Chapter 3
Dynamic Routing Methods

Multicast routing protocols generally include two components, one component for communication between routers and subtending hosts, and one component for communication between routers. Sections 3.1 and 3.2 discuss methods for communication between routers and hosts, and the subsequent sections of this chapter discuss methods for communication between routers.

Many Steiner tree methods, such as the centralized KMB method described in Section 2.1 above, are applicable to multicast routing only when the set of groups, and the sets of source and receiver nodes for each group, are known a priori, and these sets are static. The methods we describe in this chapter are applicable to multicast routing when the set of groups, and the sets of source and receiver nodes, are not known a priori, or these sets are dynamic. Some of these methods will use source trees, and others will use shared trees. The basic principle of tree-based dynamic routing methods (whether for a source tree or shared tree) is that a multicast stream should not be sent to a leaf node of a tree if there are no receiver hosts subtending the node.

For example, in Figure 3.1 (which is identical to Figure 2.6), the tree for group $g$ (indicated by the heavy solid lines) extends to leaf node 7, since there are receiver hosts behind node 7. Suppose both receiver hosts behind node 7 decide to leave $g$. Then node 7 notifies its upstream neighbor, which is node 3, that traffic for $g$ should not be sent to node 7. Node 3 then removes

![Fig. 3.1 Shared tree](image-url)
Dynamic Routing Methods

arc \((3, 7)\) from its outgoing interface list (OIL) for group \(g\). This is known as \textit{pruning} node 7 from the tree. Suppose the receiver host behind node 6 also decides to leave \(g\). Then node 6 informs node 3 that traffic for \(g\) should not be sent to node 6, so arc \((3, 6)\) is deleted from the \((\ast, g)\) OIL at node 3. Now node 3 is a leaf node of the tree. Since there are no receiver hosts behind node 3 itself, then 3 informs its upstream neighbor, node 2, that traffic for \(g\) should not be sent to node 3, so node 2 deletes arc \((2, 3)\) from the \((\ast, g)\) OIL at node 2. This process continues until no further pruning can be done.

Suppose now nodes 6, 7, and 3 have been pruned from the tree for group \(g\), and a host behind node 6 decides to rejoin \(g\). First, the host informs node 6 that it is rejoining \(g\). Then node 6 must rejoin the tree, so node 6 tells node 3 to send traffic for \(g\) down to node 6, so node 3 adds arc \((3, 6)\) to its \((\ast, g)\) OIL. Finally, node 3 tells node 2 to send traffic for \(g\) down to node 3, so node 2 adds \((2, 3)\) to its \((\ast, g)\) OIL.

3.1 Internet Group Management Protocol

Once a host learns about the existence of a multicast group (e.g., through an email or web site) it uses the \textit{Internet Group Management Protocol} (IGMP) to announce its desire to join the group. A host wishing to join group \(g\) sends an IGMP \textit{membership report} to its local router. In turn, routers listen to the IGMP messages sent by hosts on a directly attached subnet, and periodically determine which multicast groups have at least one interested receiver host on the subnet. If there are multiple routers on a subnet, one of them, called the \textit{designated router}, is elected to perform these functions. To query the hosts on a subnet, IGMP uses the \textit{all-hosts} broadcast address \(224.0.0.1\) and a \textit{Time to Live} (TTL) value of 1, which means that queries are not forwarded beyond the attached subnet. Upon receiving a query, a host sends a report listing each multicast group to which it belongs. When a host first joins a group, it immediately informs its local router. This ensures that, if the host is the first group member on the subnet, it immediately receives group traffic, without waiting for a router query.

When a router on a subnet determines that there have been no locally attached hosts interested in some group \(g\) for a specified time period, the router will stop forwarding packets for \(g\) to that subnet. The drawback of this approach is that, even if none of the hosts on a subnet want traffic for \(g\), traffic will be forwarded until a specified period has elapsed, which is a waste of bandwidth and router resources. IGMP Version 2 provides a faster method to let a router know that it should stop forwarding traffic for \(g\) to a subnet: a host may inform its local router, using an IGMP \textit{leave group} message, that it does not want traffic for \(g\). Upon hearing such a message, the router will initiate a query to determine if \textit{any} host on the subnet wants traffic for \(g\);