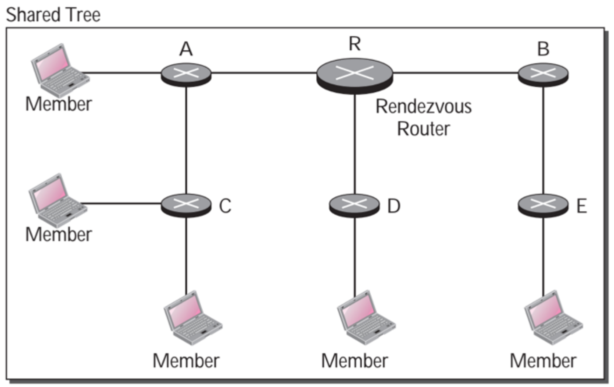
**Tree Formation**

- RP collects join messages from all group members.
- Tree formation: routers know upstream (to root) and downstream (to leaf) routers.

# Core-based Tree (CBT) Protocol

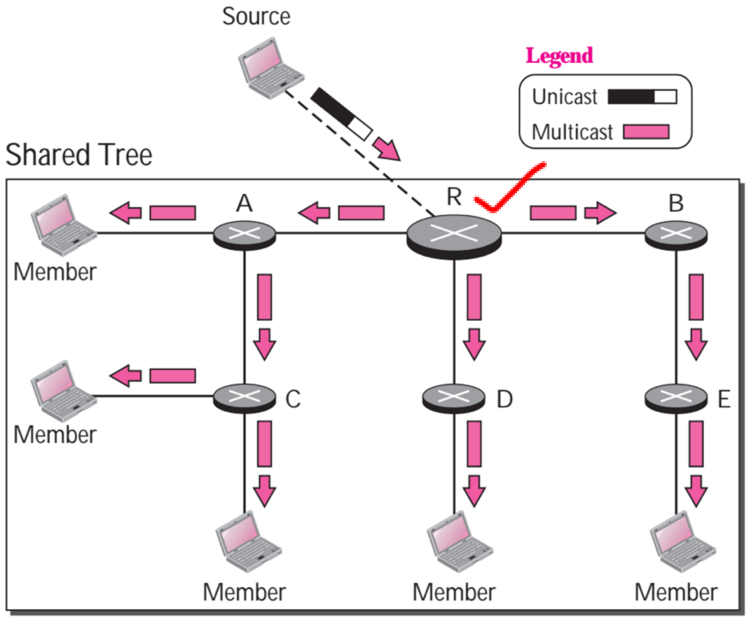
- **Leaving the Group**
  - Router sends leave message to upstream router.
  - Upstream router removes link from tree, forwards leave message.
- **Comparison with DVMRP and MOSPF**
  - Tree formation: DVMRP and MOSPF from root up, CBT from leaves down.
  - Difference in approach: DVMRP (broadcast, then prune); CBT (gradual tree formation).

**Figure 12.26** *Group-shared tree with rendezvous router*



# Core-based Tree (CBT) Protocol

- **Sending Multicast Packets**
- **After the formation of the tree, any source (belonging to the group or not) can send a multicast packet to all group members.**
- **It simply sends the packet to the rendezvous router, using the unicast address of the rendezvous router; the rendezvous router distributes the packet to all members of the group.**
- **Note that the source host can be any of**



# Core-based Tree (CBT) Protocol

- **Summary**

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

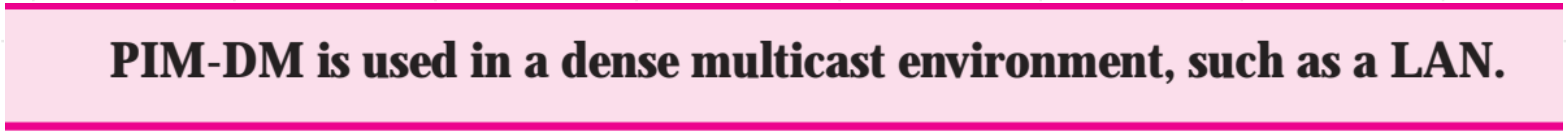
- The source, which may or may not be part of the tree, encapsulates the multicast packet inside a unicast packet with the unicast destination address of the core and sends it to the core.
- This part of the delivery uses a unicast address; the only recipient is the core router.
- The core decapsulates the unicast packet and forwards it to all interested interfaces.
- Each router that receives the multicast packet, in turn, forwards it to all interested interfaces.

# Protocol Independent Multicast (PIM)

- Name given to two independent multicast routing protocols
- Protocol Independent Multicast Dense Mode (PIM-DM) ✓
- Protocol Independent Multicast Sparse Mode (PIM-SM)

# PIM-DM

- PIM-DM is a source-based tree routing protocol that uses RPF and pruning/grafting strategies for multicasting.
- Its operation is like DVMRP; however, unlike DVMRP, it does not depend on a specific unicasting protocol.
- It assumes that the autonomous system is using a unicast protocol and each router has a table that can find the outgoing interface that has an optimal path to a destination. This unicast protocol can be a distance vector protocol (RIP) or link state protocol (OSPF).



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

# PIM-SM

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

- PIM-SM is a group-shared tree routing protocol that has a rendezvous point (RP) as the source of the tree.
- Its operation is like CBT; however, it is simpler because it does not require acknowledgment from a join message.
- In addition, it creates a backup set of RPs for each region to cover RP failures.
- One of the characteristics of PIM-SM is that it can switch from a group-shared tree strategy to a source-based tree strategy when necessary.
- This can happen if there is a dense activity area far from the RP. That area can be more efficiently handled with a source-based rather than a group-shared tree strategy.