

Routing for Mobile Hosts

Wireless hosts are often mobile, changing location over time. This mobility of a wireless host may cause the host to connect to different networks at different points of time. Mobility is not limited to wireless devices. For instance, a user may connect her laptop to different Ethernets at different times of the day. Similarly, a wireless host may not necessarily be mobile. For instance, a user may connect his desktop to a wireless network rather than a wired network (such as Ethernet). In this case, the desktop is not likely to be moved much once it has been installed. Thus, wireless connectivity and mobility are independent properties, although wireless hosts are generally more likely to be mobile.

As we have discussed previously, the IP address used for an interface connected to a particular network must include the network's address in the network part of the IP address. Such an IP address is said to be *topologically correct*. Thus, when a host disconnects from one network and connects to another network, its IP address must change so that it can be topologically correct. This creates difficulties in maintaining communication while also being mobile. In particular, consider a user that has a long-lived TCP connection. This may occur if the user is performing a large file transfer (for instance, downloading a movie) using FTP. FTP uses a TCP connection to perform the file transfer. Continuity of a TCP connection requires that the IP address of the two endpoints remain unchanged. On the other hand, topologically correct addressing requires that the IP address assigned to a mobile endpoint change when the end host moves from one network to another network. These apparently contradictory requirements cannot be satisfied without additional protocol support. *Mobile IP* provides such a functionality.

Before discussing Mobile IP, let us consider an everyday example of user mobility. In particular, consider a student who has a multi-year subscription to several magazines. This student changes his apartment every semester. How do the magazines get delivered to his new address? Ordinarily, when the student moves to a new apartment, his mail will be delivered to the old address. Fortunately, the postal office provides a *forwarding service*. To ensure that the mail will be delivered to his new address, the student can submit a *change of address* card at the post office. Thereafter, the post office will forward to the student's new address any mail that is sent to his old address. When a post office responsible for delivering mail to the old address receives a magazine for the student, the post office affixes a new address on top of the old address, and puts the magazine back in the mail system for routing to the new address. Mobile IP uses a similar mechanism to ensure that a host will continue receiving packets despite mobility.

Before proceeding further, it is worth noting that this discussion only covers the basic ideas behind mobile IP, not the exact protocol specification.

0.1 Mobile IP Terminology

In mobile IP, the role of the post offices in the above example is filled by nodes called *home agents* and *foreign agents*. Each host is associated with a *home network*, and a *home*

agent is associated with the home network. Each host (or more precisely, each interface) is assigned an IP address that is topologically correct for its home network. This address is said to be the host's *permanent address*.

From the perspective of a given host, any network other than its home network is said to be a *foreign network*. When a host is connected to a foreign network it is considered to be a *foreign host* in that network. A *foreign agent* is associated with each network, whose job is to keep track of the *foreign hosts* in that network, as we will soon discuss. When a host is connected to a foreign network, it is assigned an IP address that is topologically correct for that foreign network. This IP address is said to be the host's *foreign address* or *care-of-address* (COA).

0.2 Data Forwarding in Mobile IP

The job of a mobile host's home agent is to keep track of the *network* to which the mobile host is connected. This information can then be used for the purpose of routing packets for the mobile host. We will illustrate mobile IP by means of an example scenario. The scenario unfolds in several steps:

- Consider a mobile host MH whose permanent IP address is 130.126.142.206. The home network for MH is 130.126.142/24. The notation /24 implies that the first 24 bits of the binary representation of 130.126.142 form network part of the topologically correct addresses on this network (note that 130, 126 and 142 each correspond to 8 bits). The home agent HA1 for MH is also connected to the home network (130.126.142/24) of MH. Thus, when the mobile host MH is “home”, MH and its home agent HA1 are on the same network. Suppose that initially host MH is connected to its home network, and MH starts a TCP connection with another host referred to as a *correspondent host* (CH) with IP address 128.174.254.29. CH is thus sending IP packets to MH, with 130.126.142.206 as the destination IP address. Since MH is presently connected to its home network, the address 130.126.142.206 is topologically correct for the current network of MH. Thus, packets with destination address 130.126.142.206 will be delivered to MH by the underlying routing protocol.
- Now host MH moves, disconnecting from its home network, and connecting to the network 128.174.254/24. Topologically correct IP addresses for network 128.174.254/24 are of the form 128.174.254.*. Despite the fact that MH 130.126.142.206 is no longer connected to the network 130.126.142/24, the IP packets sent by CH continue being routed to that network, because the IP packets have destination address as 130.126.142.206. To allow these packets to reach MH at its current location, mobile IP relies on the home agent and foreign agent as follows. (Refer to Figure 1 for this discussion.)
- Each foreign agent periodically broadcasts in its network an *agent advertisement*, which is received by all the hosts on its network. When a new host joins the network, it can identify the foreign agent on receiving this advertisement. As an alternative, after

joining a new network, a mobile host may also locally broadcast a query to learn the identity of the foreign agent on that network. In our example, when our mobile host MH (with IP address 130.126.142.206) joins the foreign network, it receives an agent advertisement from foreign agent FA1 whose IP address is 128.174.254.29. This advertisement also announces the *care-of-address* (COA) that MH may use. In particular, the care-of-address may be the IP address assigned to the foreign agent itself. Let us assume that the COA will be 128.174.254.29, the foreign agent’s IP address.

On learning the IP address of the foreign agent FA1, MH sends to FA1 a registration request, which is also forwarded to the home agent of MH. The registration allows the foreign agent FA1 to learn of the presence of MH in its network, and to learn its link layer address. The registration allows the home agent HA1 to learn the care-of-address of MH.

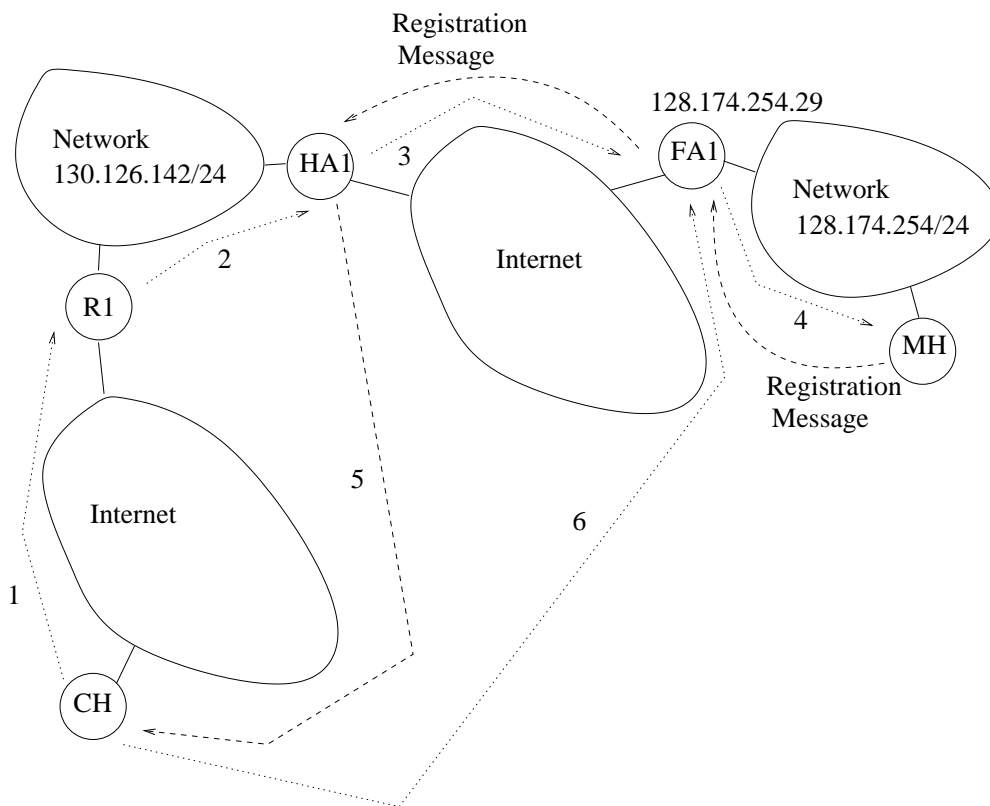


Figure 1 Registration and routing in mobile IP

- After the registration, the home agent is in a position to “re-route” the packets for MH. As a first step, after receiving the registration, the home agent ensures that it can *intercept* any packets intended for the permanent address 130.126.142.206 of MH. One mechanism to achieve this is as follows: the home agent can broadcast a *Gratuitous ARP* message on its network, which will cause other nodes on the network to associate the home agent’s link layer address with the IP address 130.126.142.206. (ARP is the abbreviation of Address Resolution Protocol.) Subsequently, any node on the home network of MH, including any routers, transmits a packet for 130.126.142.206, it will

be sent with link layer address of HA1 as the link layer receiver. Thus packets for MH sent by any correspondent host will be intercepted by the home agent (steps 1 and 2 in Figure 1).

Since the home agent is aware that MH is on a foreign network, MH can now forward the packet to the current location of MH. This is akin to the post office affixing a new address on a letter in our earlier example. In case of mobile IP, this is achieved by means of *IP-in-IP encapsulation*. Specifically, the home agent creates a new IP packet, with source IP address as its own IP address, and the destination IP address as the care-of-address of MH (namely, 128.174.254.29). The IP packet has an IP header and a body – the body of this packet consists of the original IP packet intended for 130.126.142.206. Since the IP packet is contained in this new IP packet, the protocol mechanism is called *IP-in-IP encapsulation*. In the IP header of the new packet, the protocol field specifies that the packet is IP-in-IP.

Following the underlying routing protocol, the new packet will be delivered to the foreign agent 128.174.254.29 (step 3 in Figure 1). The foreign agent will recover the original IP packet by decapsulating the received IP-in-IP packet. The recovered IP packet will then be transmitted to MH by the link layer (step 4). Recall that the link layer address of MH is known to the foreign agent due to the registration by MH.

This mechanism allows a mobile host to continue receiving packets destined to its permanent address. The packets sent by CH are routed *indirectly* via the home agent to the mobile host. This indirection allows the correspondent host to remain oblivious to the current location of the mobile host, and yet allows it to communicate with the mobile host.

Triangular Routing: The indirect routing mechanism has the shortcoming that all packets intended for MH are first routed to its home agent, and then routed to its current location, potentially resulting in a long route. This is also referred to as the *triangular routing* problem. To understand the name, visualize a triangle formed by the correspondent host, the home agent, and the mobile host. Indirect routing results in the packet traversing two sides of the triangle. Such triangular routing leads to longer delays as well as higher load on the network. This overhead can be reduced if we are willing to incorporate additional intelligence at the correspondent host (CH), to allow the packets to traverse just the third side of the above triangle (directly from CH to MH).

In particular, correspondent host CH can learn the care-of-address from the home agent HA1 (step 5 in Figure 1), and then send an IP-in-IP packet destined to foreign agent FA1, with IP destination address as 128.174.254.29, and the body of IP-in-IP packet consisting of the packet intended for MH 128.174.254.29. Thus, instead of home agent HA1, the correspondent host CH performs IP-in-IP encapsulation, and sends the packet to the current COA of MH (step 6 in Figure 1).