CHAPTER 10

Mobile IP

Adrian Farrel

Today's computers are smaller and more mobile than they once were. Processing power that used to take up a whole air-conditioned room can now be easily carried around and used anywhere. At the same time, connectivity to the Internet has become easier and more diverse. A user may now disconnect his computer in the office and reconnect from another site within the same office or elsewhere. Connectivity may be achieved through established networking technologies such as Ethernet, through dial-up lines, or using wireless networking. In the latter case, the point of attachment may change even while the user is connected since the user may travel between base stations of a wireless local area network (LAN) or a mobile phone system.

The infrastructure to support IP telephony and IP over dial-up links is discussed in subsequent sections of this chapter. This section examines the problems and solutions for handling IP when a host's physical location changes.

10.1 The Requirements of Mobile IP

Mobile IP allows a node to change its point of attachment to the Internet without needing to change its IP address. This is not simply a configuration simplification, but can facilitate continuous application-level connectivity as the node moves from point to point.

A possible solution to this problem would be to distribute routes through the network to declare the node's new location and to update the routing tables so that packets can be correctly dispatched. This might, at first, seem attractive, but it is a solution that scales very poorly since it would be necessary to retain host-specific routes for each mobile host. As the number of mobile hosts in the Internet increases (and the growth of web access from mobile devices such as cell phones and palm-tops is very rapid), it would become impractical to maintain such tables in the core of the Internet.

The solution developed by the IETF involves protocol extensions whereby packets targeted at a mobile host are sent to its home network (as if the host were not mobile) and passed to a static (nonmobile) node called the node's *home agent*. The mobile host registers its real location with the home agent, which is responsible for forwarding the packets to the host.

If the mobile host is at home (attached to its home network), forwarding is just plain old IP forwarding, but if the host is roving, packets must be tunneled across the Internet to a *care-of address* where the host has registered its attachment to a *foreign agent*. At the care-of address (the end of the tunnel) the packets are forwarded to the mobile host. This is illustrated in Figure 10.1.

Note that this tunneling process is only required in one direction. Packets sent by the mobile host may be routed through the network using the standard IP procedures.

It is worth observing that although mobile IP can be used to address any IP mobility issue, its use within wireless LANs and mobile phone networks might be better served by link-layer (i.e., sub-IP) procedures such as link-layer handoff. These processes are typically built into the link-layer mechanisms and involve less overhead than mobile IP. Such processes do, however, require that the mobile host remains logically connected within the IP subnet to which its address belongs—it becomes the responsibility of the link layer to maintain connections or virtual connections into that subnet.

An alternative to tunneling in mobile IP might be to use source routing within IP. IPv4 has been enhanced with optional extensions to support source routing. However, since the source routing extensions to IPv4 are a relatively new development and are in any case optional, many (or even most) deployed IPv4 nodes do not support them. This means that they are not a lot of use for developing mobile IP services over existing IPv4 networks. They may be

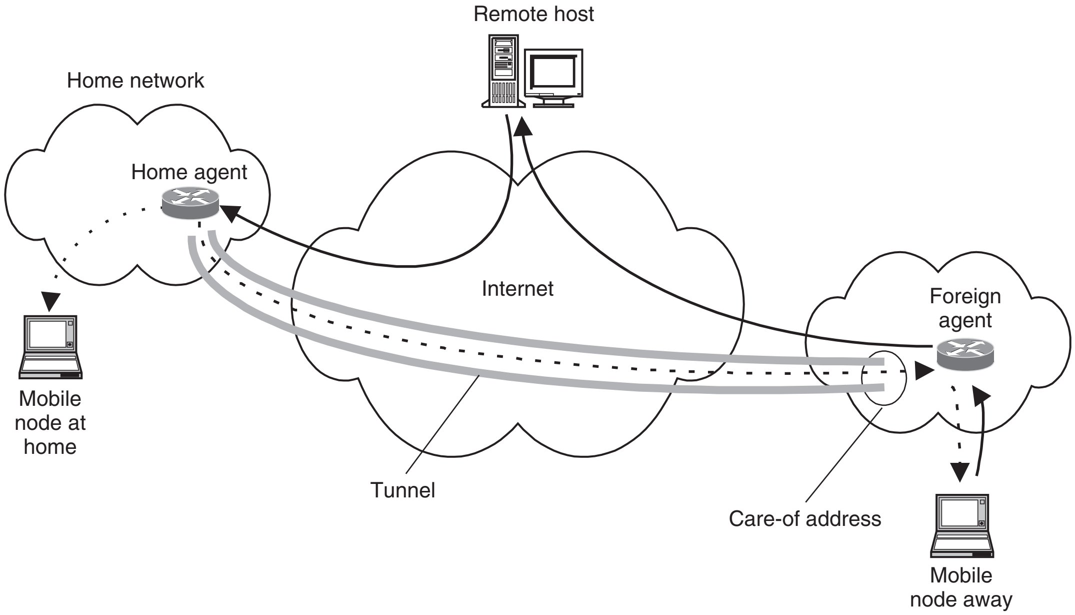

Figure 10.1 If the mobile node is away from home, IP traffic is sent to a home agent and tunneled across the Internet to a foreign agent for delivery to the mobile node.

of more use in new networks that are being constructed for the first time since the Service Providers can insist on these extensions from their equipment vendors.

IPv6 offers some alternatives to tunneling for mobile IP by using the routing extension header. In this way the mobile node can establish communications with its home agent and then use information learned to directly route packets to the destination, bypassing the home agent. Since this feature is built into IPv6 and so supported by all IPv6 implementations, it makes IPv6 a popular option for mobile IP deployments.

10.2 Extending the Protocols

Specific protocol exchanges are necessary to allow the mobile node to register with either its home agent or some remote foreign agent. Similarly, once a mobile node has registered with a foreign agent, a further registration process with the home agent is needed to get it to redirect traffic and to supply the care-of address. Additionally, foreign agents may advertise their capabilities so that mobile nodes that connect to them know that registration for mobile IP is an option. The messages to support these functions are described in RFC 3344.

Mobile nodes discover available home and foreign agents through extensions to the ICMP router discovery process. The agents advertise their mobile IP capabilities through new TLVs, shown in Figure 10.2, that follow the Router Advertisement fields in an ICMP Router Advertisement Message. The TLVs give the capabilities of the agent and list a set of useable care-of addresses and the length of validity of the registration. The meanings of the capabilities bit flags are shown in Table 10.1.

Note that regardless of the capability set advertised, a foreign agent must always support IP in IP encapsulation as defined in RFC 2003. This is the favored tunneling mechanism.

A mobile node tells its home agent about its care-of address using a registration procedure built as a new miniprotocol that uses UDP as its transport. The UDP port number 434 is reserved for agents to listen on for incoming registration requests from mobile nodes. The registration is a simple request–reply exchange using the messages shown in Figure 10.3.

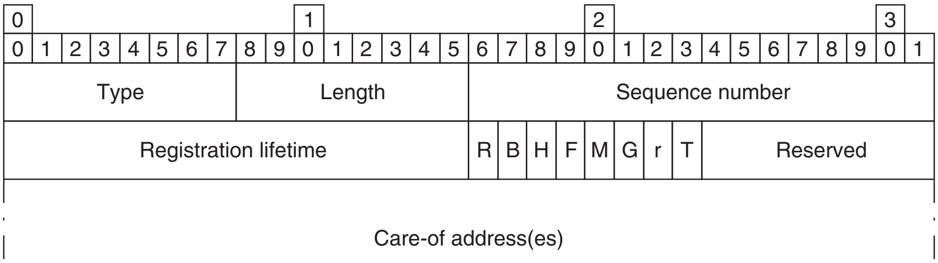

Figure 10.2 The mobile IP agent advertisement ICMP TLV.

Table 10.1 The Agent Capability Flags Within the Mobile IP Agent Advertisement ICMP TLV.

Flag	Meaning
R	The mobile nodes must complete registration procedures to make use of this foreign agent.
B	The agent is busy and will not accept registrations from additional mobile nodes.
H	This agent offers service as a home agent on the link on which this Agent Advertisement message was sent.
F	This agent offers service as a foreign agent on the link on which this Agent Advertisement message was sent.
M	This agent supports receiving tunneled datagrams (from the home agent) that use minimal encapsulation as defined in RFC 2004.
G	This agent supports receiving tunneled datagrams (from the home agent) that use GRE encapsulation as defined in RFC 2784.
r	Reserved (must be zero).
T	This agent supports reverse tunneling as defined in RFC 3024.

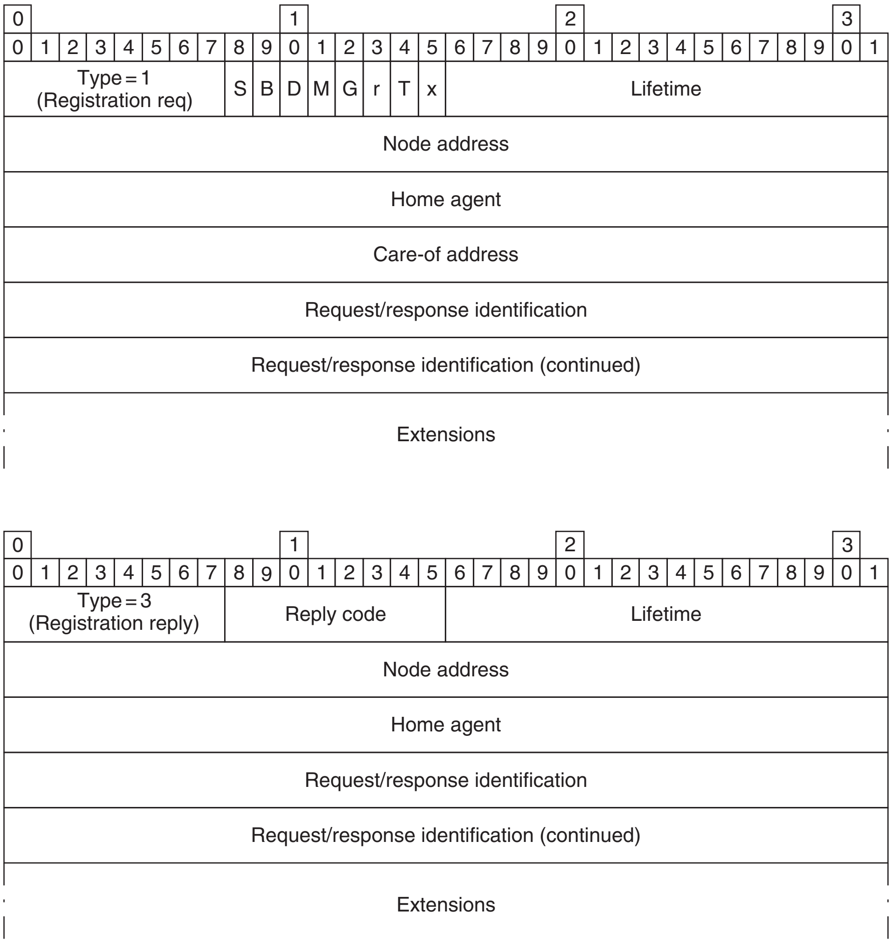

Figure 10.3 The mobile node registration request and reply messages.

The capability bits in the Registration message are inherited with some modification from the ICMP Advertisement message flags shown in Table 10.1—their precise meanings are given in Table 10.2. The Request/Response Identification is a 64-bit random number used by the requester to prevent replay attacks by malicious agents. The Reply Code in the Reply message indicates the success or failure of the request—a host of rejection reasons are allowed, as shown in Table 10.3.

Extensions to the Request and Reply messages exist to convey authentication details. The extensions are defined as TLVs for use in communication between the different components of the mobile IP network. Thus, there are extensions for Mobile-Home Authentication, Mobile-Foreign Authentication, and Foreign-Home Authentication.

10.3 Reverse Tunneling

In some environments, routers examine not only the destination IP address, but also the source IP address, when making a decision about how to forward a packet. This processing allows the router to make some attempts to filter out spoofed packets. However, in mobile IP, the source IP address of a packet sent by the mobile node may be unexpected within the context of the foreign network and may be discarded by a router. This undesirable problem is overcome by tunneling packets from the mobile node back to the home agent, and having the home agent forward them from there. This process, known as reverse tunneling, effectively reverses the path of packets that are sent to the mobile node.

Ideally, reverse tunnels would be established by the mobile nodes; however, this only works if the mobile node is colocated with the care-of address. If a foreign agent is used to provide

Table 10.2 The Capability Flags Within the Mobile IP Registration Request Message.

Flag	Meaning
S	This bit indicates that the mobile node is requesting that this binding supplement the previous binding rather than replacing it.
B	The mobile node requests that broadcast datagrams be tunneled to it along with any datagrams that are specifically addressed to it.
D	The mobile node will itself decapsulate datagrams that are tunneled to the care-of address. That is, the mobile node is colocated with the care-of address.
M	The mobile node requests the use of minimal encapsulation tunneling as defined in RFC 2004.
G	The mobile node requests the use of GRE encapsulation tunneling as defined in RFC 2784.
r	Reserved (must be zero).
T	The mobile node requests the use of reverse tunneling as defined in RFC 3024 (see below).
x	Reserved (must be zero).

Table 10.3 Mobile IP Registration Reply Message Reply Codes.

Reply Code	Meaning
0	Registration accepted
1	Registration accepted, but simultaneous mobility bindings unsupported
Rejections from the Foreign Agent	
64	Reason unspecified
65	Administratively prohibited
66	Insufficient resources
67	Mobile node failed authentication
68	Home agent failed authentication
69	Requested lifetime too long
70	Poorly formed Request
71	Poorly formed Reply
72	Requested encapsulation unavailable
73	Reserved and unavailable
74	Requested reverse tunnel unavailable
75	Reverse tunnel is mandatory and T-bit not set
76	Mobile node too distant
77	Invalid care-of address
78	Registration timeout
79	Delivery style not supported
80	Home network unreachable (ICMP error received)
81	Home agent host unreachable (ICMP error received)
82	Home agent port unreachable (ICMP error received)
88	Home agent unreachable (other ICMP error received)
Rejections from the Home Agent	
128	Reason unspecified
129	Administratively prohibited
130	Insufficient resources
131	Mobile node failed authentication
132	Foreign agent failed authentication
133	Registration Identification mismatch
134	Poorly formed Request
135	Too many simultaneous mobility bindings
136	Unknown home agent address
137	Requested reverse tunnel unavailable
138	Reverse tunnel is mandatory and T-bit not set
139	Requested encapsulation unavailable

the care-of address, the reverse tunnel is managed by the foreign agent. There are two options:

1. In the Direct Delivery style of reverse tunneling, the mobile node sends packets directly to the foreign agent as its default router and lets the foreign agent intercept them, and tunnel them to the home agent.

2. In the Encapsulating Delivery style of reverse tunneling, the mobile node sends packets to the foreign agent using a tunnel. The foreign agent decapsulates the packets and retunnels them to the home agent.

Signaling extensions for reverse tunneling are defined in RFC 3024 and basically involve the use of the T-bit shown in Tables 10.1 and 10.2, and the reply codes 74–76, 79, and 137–139 shown in Table 10.3.

10.4 Security Concerns

The standards for mobile IP mandate the use of strong authentication cryptography for the registration process between a mobile node and its home agent. This is the most vulnerable part of the mobile IP process and might, if intercepted or spoofed, cause the interception or diversion of all traffic sent from the home agent to the mobile node on behalf of the remote point of contact. Strong authentication may also be used between the mobile node and the foreign agent and between the foreign agent and the home agent. Agent discovery messages are not subject to authentication because there is currently no IP-based authentication key distribution protocol.

The data exchanged between hosts participating in mobile IP may also be encrypted. Any of the standard approaches may be used, giving rise to three models. In the first, the source of the data encrypts it and sends it through the home agent to the mobile node, which decrypts it. In the second model, the home agent chooses whether to encrypt the data it forwards according to whether the mobile node is away from or at home—in this way data forwarded to a roving mobile node is encrypted across the unknown part of the network and is decrypted by the mobile node. In the final model, IPsec is used as the tunneling protocol between the home agent and the foreign agent and the mobile node does not need to have encryption/decryption capabilities.

Further Reading

Mobile IP

Mobile IP is discussed by the Mobile IP Working Group of the IETF. Their web site is http://www.ietf.org/html.charters/mobileip-charter.html. Some key RFCs are:

- RFC 2005—Applicability Statement for IP Mobility Support.
- RFC 2794—Mobile IP Network Access Identifier Extension for IPv4.
- RFC 3024—Reverse Tunneling for Mobile IP.
- RFC 3344—IP Mobility Support for IPv4.

Media gateway control is worked on by the Megaco Working Group located at http://www.ietf.org/html.charters/megaco-charter.html.

Some important RFCs are:

- RFC 2824—Call Processing Language Framework and Requirements.
- RFC 2871—A Framework for Telephony Routing over IP.
- RFC 3219—Telephony Routing over IP (TRIP).
- RFC 3216—SIP: Session Initiation Protocol.
- RFC 3312—Integration of Resource Management and Session Initiation Protocol (SIP).
- RFC 3428—Session Initiation Protocol (SIP) Extension for Instant Messaging.
- RFC 2805—Media Gateway Control Protocol Architecture and Requirements.
- RFC 3015—Megaco Protocol Version 1.0.
- RFC 3054—Megaco IP Phone Media Gateway Application Profile.