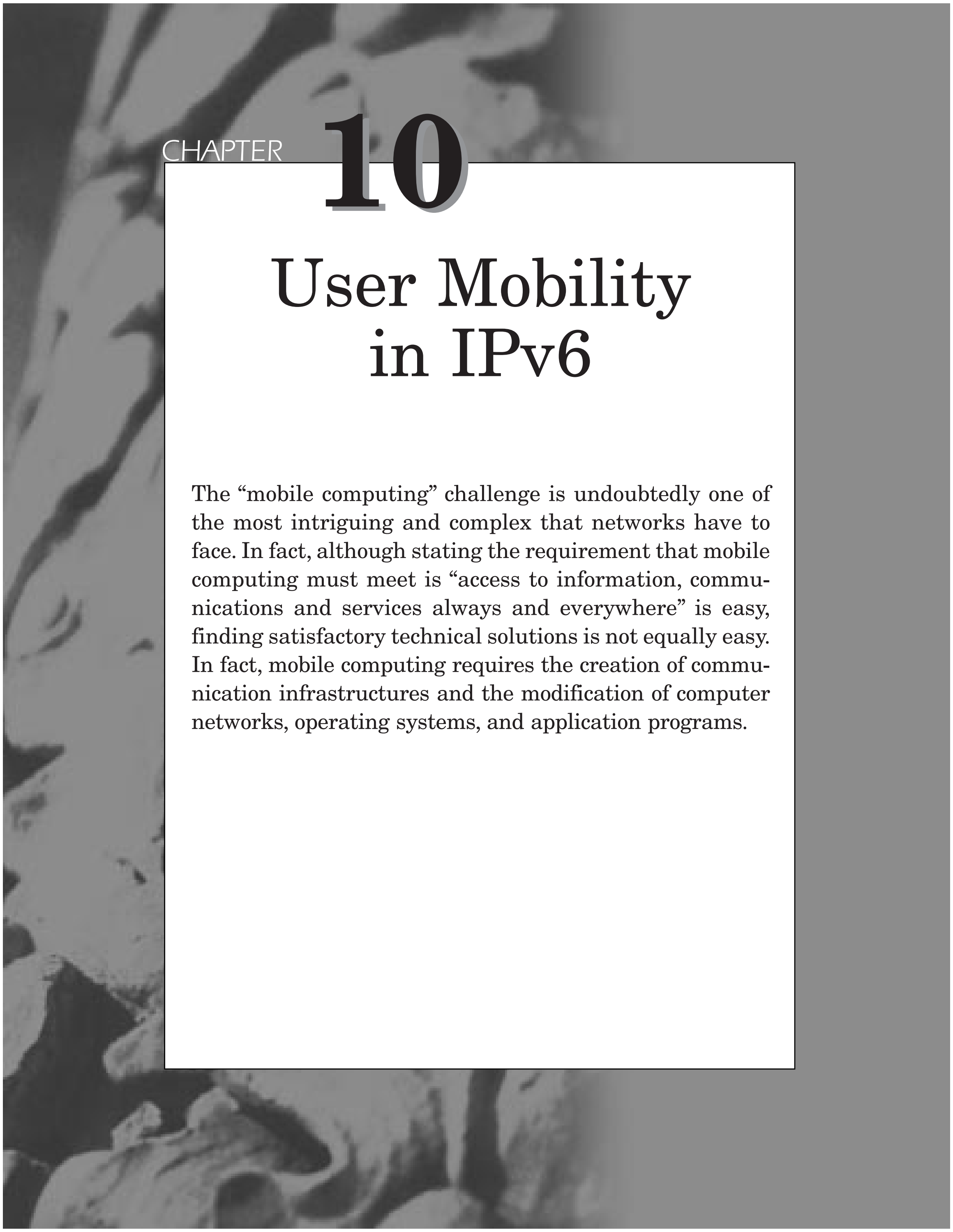

CHAPTER 10

User Mobility in IPv6

The "mobile computing" challenge is undoubtedly one of the most intriguing and complex that networks have to face. In fact, although stating the requirement that mobile computing must meet is "access to information, communications and services always and everywhere" is easy, finding satisfactory technical solutions is not equally easy. In fact, mobile computing requires the creation of communication infrastructures and the modification of computer networks, operating systems, and application programs.

IPv6 represents a real turning point for mobile computing. In fact, because IPv6 has been completely redesigned, since its conception it has foreseen the need to effectively support mobile computing and has not been bound, in the choice of solutions, by requirements of compatibility with past versions.

As we mentioned in Chapter 1, a growing number of Internet users don't work at their office desks anymore but work while traveling. The following cases occur more frequently: First, when users are employees of a company with several workstations and they want to be able to work in the same way at all workstations, by connecting their portable PCs to wired networks of the company's different workstations or to the telephone network (in this case, ISDN) at their stations; the second case happens when nomadic users (from which the term *nomadic computing* is derived) travel and work only seldomly at their offices, supposing they even have offices.

This second type of mobile user, who is usually equipped with a mobile PC and with a PCMCIA board for a mobile telephone, connects to the Internet through a public mobile radio network.

Clearly, the requirement to provide support for mobility in IPv6 is a matter of primary importance. In Northern America, estimates indicate that there will be from 20 to 40 million mobile users in 2007. Also, this requirement is clearly one of the more complex to be met because it has to deal with a multitude of problems that range from those related to radio transmission (reliability, roaming, hand-off) to IP protocols (identification, addressing, configuration, routing) to equally important security problems.

10.1 Mobility Problems

IPv6 addressing and routing schemes, already analyzed in Chapters 2 and 4, entail that a host address depends from the point where the host is connected to the network. This is exactly the opposite of what is needed for mobility, because a mobile host frequently changes its connection point to the network and therefore must change its address with equal rapidity.

A first solution consists of handling the mobility by operating at DNS (Domain Name Service) level. In Section 2.3, we saw that, in IPv6, hosts are identified by names, addresses are variable in time and not mnemonic, and names are translated into addresses by the DNS. This approach is not feasible because the DNS has been designed to minimize information search times but not updating times. It is therefore impossible to think that, when a host moves, it propagates its new address through the DNS, because updating could take many days, whereas the host should be allowed to move up to once per second.

In general, it is not possible to think that an IP host changes its address when it moves. In fact, the TCP/IP network architecture has an imperfect layered structure, in which the TCP uses not only the source and destination TCP ports but also the source and destination IP addresses as the connection identifier. This means that if the IP address of a host is changed, then all sessions of upper layer protocols related to this host will be terminated. This problem was examined in Section 6.7.2, where we saw that the process of changing addresses usually requires several days while new and old addresses coexist.

The preceding situation is a result of the fact that IP addresses, in the TCP/IP network architecture, have two different purposes: to identify connections endpoints and to determine the packet's routing. The fact that IP addresses identify connection endpoints means that they must remain stable and that a mobile host must therefore always be identified by the same address that is associated with the DNS name. Because the address is used also for routing purposes, a mobile host must acquire one or more addresses from the network to which it is connected (*foreign network*) to be used for routing packets.

The host permanent address, called the *home address,* is the address of the host when it is connected to its default network, called the *home network*. Addresses that the mobile host acquires when it is connected to a foreign network are called *care-of addresses.* The care-of address is acquired by the mobile host when it connects to a foreign network through a stateless autoconfiguration procedure (see Section 6.7.1) or a stateful procedure through DHCP (see Section 6.7.3).

Problems of mobility management in IPv6 are therefore problems of management of relationships between home addresses and care-of addresses, and problems of the use of the appropriate type of address in relation to the context. Moreover, when the mobile host is connected to a foreign network, it must delegate a router of its home network to "represent" it when it is absent. This router assumes the name of *home agent*.

A home agent usually serves all mobile hosts of a home network by forwarding messages addressed to them. To do so, the home agent traces all movements, and in particular, it records in memory, called a *binding cache*, the mapping between home addresses and care-of addresses.

From this scenario, we can see that IPv6 is suitable for providing support for the mobility on heterogeneous networks and that it can be used both for moving from an Ethernet network to another and for moving from an Ethernet network to a wireless network. Moreover, note that IPv6 has been conceived to support the “macro” mobility and that it is less suitable for the “micro” mobility, in which, for example, a host moves between two cells of a wireless LAN. In the latter case, the mobility can be more efficiently implemented by using link layer mechanisms (layer 2 of the OSI model).

10.2 Operation of a Mobile Host in IPv6

When a mobile host is connected to a foreign network, it decides to acquire a care-of address through a stateful or a stateless procedure on the basis of Router Advertisement messages received and, more specifically, of M and O bits received (see Section 5.5.5).

Each time a mobile host changes its connection point at the link layer from an IPv6 subnet to another IPv6 subnet, it must acquire a new care-of address, which becomes its *primary care-of address*. Other care-of addresses previously acquired can be maintained to allow the host to continue to receive packets addressed to previous care-of addresses. This procedure can be useful in using radio networks in which a host can decide to configure itself on the cell from which it receives the highest power signal but to continue to receive signals also from other cells that previously served it.

The mapping between the home address and the primary care-of address is called *binding*. Every time the mobile host configures a new primary care-of address, and therefore a new binding, it must communicate the address to its home agent through a *Binding Update* message (see Section 10.4.1). The Binding Update message must also be sent to all nodes with which the mobile host had an exchange of packets and which could have obsolete information in their binding caches. For this reason, the mobile host maintains a data structure, called a *Binding Update List*, that contains addresses of all nodes to which it sent Binding Update messages and the relative remaining temporal validity.

A mobile host, in whatever instant, can be reached by sending a message to its home address. If the mobile host is not connected to its home network, all packets forwarded to it will be intercepted by the home agent, which will transmit them to the mobile host through a tunnel (see Section 7.5.6) by using its primary care-of address.

When a packet arrives at the mobile host through a tunnel, the mobile host realizes that it has been forwarded by the home agent and sends a Binding Update message to the source node. When the source node receives this message, it creates in its binding cache an entry that contains the home address and the care-of address. This information allows the source node to directly forward the following packets to the care-of address through a Routing Header (see Section 3.2.5) instead of through a tunnel (a technique used only by the home agent).

Therefore, only the first packet of a sequence of packets exchanged between a source node and a mobile host passes through the home agent, whereas all other packets are directly transmitted by the source to the mobile host through the Routing Header. This process is fundamental in obtaining a scalable and reliable solution and in minimizing the network load.

When the mobile host moves (changes its primary care-of address), it forwards a Binding Update message to all nodes listed in the Binding Update List.

The Binding Update message must include an Authentication Header (see Chapter 8) to avoid a situation in which potential hackers could redirect someone else's traffic toward themselves by a fraudulent use of these messages.

10.3 Examples of Operation of a Mobile Host in IPv6

To better understand the topics presented in the preceding section, let's consider the example shown in Figure 10-1.

The host Z is usually connected to subnet A, which is its home network, and Z acquires from A the address A::1, which is its home address. (Note that the syntax for this address is not formally correct, but only an example.) This address A::1 is put into a relationship with the name Z at the DNS level. In the same way, W is connected to the subnet C, and from C, it acquires the address C::5.

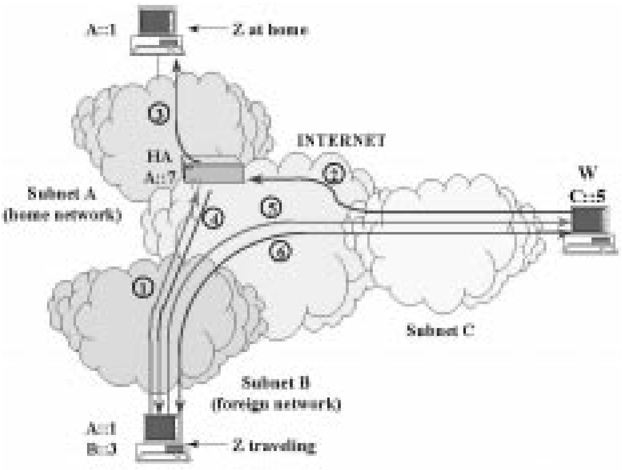

Figure 10-1
Example of mobility

When W wants to forward packets to Z, it asks the DNS and obtains the address A::1. Then W generates IPv6 packets whose destination address is A::1 and source address is C::5 (2). These packets are routed by IPv6 routing and reach the destination subnet A.

At this point, three situations are possible:

- Node Z is connected to its home network. Packets are delivered to Z by using classical IPv6 routing procedures (3).
- Node Z is connected to subnet B, which acts as a foreign network. Z acquires from B its primary care-of address B::3, which is communicated through a Binding Update (1) message to its home agent (HA). Packets received by the home agent are forwarded to Z through a tunnel from A::7 to B::3 (4). When B::3 extracts packets from the tunnel, it checks whether they are addressed to A::1—that is, to itself. At this point, Z sends a Binding Update message to W (5), and W stores the message in its binding cache. From this moment on, W communicates with Z without passing through the home agent, but forwards packets to Z through a Routing Header that forces a source routing on B::3 (6).
- The third possible situation is that Z is not connected in any place. The router connected to the subnet A tries to reach Z at the address A::1, and because it fails, it communicates this failure to the source node by using an ICMP message.

If Z moves from subnet B to subnet D, it acquires a new address belonging to subnet D (for example, D::11) that becomes its new primary care-of address. This new address is communicated through a Binding Update message both to its home agent and to W.

10.4 Options Format

The information necessary to support an IPv6 host's mobility is exchanged through four options implemented in a Destination Option extension header (see Section 3.2.8). Because a Destination Option extension header can be part of any IPv6 packet, options for the mobility can be associated with the following:

- Normal IPv6 packets containing payloads such as TCP or UDP.
- Independent packets, containing only options. In this second case, the Next Header field of the Destination Option Header must be set equal to value 59 to indicate the lack of more headers (see Section 3.2.5).

Options are codified according to the TLV (Type, Length, Value) format (see Section 3.2.2).

10.4.1 Binding Update Option

The Binding Update option (see Figure 10-2) is used by the mobile node to communicate to its home agent, or to the corresponding nodes, its present binding.

The 8-bit *Option Type* field has value 192.

The 8-bit *Option Length* field contains the length in octets of the option, Option Type and Option Length field not included. This field has a minimum value of 6 if both the Care-of Address (C = 0) and the Home Link Local Address (L = 0) are not present. Its maximum value is 38 if both the addresses (C = 1, L = 1) are present.

The 1-bit *A* (Acknowledge) field is set by the source node to request the node that receives the Binding Update option to send a Binding Acknowledgment message.

The 1-bit *H* (Home Registration) field is set by the source node to request the node that receives the Binding Update option to perform as its home agent. The IPv6 packet destination address containing this option must be that of a router interface whose prefix is the same of the mobile node's home address.

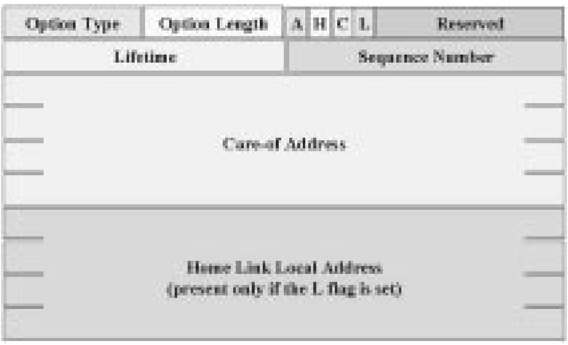

Figure 10-2
The Binding Update option

The 1-bit *C* (Care-of Address Present) field is set by the source node to indicate the presence of the care-of address in the Binding Update option.

The 1-bit *L* (Home Link Local Address Present) field is set by the source node to indicate the presence of the Home Link Local Address in the Binding Update option. This bit is set by the source node to request the destination node to perform like a proxy—that is, to participate in the Neighbor Discovery process in place of the mobile host. When this bit is set, the bit H also must be set.

The 12-bit *Reserved* field is reserved for future use. It must be initialized to zero during transmission and ignored on reception.

The 16-bit *Lifetime* field contains the validity interval of the binding information in seconds—that is, how long the binding information must be considered valid in the binding cache. The value zero indicates that the binding information must be deleted from the binding cache; the value 0xffff indicates that the binding information must be indefinitely maintained.

The 16-bit *Sequence Number* field is used to set the mapping between Binding Update messages and Binding Acknowledgment messages. Each Binding Update sent by a mobile node must use a sequence number greater than the sequence number value sent in the previous Binding Update (if any) to the same destination address (modulo 2^{16}).

The 128-bit *Care-of Address* field contains the IPv6 address acquired from the mobile node on the foreign network. IPv6 address codification was analyzed in Chapter 4 of this book. When the care-of address is set equal to the home address, the Binding Update option indicates that it is necessary to cancel existing associations from binding caches for the mobile node and that no new association must be created by the message.

The 128-bit *Home Link Local Address* field contains the IPv6 link local address used by the mobile node during its last connection to the home network. This field, which is optional, is present only if the field L has value 1.

Like in the case of other IPv6 options, the three most significant bits of the Option Type field have a particular meaning (see Section 3.2.2). Because the field has value 192, the bits have value 110. This particular value specifies the following:

- In the case of the two most significant bits (11) that, if a node doesn't recognize the option, it must discard the packet and communicate this fact to the source node through an ICMP Parameter Problem message, only if the destination address is not multicast
- In the case of the third bit (0) that the option cannot be modified en route

Also, optional fields, not currently defined, can be added after the Binding Update option; the presence of these fields can be detected from the value of the Option Length field.

10.4.2 The Binding Acknowledgment Option

The Binding Acknowledgment option is used to confirm the receipt of a Binding Update option. It is generated only if the mobile node explicitly requests it by setting the bit A in the Binding Update option. The format of the Binding Acknowledgment option is shown in Figure 10-3.

The 8-bit *Option Type* field has value 193.

The 8-bit *Option Length* field contains the option's length in octets, Option Type and Option Length fields not included. This field has value 9.

The 8-bit *Status* field can assume the values listed in Table 10-1. Values smaller than 128 indicate that the Binding Update option has been accepted; values greater than or equal to 128 indicate that it has been rejected.

Figure 10-3
ICMP Message of Binding Acknowledgment

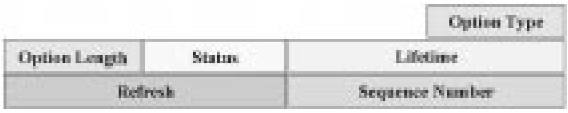

Table 10-1

Possible values for the Status field

Value	Meaning
0	Option accepted
128	Option rejected: unspecified reason
129	Option rejected: poorly formed binding update
130	Option rejected: operation administratively prohibited
131	Option rejected: insufficient resources
132	Option rejected: home registration not supported
133	Option rejected: the network is not the home network
134	Option rejected: Sequence Number field value too small
135	Option rejected: dynamic home agent address discovery response

The *Lifetime* field contains the time the node maintains the information stored in its binding cache.

The *Refresh* field contains the period of time after which the mobile node must send a Binding Update message to update the information in the binding cache.

The 16-bit *Sequence Number* field is used to set the mapping between Binding Update messages and Binding Acknowledgment messages.

Also, optional fields, not currently defined, can be added after the Binding Acknowledgment option; the presence of these fields can be detected from the value of the Option Length field.

10.4.3 The Binding Request Option

The Binding Request option is used to request the mobile node to send a Binding Update. This option is used by a node with one entry in the binding cache, whose temporal validity is going to expire, to obtain updated information. The format of the Binding Request option is shown in Figure 10-4.

The 8-bit *Option Type* field has value 194.

The 8-bit *Option Length* field contains the length of the option in octets, Option Type field and Option Length field not included. This field has value zero.

Also, optional fields, not currently defined, can be added after the Binding Request option; the presence of these fields can be detected from the value of the Option Length field.

10.4.4 The Home Address Option

The Home Address destination option is used in a packet sent by a mobile node to inform the destination of the packet of the mobile node Home Address. If we include this option in the packet, the receiving node can substitute the mobile node's home address for this care-of address, thus making the use of the care-of address transparent to the receiving node. The format of the Home Address option is shown in Figure 10-5.

The 8-bit *Option Type* field has value 195.

The 8-bit Option Length field contains the length of the option in octets, Option Type field and Option Length field not included. This field has value 8.

The 128-bit *Home Address* field contains the IPv6 home address of the mobile node sending the packet.

Also, optional fields, not currently defined, can be added after the Home Address option; the presence of these fields can be detected from the value of the Option Length field.

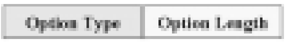

Figure 10-4
The Binding Request option

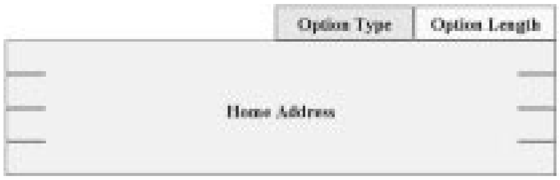

Figure 10-5
The Home Address option

10.5 Characteristics of Nodes

The mobility creates some new requirements on the architecture and on functions of IPv6 nodes. In particular, some of these requirements must be met by all the nodes, whereas others are typical of routers or of mobile nodes.

10.5.1 General Requirements

All IPv6 nodes must meet the following requirements:

- To receive a Binding Update option and to generate a Binding Acknowledgment message, if requested.
- To administer a binding cache in which the information received from Binding Update messages must be stored.
- To administer a Security Association to be jointly used with an IPv6 Authentication Header (see Section 8.1.1). In fact, when an IPv6 node receives a Binding Update option, it must check the identity of the source node through the Authentication Header and, only if the check is positive, store the received information in the binding cache.

10.5.2 Router Requirements

Because an IPv6 router can contain information about a mobile host in its binding cache, all IPv6 routers must meet the following requirement:

- Each IPv6 router must be able to use its binding cache for routing packets. This means that, if a router has in its binding cache an entry relevant to the destination address of the packet it is routing, it should encapsulate the packet in a tunnel and send it to the care-of address.

  Moreover, to allow a mobile node to leave its home, at least a router of its home network must be able to operate as a home agent. Routers able to operate as home agents must meet the following additional requirements:
- To administer a list of nodes for which they operate as home agents

- To intercept packets addressed to mobile hosts on the local network, for example, by replacing mobile hosts in the Neighbor Discovery procedure
- To retransmit intercepted packets by creating a tunnel toward mobile hosts' care-of addresses

10.5.3 Mobile Node Requirements

Mobile nodes must meet the following requirements:

- To receive packets through a tunnel
- To send Binding Updates and to receive Binding Acknowledgments
- To administer a Binding Update List in which to store all nodes that have been sent Binding Update messages whose temporal validity has not yet expired

10.6 Transmission of Packets to a Mobile Node

We have already seen that the first packet toward a mobile host connected to a foreign network is routed toward the home network; here it is captured by the home agent and retransmitted in a tunnel to the care-of address. The receipt of the packet by the mobile host produces the transmission of a Binding Update message to the source node, whose information is stored in the binding cache.

At this point, the source node, having valid information for the destination node in its binding cache, should directly send packets using a Routing Header.

For example, in the case it doesn't need to use the Routing Header for other purposes, the source node generates a packet with the care-of address as the IPv6 destination address and with the Routing Header shown in Figure 10-6 (see also Section A.2 in Appendix A).

The Routing Header in Figure 10-5 indicates the existence of only one address to be processed (Segment Left = 1), and this address is the home address. The IPv6 packet is routed to the destination node using the IPv6 destination address—that is, the care-of address. When the packet reaches the destination node, the node processes the Routing Header and

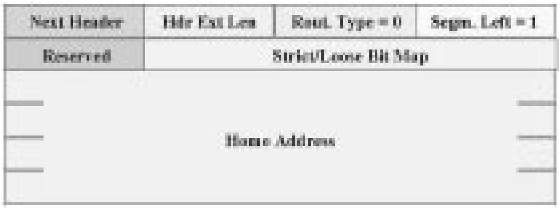

Figure 10-6 Example of Routing Header

determines that the packet must be routed toward the home address—that is, toward itself.

This process allows the upper layer protocols to see the home address as a destination address and therefore not to perceive the mobility.

10.7 Other Functions of Mobile Nodes

Besides the functions just described, a mobile host must also be able to detect its mobility, to transmit, to receive multicast packets, and to return home.

10.7.1 Mobility Detection

A mobile host can use all mechanisms at its disposal to detect its mobility. The main mechanism is the Neighbor Discovery, described in Chapter 6. In fact, mobile hosts must use the Neighbor Discovery to locate the presence of new routers and new network prefixes. Moreover, the mobile host must use the Neighbor Unreachability Detection procedure (see Section 6.6) to check the reachability of its default router because the possibility of it becoming unreachable is much higher than usual.

10.7.2 Multicast Traffic Handling

The mobile node must belong to a multicast group to receive multicast traffic. This traffic handling can be implemented in the following two ways:

- The mobile host can ask the multicast router present on the foreign network to belong to the multicast group.
- The mobile host can ask the multicast router present on its home network to belong to the multicast group through a bi-directional tunnel with its home agent.

Likewise, a mobile host willing to transmit multicast packets offers two possibilities: to transmit them directly on the foreign network or to transmit them to its home agent through a tunnel. Because multicast routing depends on the IPv6 source address, in the first case, the mobile host will use its primary care-of address; whereas in the second case, it will use its home address. Note that the second solution treats the home agent also as a multicast router.

10.7.3 Home Again

A mobile host detects its return home when it receives the prefix of its home network through Neighbor Discovery messages. At this point, the mobile host transmits to its home agent a Binding Update message in which the care-of address is equal to its home address to request its home agent not to intercept packets addressed to it anymore because the mobile host is home again. The Binding Update message must be transmitted with the bit A = 1 and repeated until the home agent sends a Binding Acknowledgment message.

The mobile host must also send a Neighbor Advertisement message with the Override flag set (see Section 5.5.7), to request all hosts on the home network to update the neighbor information in their caches. This operation must be repeated a limited number of times both for the home address and for the link local address.

REFERENCES

[1] Several authors, *Issues in Mobile Computing Systems*, IEEE Personal Communications, Vol. 2, No. 6, December 1995.

[2] P. Bhagwat, C. Perkins, S. Tripathi, *Network Layer Mobility: An Architecture and Survey*, IEEE Personal Communications, Vol. 3, No. 3, June 1996, pp. 54-64.

[3] D. B. Johnson, C. Perkins, *Mobility Support in IPv6*, July 1997.