CHAPTER 8

LAYER 3 CONNECTIVITY: MOBILE IPv6 TECHNOLOGIES FOR THE IoT

This chapter provides an in-depth view of mobile IPv6 (MIPv6). It starts with an overview of the key concepts (Section 8.1) and then provides a more detailed protocol-level description (Section 8.2). MIPv6 is specified in RFC 3775; this RFC is known as the "MIPv6 base specification." For a more complete description of MIPv6 and several extensions to the base specification, the reader may wish to refer to Reference 1. MIPv6 is one of several approaches that can be utilized to manage mobility in an IoT/machine-to-machine (M2M) environment.

8.1 OVERVIEW

MIPv6 specifies a protocol that allows nodes to remain reachable while moving around in the IPv6 Internet. An entity that implements the MIPv6 protocol is a MIPv6 entity. There are three types of entities defined in the MIPv6 protocol:

- Mobile node (MN): A node that can change its point of attachment from one link to another while still being reachable via its home address.
- Correspondent node (CN): A peer node with which an MN is communicating. The CN may be either mobile or stationary. A CN does not necessarily require MIPv6 support, but it does require IPv6 support.

Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications, First Edition. Daniel Minoli.

- Home agent (HA): A router on an MN's home link with which the MN has registered its current care-of address (CoA) described below. While the MN is away from home, the HA intercepts packets on the home link destined to the MN's home address, encapsulates them, and routes them to the MN's CoA.

If an MN is not currently attached to its home network (also called the home link[1]), the MN is said to be "away from home." Each MN is *identified* by its home address (which we also call stationary home address), regardless of its current point of attachment to the remote network (e.g., the Internet); this is a globally unique, explicit IPv6 address. While situated away from its home, on a foreign link (also known as foreign network [FN][2]), an MN is also associated with an "in-care-of-address" known, in fact, as care-of address, or CoA, which provides information about the MN's current location. Clearly, the CoA changes depending on the current location of the MN. The CoA is used for *routing* (i.e., delivering) IPv6 packets addressed to an MN's home address; packets sent to the MN's home address are transparently routed to the MN via its current CoA. The CoA must be a unicast routable address, typically specified by the source address field in the IPv6 header; the IPv6 source address must be a topologically correct source address. The MN is assumed to be seeking to communicate with a CN, also an IPv6-ready node. The MIPv6 protocol enables IPv6 nodes to cache the binding of an MN's home address with its CoA; these underlying mechanisms ascertain that communications (e.g., TCP sessions) are maintained while the MN is physically moving, and, thus, connecting via an FNs. MIPv6 operations involve movement detection, IP address configuration, and location update. Table 8.1 provides some basic MIPv6 nomenclature used in this chapter as defined in Reference 2. Figure 8.1 depicts the basic MIPv6 environment.

The binding (association) between the two IP addresses utilized in MIPv6 (the home address and the CoA) is kept at a well-known location, the HA, which is used to support connectivity; the HA is a router in the MN's home network. The CN performs packet routing toward the MN using the routing header. The CN learns the position of an MN by processing binding updates (BUs). Whenever the MN connects to an FN, it sends a BU to the HA and CNs; an MN keeps a list of the CNs to which it sent a BU. The recipients of the BUs reply with a binding acknowledgement (BA). Security is a consideration; therefore, BU information requires protection and authentication; broadly speaking, IP Security (IPsec) can be used for this.[3] Figure 8.2 depicts the basic routing/forwarding operation of the HA (this is the tunnel mode).

Note: The MN may have multiple CoAs. The CoA sent to the HA in the BU is called the primary CoA. For example, in the case of a wireless networks, an MN might be reachable through multiple links at the same time (e.g., with overlapping

[1]The home link is defined as the link on which a mobile node's home subnet prefix is defined.
[2]The FN can be the Internet or a network that is connected to the Internet.
[3]BUs can be protected using IPSec extensions headers (as covered in Chapter 2), or by the use of the binding authorization data option (this option employs a binding management key [known as Kbm] which can be established through the return-routability procedure).

TABLE 8.1 Basic MIPv6 Terminology

Term	Description
Binding	The association of the home address of an MN with an in-CoA for that MN, along with the remaining lifetime of that association
Binding authorization	Mechanism where correspondent's registration is authorized, enabling the recipient to conclude that the sender has the right to specify a new binding
Binding cache	A cache of bindings for other nodes. This cache is maintained by HAs) and CNs. The cache contains both "correspondent registration" entries and "home registration" entries
Binding management key	(also known as Kbm) A key used for authorizing a binding cache management message (e.g., BU or BA). Return-routability provides a way to create a binding management key
BU list	A list that is maintained by each MN. The list has an item for every binding that the MN has or is trying to establish with a specific other node. Both correspondent and home registrations are included in this list. Entries from the list are deleted as the lifetime of the binding expires
Care-of address (CoA)	A unicast routable IPv6 address associated with an MN while visiting a foreign link; the subnet prefix of this IP address is a foreign subnet prefix. Among the multiple CoAs that an MN may have at any given time (e.g., with different subnet prefixes), the one registered with the MN's HA for a given home address is called its "primary" CoA
Care-of init cookie	A cookie sent to the CN in the care-of test init message, to be returned in the care-of test message
Care-of keygen token	A keygen token sent by the CN in the Care-of test message
Cookie	A cookie is a random number used by an MN to prevent spoofing by a bogus CN in the return-routability procedure
Correspondent node (CN)	A peer node with which an MN is communicating. The CN may be either mobile or stationary
Correspondent registration	A return-routability procedure followed by a registration, run between the MN and a CN
Destination option	Options that are carried by the IPv6 DESTINATION OPTIONS extension header. Destination options include optional information that is examined only by the IPv6 node given as the destination address in the IPv6 header, not by routers in between. MIPv6 defines one new destination option, the home address destination option
Foreign link	Any link other than the MN's home link. Also known as FN
Foreign subnet prefix	Any IP subnet prefix other than the MN's home subnet prefix
Home address	A unicast routable address assigned to an MN, used as the permanent address of the MN; this address is within the MN's home link. Standard IP routing mechanisms will deliver packets destined for an MN's home address to its home link. MNs can in principle have multiple home addresses, for instance when there are multiple home prefixes on the home link

(*continued*)

TABLE 8.1 (***Continued***)

Term	Description
Home agent (HA)	A router on an MN's home link with which the MN has registered its current CoA. While the MN is away from home, the HA intercepts packets on the home link destined to the MN's home address, encapsulates them, and tunnels them to the MN's registered CoA
HA list	HAs need to know which other HAs are on the same link. This information is stored in the HA list; the list is used for informing MNs during dynamic HAAD
Home init cookie	A cookie sent to the CN in the home test init (HoTi) message, to be returned in the home test (HoT) message
Home keygen token	A keygen token sent by the CN in the HoT message
Home registration	A registration between the MN and its HA, authorized by the use of IPsec
Home subnet prefix	The IP subnet prefix corresponding to an MN's home address
Interface identifier	A number used to identify a node's interface on a link. The interface identifier is the remaining low-order bits in the node's IP address after the subnet prefix
IP Security (IPsec) security association	A cooperative relationship formed by the sharing of cryptographic keying material and associated context. SAs are simplex; that is, two SAs are needed to protect bidirectional traffic between two nodes, one for each direction
Keygen token	A number supplied by a CN in the return-routability procedure to enable the MN to compute the necessary binding management key for authorizing a BU
Layer 2 (L2) handover	A process by which the MN changes from one link-layer connection to another
Layer 3 (L3) handover	Subsequent to an L2 handover, an MN detects a change in an on-link subnet prefix that would require a change in the primary CoA. For example, a change of access router subsequent to a change of wireless access point typically results in an L3 handover
Link-layer address	A link-layer identifier for an interface, such as IEEE 802 addresses on Ethernet links
Mobility message	A message containing a mobility header
Nonce	Random numbers used internally by the CN in the creation of keygen tokens related to the return-routability procedure. The nonces are not specific to an MN and are kept secret within the CN
Registration	The process during which an MN sends a BU to its HA or a CN, causing a binding for the MN to be registered
Return-routability procedure	A procedure that authorizes registrations by the use of a cryptographic token exchange
Routing header	A routing header may be present as an IPv6 header extension and indicates that the payload has to be delivered to a destination IPv6 address in some way that is different from what would be carried out by standard Internet routing
Unicast routable address	An identifier for a single interface such that a packet sent to it from another IPv6 subnet is delivered to the interface identified by that address

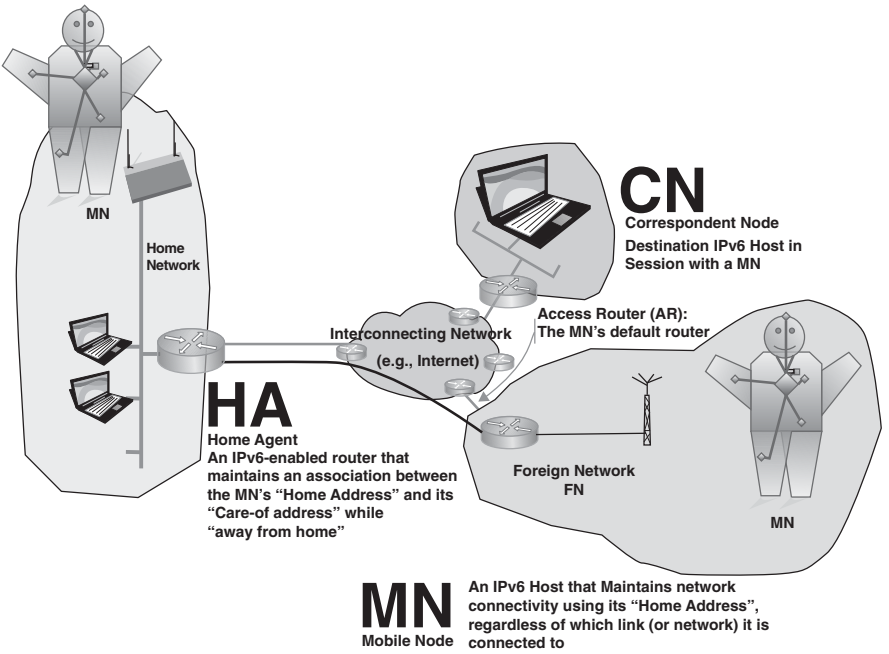


FIGURE 8.1 Basic MIPv6 environment.

wireless cells). The MN must ensure that its primary CoA always has a prefix that is advertised by its current default router.

Note: An MN may use various and multiple types of network interfaces to obtain durable and wide-area network connectivity, for example using protocols such as IEEE 802.2, 802.11, 802.16, cellular radios, etc. Note, however, that while an MN may have several CoA but only one, called the primary CoA, can be registered with its HA and the CNs. There are cases where it is desirable for the MN to get Internet access through multiple accesses simultaneously, in which case the MN would be configured with multiple active IPv6 CoAs. In RFC 5648, MIPv6 and Network Mobility (NEMO) basic support are extended to allow the binding of more than one CoA to a home address.

At least one IPv6-capable router on the home network must be able to act as HA. The HA supports the following functions:

- Maintains the MN's binding information;
- Intercepts packets that arrive at the MN's home network and whose destination address is its HA;
- Tunnels (i.e., provides IPv6 encapsulation) these packets to the MN; and
- Provides reverse tunneling from the MN to the CN (i.e., provides IPv6 de-encapsulation).
- MIPv6 makes use of IPv6 packet formats and procedures, and, furthermore,

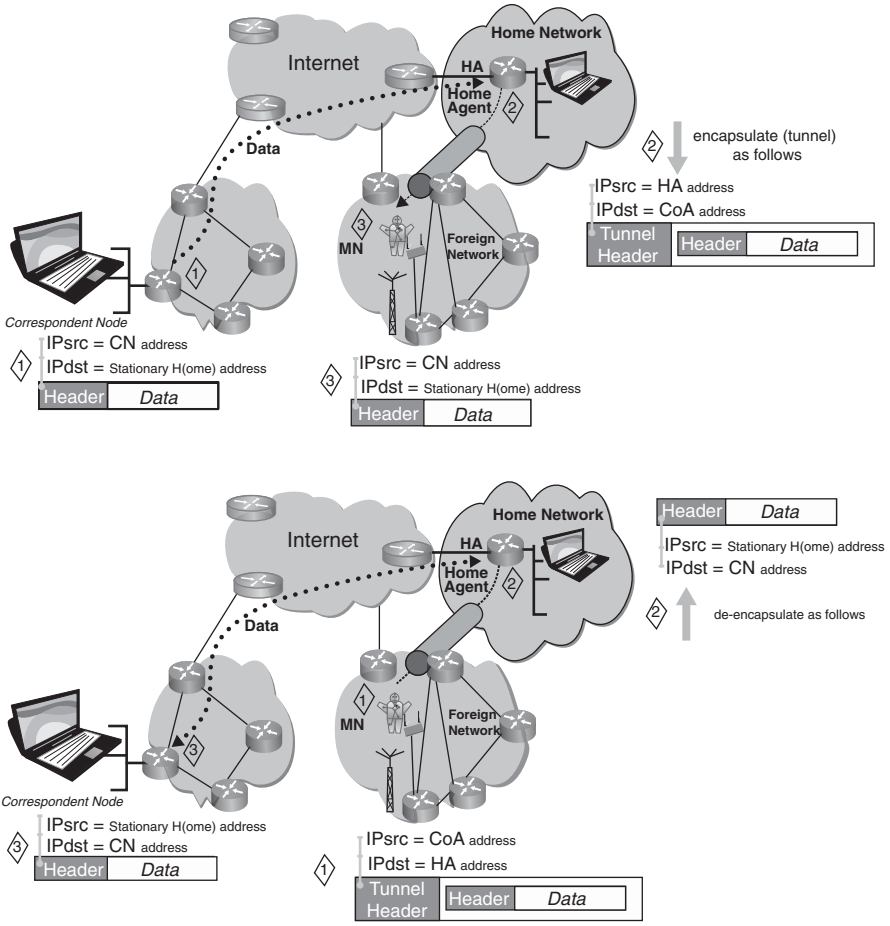


FIGURE 8.2 HA tunneling.

1. Establishes new extension header, specifically the mobility header (described further in Section 8.2).
2. Adds a new routing header type (routing header type 2); MIPv6 defines a routing header that allows packets to be routed directly from a CN to MN via the MN's CoA. This is achieved by inserting the MN's CoA into the IPv6 destination address field. Once the packet arrives at the location specified by the CoA, the MN retrieves its home address from the routing header; this is then used as the final destination of the packet. The newly defined routing header uses a different type than the type used for "regular" IPv6 routing; this, for example, allows firewalls to utilize different security rules for MIPv6 packets that would be used for source-routed IPv6 packets (see Fig. 8.3). And,

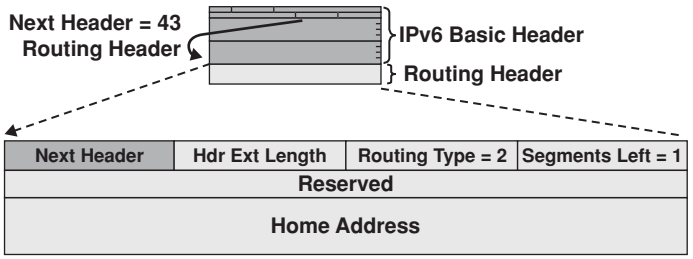


FIGURE 8.3 New routing header type for MIPv6.

3. Adds a new destination option; The destination option extension header is used to support home address option. This option is utilized in a packet sent by an MN while it is on an FN to inform the recipient of the MN's home address (see Fig. 8.4).

HA address discovery (HAAD) is an important mechanism. MIPv6 introduces four new Internet control message protocol version 6 (ICMPv6) messages to support its processes. Two of the new ICMPv6 messages are employed in the dynamic home agent address discovery (DHAAD) process; these messages support the (i) HAAD request (using the HA's anycast address of its own home subnet prefix) and (ii) HAAD reply. The other two ICMPv6 are used for renumbering and mobile configuration mechanisms; these messages support (i) mobile prefix solicitation and (ii) mobile prefix advertisement. The utilization of these four ICMPv6 messages plus the neighbor discovery protocol (NDP) makes MIPv6 independent of the underlying (layer 2) networking technology.

The NDP is modified with MIPv6 to support requisite mobility functions, as follows. The modified router advertisement message format has a single flag indicating HA service. The modified prefix information option format allows a router to advertise its global address. Other modifications include: (i) a new advertisement interval option format; (ii) a new HA information option format; and (iii) changes to sending router advertisements.

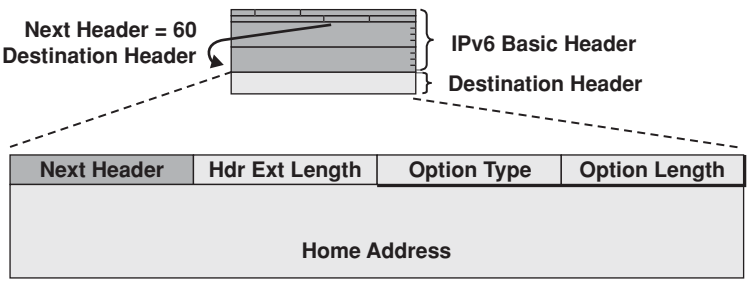


FIGURE 8.4 Destination option extension header.

Communications with MNs takes place in two ways:

1. Bidirectional tunneling. In this approach, the HA plays a crucial role, although this implies that the network traffic to this node can be high; however, the CN has no requirements related to mobility support—also, the MNs have no direct visibility related to the CN. This approach was depicted in Figure 8.2.
2. Direct routing (aka route optimization). In this approach, the HA plays a lesser role, but the overall mechanism is more complex. To support this operation, the MNs have three basic functions to manage communication (in addition to gaining access to the FN): (i) perform IPv6 packet encapsulation and de-encapsulation; (ii) send BUs and receive BAs (this entails processing the mobility header); and (iii) keep track of BUs that are sent. To support this operation, the CNs have three basic functions to manage communication: (i) process the mobility header (BUs, BAs); (ii) process/use routing headers type 2; and, (iii) maintain a binding cache. This approach is depicted in Figure 8.5.

If a binding exists, the MN will send the packets directly to the CN; otherwise, if a binding does not exist, the MN must use tunneling. MIPv6 route optimization as described in RFC 3775 enables MNs and CNs to communicate via a direct routing path despite changes in IP connectivity on the MN side. Both end nodes use a stable "home address" in identifying the MN at stack layers above IP, while payload packets are sent or received via a CoA that routes to the MN's current network attachment. MIPv6 swaps the home address and COA when a payload packet traverses the IP layer. The association between an MN's home address and CoA is the "binding" for the MN. It is the responsibility of the MN to update its binding at the CN through a "correspondent registration" when it changes IP connectivity. A correspondent registration further involves the MN's HA, which proxies the MN at the home address and mainly serves as a relay for payload packets exchanged with CNs that do not support route optimization. The MN keeps the HA up to date about its current CoA by means of "home registrations" (3). See Figure 8.6.

Higher-layer protocols, for example user datagram protocol (UDP), transmission control protocol (TCP), real-time streaming protocol (RTSP), real-time transport protocol (RTP), generally treat the MN's home address as its IP address for most packets. For packets sent that are part of transport-level connections established while the MN was at home, the MN must use its home address; for packets sent that are part of transport-level connections that the MN may still be using after moving to a new location, the MN also uses its home address.

In summary, the MIPv6 protocol requires the MN to own a home address and to have an assigned HA to the MN. The MN needs to register with the HA in order to enable its reachability and mobility, when away from its home link. The registration process itself may require an establishment of IPsec security associations (SAs) and cryptographic material between the MN and the HA. Alternatively, the registration process may be secured using a mobility message authentication option, which enables IPv6 mobility in an MN without having to establish an IPsec SA with its HA. According to the latest RFCs, the only SA that is preconfigured is

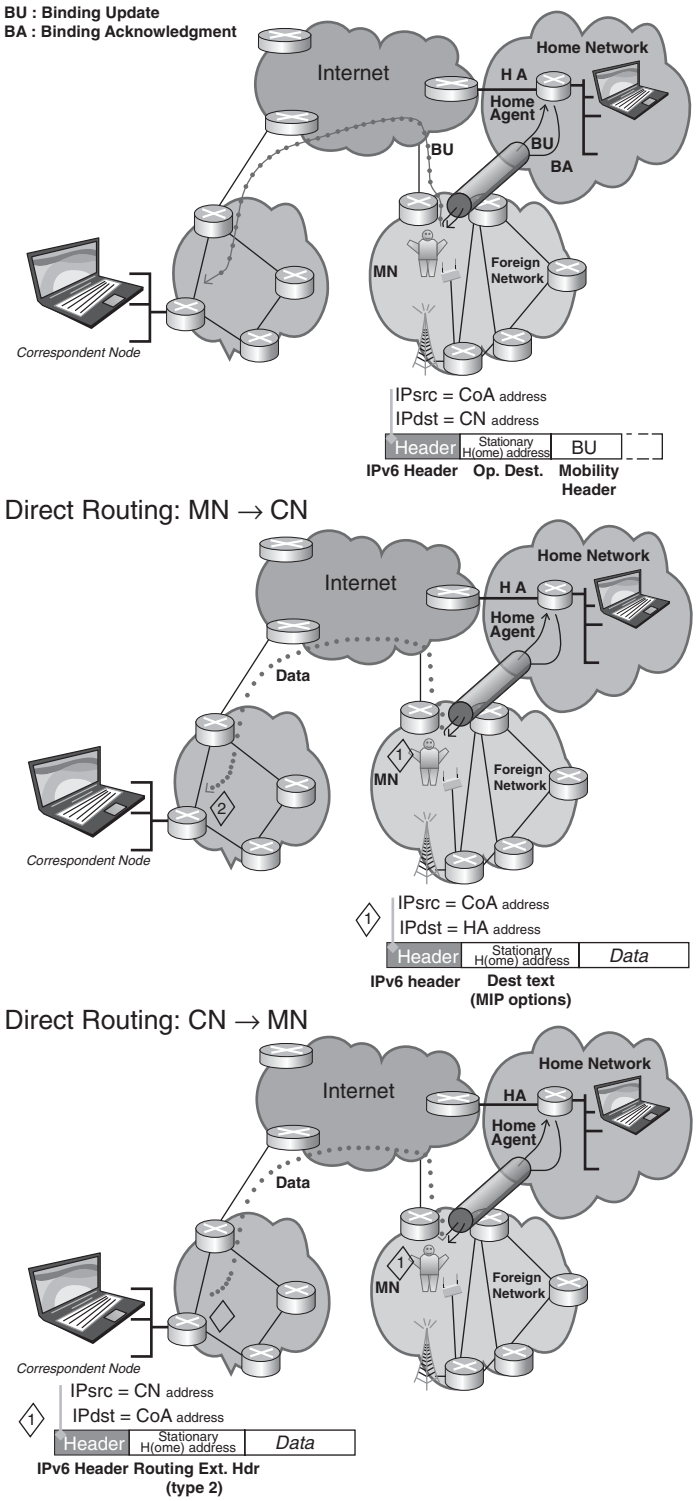


FIGURE 8.5 Direct communication.

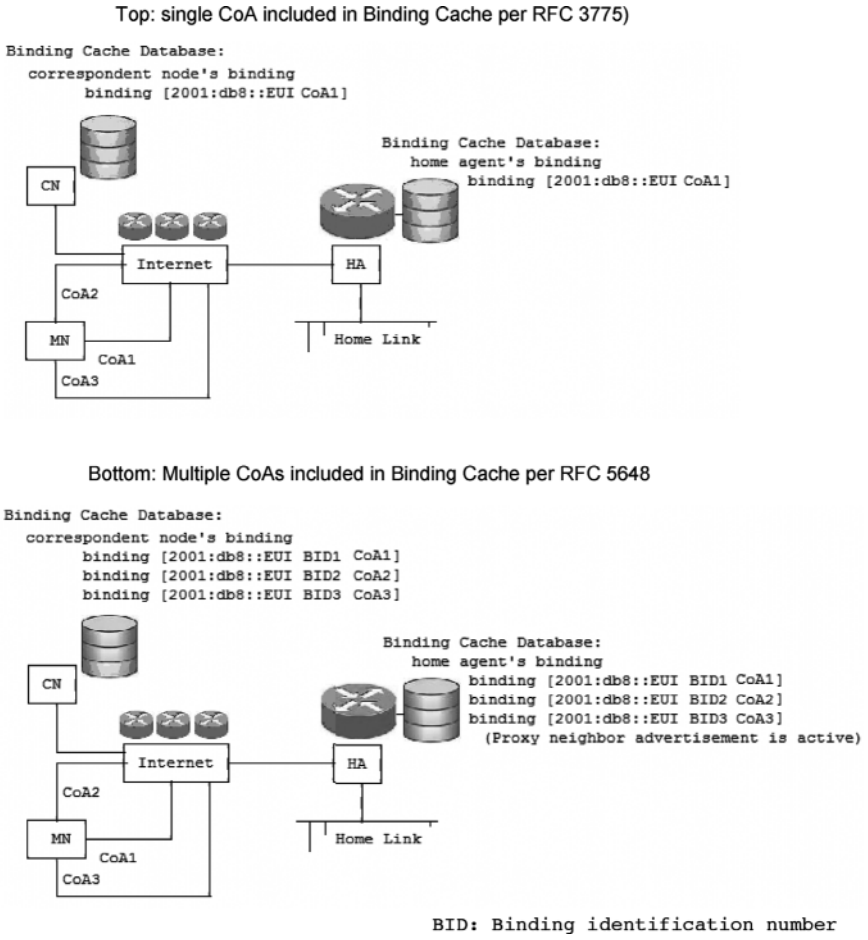


FIGURE 8.6 CoA registration.

a shared secret between the MN and the home authentication, authorization, and accounting (AAA) server; this is in contrast with an earlier version of the MIPv6 model. Automatically providing the collection of home address, HA address, and keying material is generally referred to as the MIPv6 bootstrapping problem (4).

Table 8.2 provides a listing (from reference 5) of MIPv6 implementations as available in the recent past.

The sections that follow provide more in-depth information about MIPv6 processes and procedures.

8.2 PROTOCOL DETAILS

The sections that follow are summarized from relevant RFCs, including RFC 3775. Only a subset of concepts is described; the interested reader should always consult the

TABLE 8.2 Recent Implementations on MIPv6 Technology (Partial List)

- 6 Wind
- Cisco—HA
- Elmic systems now Treck Inc.
- Ericsson
- HP—HP-UX (HA, CN) and Tru64 (HA, CN)
- Keio University (wide) —HA, MN, CN, and IPsec
- Microsoft Window XP, Vista
- NEC-MN, HA, CN, and IPsec
- Nokia-MN, HA, CN
- Samsung—MN, CN
- Siemens
- University of Helsinski (Linux) —MN, CN
- 6NET MIPv6 implementation survey

primary RFC for complete and detailed information. The key concepts were already discussed in Section 8.1, but this section provides additional details.

8.2.1 Generic Mechanisms

8.2.1.1 MIPv6 Basic Operation As noted, an MN is always addressable at its home address, whether it is currently attached to its home link or is away from home. The "home address" is an IP address assigned to the MN within its home subnet prefix on its home link. While an MN is at home, packets addressed to its home address are routed to the MN's home link using traditional routing mechanisms. While an MN is attached to some foreign link away from home, it is also addressable at one or more CoAs. A CoA is an IP address associated with an MN that has the subnet prefix of a particular foreign link. The MN acquires its CoA using traditional IPv6 mechanisms, such as stateless or stateful autoconfiguration. As long as the MN stays in this location, packets addressed to this CoA will be routed to the MN. The MN may also accept packets from several CoAs, this being the case, for example, when it is moving to a new location but still reachable at the previous link. The MIPv6 specification requires that home and CoAs must be unicast routable addresses. The association between an MN's home address and CoA is known as a "binding" for the MN. While away from home, an MN registers its primary CoA with a router on its home link, requesting this router to function as the "HA" for the MN. The MN performs this binding registration by sending a BU message to the HA. The HA replies to the MN by returning a BA message. The exchange of BUs, BAs, and other control messages is referred to as "signaling."

Note: In addition to the binding cache, each HA also maintains an HA list. This list has information about routers on the same link that is acting as an HA and is used by the HAAD mechanism—a router is known to be acting as an HA, if it sends

TABLE 8.3 Binding Cache Content

Content	Description
Home address	The home address of the MN for which this is the binding cache entry. This field is used as the key for searching the binding cache for the destination address of a packet being sent
CoA	The CoA for the MN indicated by the home address field in this binding cache entry
Lifetime value	The lifetime value indicates the remaining lifetime for this binding cache entry. The lifetime value is initialized from the lifetime field in the BU that created or last modified this binding cache entry
Flag	This flag indicates whether or not this binding cache entry is a home registration entry (applicable only on nodes that support HA functionality)
Maximum value	The maximum value of the sequence number field received in previous BUs for this home address. The sequence number field is 16 bits long (it uses modulo 2^{16} math)
Usage information	Usage information for this binding cache entry. This is needed to implement the cache replacement policy in use in the binding cache. Recent use of a cache entry also serves as an indication that a BRR should be sent when the lifetime of this entry nears expiration

a router advertisement in which the HA (H) bit is set. The HA maintains a separate HA list for each link on which it is serving as an HA.

Any node communicating with an MN is referred to as a "correspondent node" of the MN and may itself be either a stationary device or a mobile device. MNs are also able to provide information about their current location to CNs. This happens through the correspondent registration. As a part of this procedure, a return-routability test is performed in order to authorize the establishment of the binding.

There are two possible modes for communications between the MN and a CN, as previously noted, as follows:

- The first mode, "bidirectional tunneling," *does not require MIPv6 support from the CN* and is available even if the MN has not registered its current binding with the CN. Packets from the CN are routed to the HA and then tunneled to the MN. Packets to the CN are tunneled from the MN to the HA ("reverse tunneled") and then routed normally from the home network to the CN. In this mode, the HA uses proxy neighbor discovery to intercept any IPv6 packets addressed to the MN's home address on the home link. Each intercepted packet is tunneled to the MN's primary CoA.
- The second mode, "route optimization[4]" (also called above, "direct routing"), requires the MN to register its current binding at the CN. Packets from the CN can be routed directly to the CoA of the MN. When sending a packet to any IPv6 destination, the CN checks its cached bindings (see Table 8.3) for an entry for

[4]The acronym RO is also used by some practitioners.

the packet's destination address. If a cached binding for this destination address is found, the node uses a new type of IPv6 routing header to route the packet to the MN by way of the CoA indicated in this binding. Routing packets directly to the MN's CoA allows the shortest communications path to be used. It also eliminates congestion at the MN's HA and home link. In addition, the impact of any possible failure of the HA or networks on the path to or from it is reduced.

When routing packets directly to the MN, the CN sets the destination address in the IPv6 header to the CoA of the MN. A new type of IPv6 routing header is also added to the packet to carry the desired home address. Similarly, the MN sets the source address in the packet's IPv6 header to its current CoAs. The MN adds a new IPv6 "home address" destination option to carry its home address. The inclusion of home addresses in these packets makes the use of the CoA transparent above the network layer (e.g., at the transport layer).

Note: MIPv6 requires the MN to know its HA address, its own home address, and the cryptographic materials (e.g., shared keys or certificates) needed to set up IPsec SAs with the HA in order to protect MIPv6 signaling. The MIPv6 base protocol does not specify any method to automatically acquire this information, which means that network administrators are normally required to manually set configuration data on MNs and HAs. However, in real deployments, manual configuration does not scale as the MNs increase in number (6). A bootstrapping process can be beneficial. Also, according to the latest RFCs, the only SA that is preconfigured is a shared secret between the MN and the home AAA server; this is in contrast with an earlier version of the MIPv6 model.

8.2.1.2 IPv6 Protocol Extensions

MIPv6 defines a new IPv6 protocol, using the mobility header. This header is used to carry the messages summarized in Table 8.4.

8.2.1.3 New IPv6 Destination Option

MIPv6 defines a new IPv6 destination option, the home address destination option. This option is described in more detail in Section 8.2.2.

8.2.1.4 New IPv6 ICMP Messages

As alluded to earlier, MIPv6 also introduces four new ICMPv6 message types, two for use in the dynamic HAAD mechanism and two for renumbering and mobile configuration mechanisms.

- *HAAD request.* The ICMP HAAD request message is used by an MN to initiate the dynamic HAAD mechanism. The MN sends the HAAD request message to the MIPv6 HA anycast address for its own home subnet prefix.
- *HAAD reply.* The ICMP HAAD reply message is used by an HA to respond to an MN that uses the dynamic HAAD mechanism.
- *Mobile prefix solicitation*. The ICMP mobile prefix solicitation message is sent by an MN to its HA while it is away from home. The purpose of the message is to solicit a mobile prefix advertisement from the HA, which will allow the MN

TABLE 8.4 Mobility Header Messages

Message	Description
HoTi HoT Care-of test init Care-of test	These messages are used to perform the return-routability procedure from the MN to a CN
BU	Message is used by an MN to notify a CN or the MN's HA of its current binding. The BU sent to the MN's HA to register its primary CoA is marked as a "home registration"
BA	Message is used to acknowledge receipt of a BU, if an acknowledgement was requested in the BU, the BU was sent to an HA, or an error occurred
BRR	Message is used by a CN to request an MN to re-establish its binding with the CN. This message is typically used when the cached binding is in active use, but the binding's lifetime is close to expiration. The CN may use, for instance, recent traffic and open transport layer connections as an indication of active use
Binding error	Message is used by the CN to signal an error related to mobility, such as an inappropriate attempt to use the home address destination option without an existing binding

to gather prefix information about its home network. This information can be used to configure and update home address(es) according to changes in prefix information supplied by the HA.

- *Mobile prefix advertisement.* An HA will send a mobile prefix advertisement to an MN to distribute prefix information about the home link while the MN is traveling away from the home network. This occurs in response to a mobile prefix solicitation with an advertisement, or by an unsolicited advertisement.

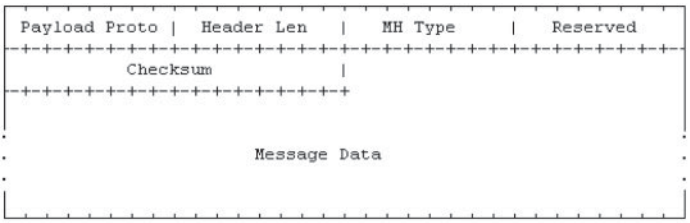
8.2.1.5 Mobile IPv6 Security MIPv6 incorporates a number of security features. These include the protection of BUs both to HAs and to CNs, the protection of mobile prefix discovery, and the protection of the mechanisms that MIPv6 uses for transporting data packets:

- BUs are protected by the use of IPsec extension headers, or by the use of the binding authorization data option (this option employs a binding management key, Kbm, which can be established through the return-routability procedure).
- Mobile prefix discovery is protected through the use of IPsec extension headers.
- Mechanisms related to transporting payload packets—such as the home address destination option and type 2 routing header—have been specified in a manner that restricts their use in attacks.

Although these basic security mechanisms are adequate for some environments and applications, there are limitations with these for other environments.

8.2.2 New IPv6 Protocol, Message Types, and Destination Option

8.2.2.1 Mobility Header The mobility header is an extension header used by MNs, CNs, and HAs in all messaging related to the creation and management of bindings. The subsections within this section describe the message types that may be sent using the mobility header. The mobility header is identified by a next header value of 135 in the immediately preceding header and has the format depicted in Figure 8.7.



Payload Proto	8-bit selector. Identifies the type of header immediately following the mobility header. Uses the same valu es as the IPv6 next header field. This field is intended to be used by a future extension.
Header Len	8-bit unsigned integer, representing the length of the mobility header in units of 8 octets, excluding the first 8 octets.
MH Type	8-bit selector. Identifies the particular mobility message in question.
Reserved	8-bit field reserved for future use. The value must be initialized to zero by the sender and must be ignored by the receiver.
Checksum	16-bit unsigned integer. This field contains the checksum of the mobility header.
Message Data	A variable length field containing the data specific to the indicated mobility header type.

The message types are as follows:

Binding refresh request (BRR) Message	The BRR message requests a mobile node to update its mobility binding. This message is sent by correspondent nodes. The BRR message uses the MH Type value 0.
Home test init (HoTI) message	A mobile node uses the HoTI message to initiate the return-routability procedure and request a home keygen token from a correspondent node. The Home test init message uses the MH type value 1. This message is tunneled through the home agent when the mobile node is away from home. Such tunneling should employ IPsec ESP in tunnel mode between the HA and the mobile node. This protection is indicated by the IPsec security policy database.
Care-of test init (CoTI) message	A mobile node uses the CoTI message to initiate the return-routability procedure and request a care-of keygen token from a correspondent node. The Care-of test init message uses the MH type value 2.
Home test (HoT) message	The HoT message is a response to the Home test init message and is sent from the correspondent node to the mobile node. The HoT message uses the MH type value 3.
Care-of test (CoT) message	The CoT message is a response to the CoT Init message and is sent from the correspondent node to the mobile node. The CoT message uses the MH type value 4.
Binding update (BU) message	The BU message is used by a mobile node to notify other nodes of a new CoA for itself. The BU uses the MH type value 5.
Binding acknowledgement (BA) message	The BA is used to acknowledge receipt of a BU. The BA has the MH type value 6.
Binding error (BE) message	The BE message is used by the correspondent node to signal an error related to mobility, such as an inappropriate attempt to use the home address destination option without an existing binding. The BE message uses the MH type value 7.

FIGURE 8.7 Mobility header (details).

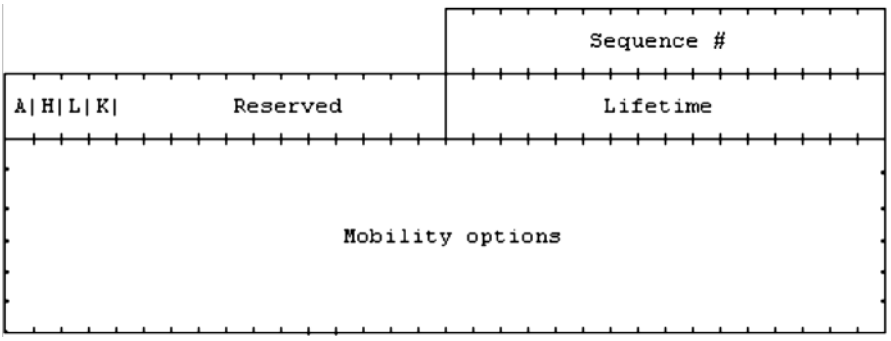


FIGURE 8.8 Message data field for BU (BU) message.

Two important messages are the BU message and the BA message.

The BU message is used by an MN to notify other nodes of a new CoA it has acquired. The format of the message data field in the mobility header for the BU message is shown in Figure 8.8. The fields/flags are described next.

- Acknowledge (A). The acknowledge (A) bit is set by the sending MN to request a BA be returned upon receipt of the BU.
- Home registration (H). The home registration (H) bit is set by the sending MN to request that the receiving node should act as this node's HA. The destination of the packet carrying this message must be that of a router sharing the same subnet prefix as the home address of the MN in the binding.
- Link-local address compatibility (L). The link-local address compatibility (L) bit is set when the home address reported by the MN has the same interface identifier as the MN's link-local address.
- Key management mobility capability (K). If this bit is cleared, the protocol used for establishing the IPsec SAs between the MN and the HA does not survive movements; it may then have to be rerun.
- Reserved. These fields are unused. They must be initialized to zero by the sender and must be ignored by the receiver.
- Sequence number. A 16-bit unsigned integer used by the receiving node to sequence BUs and by the sending node to match a returned BA with this BU.
- Lifetime. 16-bit unsigned integer. The number of time units remaining before the binding must be considered expired. A value of zero indicates that the binding cache entry for the MN must be deleted.
- Mobility options. Variable-length field of such length that the complete mobility header is an integer multiple of 8 octets long. This field contains zero or more Type/Length/Value (TLV)-encoded[5] mobility options. The following options are valid in a BU:

[5]Type, Length, Value.

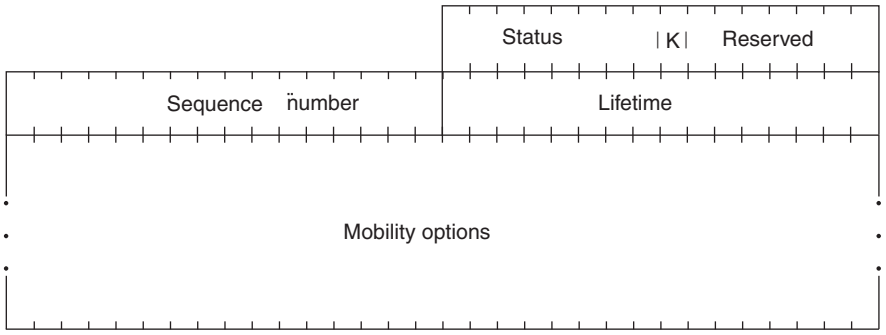


FIGURE 8.9 Message data field for BA message.

- Binding authorization data option (this option is mandatory in BUs sent to a CN);
- Nonce indices option;
- Alternate CoA option

The CoA is specified either by the source address field in the IPv6 header or by the alternate CoA option, if present. IPv6 source address must be a topologically correct source address. BUs for a CoA that is not a unicast routable address must be silently discarded. Similarly, the BU must be silently discarded if the CoA appears as a home address in an existing binding cache entry, with its current location creating a circular reference back to the home address specified in the BU (possibly through additional entries).

The BA message is used to acknowledge the receipt of a BU. The format of the message data field in the mobility header for the BA message is shown in Figure 8.9. The fields/flags are described next.

– Key management mobility capability (K). If this bit is cleared, the protocol used by the HA for establishing the IPsec SAs between the MN and the HA does not survive movements (it may then have to be rerun).
– Reserved. These fields are unused. They must be initialized to zero by the sender and must be ignored by the receiver.
– Status. 8-bit unsigned integer indicating the disposition of the BU. Values of the status field less than 128 indicate that the BU was accepted by the receiving node. Values greater than or equal to 128 indicate that the BU was rejected by the receiving node. The following status values were originally defined:

0	BU accepted
1	Accepted but prefix discovery necessary
128	Reason unspecified
129	Administratively prohibited
130	Insufficient resources

131	Home registration not supported
132	Not home subnet
133	Not HA for this MN
134	Duplicate address detection failed
135	Sequence number out of window
136	Expired home nonce index
137	Expired care-of nonce index
138	Expired nonces
139	Registration type change disallowed

- Sequence number. The sequence number in the BA is copied from the sequence number field in the BU. It is used by the MN in matching this BA with an outstanding BU.
- Lifetime. The granted lifetime, in time units of 4 s, for which this node should retain the entry for this MN in its binding cache.
- Mobility options. Variable-length field of such length that the complete mobility header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver must ignore and skip any options which it does not understand.

BUs and BAs follow the rules discussed in RFC 3776[6] (7) and summarized in Table 8.5.

A CN registration involves six message transmissions at the MN, totaling about 376 bytes. This signaling overhead may be acceptable if movements are infrequent. For example, an MN that moves once every 30 min generates an average of 1.7 bps of signaling traffic. Higher mobility causes more substantial overhead, however. A cell size of 100 m and a speed of 120 km/h yields a change in IP connectivity every 3 s and about 1000 bps of signaling traffic. This is significant compared to a highly compressed voice stream with a typical data rate of 10,000 to 30,000 bps. Furthermore, base MIPv6 requires MNs to renew a correspondent registration at least every 7 min. The signaling overhead amounts to 7.16 bps if the MN communicates with a stationary node. It doubles if both peers are mobile. This overhead may be negligible when the nodes communicate, but it can be an issue for MNs that are inactive and stay at the same location for a while because these MNs are typically designed to go to standby mode to conserve battery power. Also, the periodic refreshments consume a fraction of the wireless bandwidth that one could use more efficiently (3).

8.2.2.2 Mobility Options Mobility messages can include zero or more mobility options. This allows optional fields that may not be needed in every use of a particular mobility header, as well as future extensions to the format of the messages. Such options are included in the message data field of the message itself, after the fixed portion of the message data. The presence of such options is be indicated by the header Len of the mobility header. See Figure 8.10.

[6]RFC 3776 has been updated in RFC 4877.

TABLE 8.5 BUs and BAs

MN Status	Message	Description
MN is away from its home	BUs	When the MN is away from its home, the BUs sent by it to the HA must support at least the following headers in the following order: IPv6 header (source = CoA, destination = HA) Destination options header Home address option (home address) ESP header in transport mode Mobility header BU Alternate CoA option (CoA)
	BAs	The BA sent back to the MN when it is away from home must support at least the following headers in the following order: IPv6 header (source = HA, destination = CoA) Routing header (type 2) Home address ESP header in transport mode Mobility header BA
MN is at home	BUs	When the MN is at home, the above rules are different since the MN can use its home address as a source address; this typically happens for the de-registration BU when the mobile is returning home. Here the BUs must support at least the following headers in the following order: IPv6 header (source = home address, destination = HA) ESP header in transport mode Mobility header BU
	BAs	The BA messages sent to the home address must support at least the following headers in the following order: IPv6 header (source = HA, destination = home address) ESP header in transport mode Mobility header BA

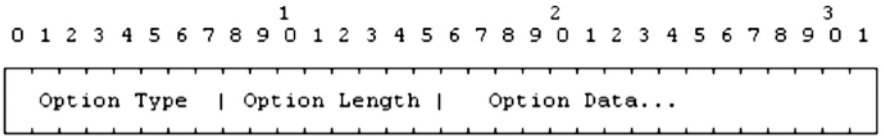


FIGURE 8.10 Format of mobility options.

8.2.2.3 Home Address Option The home address option is carried by the destination option extension header (next header value = 60). It is used in a packet sent by an MN while away from home, to inform the recipient of the MN's home address. See Figure 8.11.

8.2.2.4 Type 2 Routing Header MIPv6 defines a new routing header variant, the type 2 routing header, to allow the packet to be routed directly from a correspondent to the MN's CoA. The MN's CoA is inserted into the IPv6 destination address field. Once the packet arrives at the CoA, the MN retrieves its home address from the routing header; this address is used as the final destination address for the packet. The type 2 routing header is shown in Figure 8.12.

The new routing header uses a different type than defined for "regular" IPv6 source routing, enabling firewalls to apply different rules to source routed packets than to MIPv6. This routing header type (type 2) is restricted to carry only one IPv6 address. All IPv6 nodes that process this routing header must verify that the address contained within is the node's own home address in order to prevent packets from being forwarded outside the node. The IP address contained in the routing header must be a unicast routable address, being that it is the MN's home address. Furthermore, if the scope of the home address is smaller than the scope of the CoA, the MN must discard the packet.

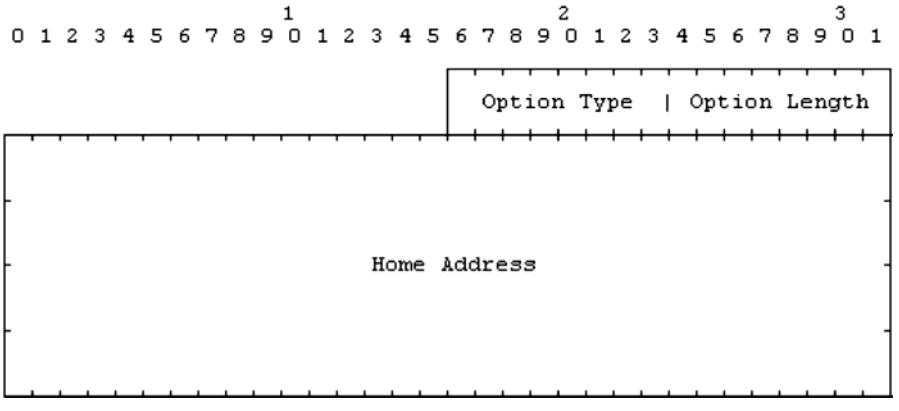
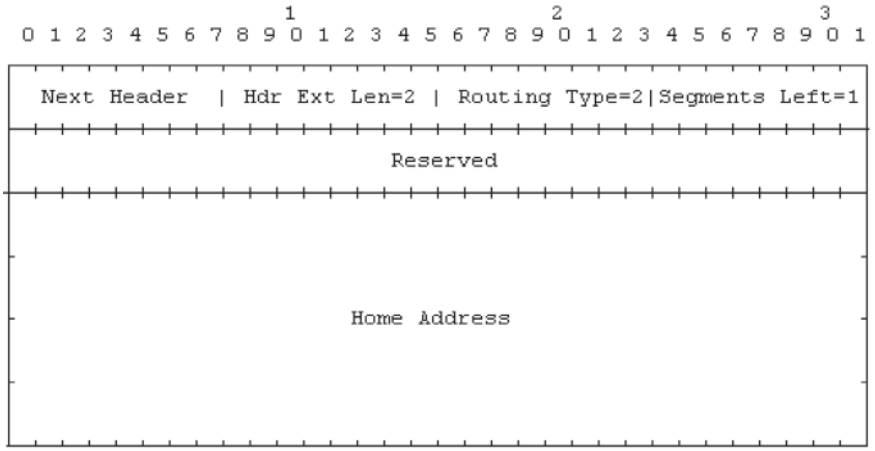


FIGURE 8.11 Format of home address option.



Next header	8-bit selector. Identifies the type of header immediately following the routing header. Uses the same values as the IPv6 next header field.
Hdr ext Len	2 (8-bit unsigned integer); length of the routing header in 8-octet units, not including the first 8 octets.
Routing type	2 (8-bit unsigned integer).
Segments left	1 (8-bit unsigned integer).
Reserved	32-bit reserved field. The value must be initialized to zero by the sender and must be ignored by the receiver.
Home address	The home address of the destination mobile node.

FIGURE 8.12 Type 2 routing header.

8.2.3 Modifications to IPv6 Neighbor Discovery

Modifications to existing protocols are described herewith as described in RFC 3775.

8.2.3.1 Modified Router Advertisement Message MIPv6 modifies the format of the router advertisement message by the addition of a single flag bit to indicate that the router sending the advertisement message is serving as an HA on this link.

8.2.3.2 Modified Prefix Information Option MIPv6 requires knowledge of a router's global address in building an HA list as part of the dynamic HAAD mechanism. MIPv6 extends neighbor discovery defined in RFC 2461 (8) to allow a router to advertise its global address by the addition of a single flag bit in the format of a prefix information option for use in router advertisement messages.

8.2.3.3 New Advertisement Interval Option MIPv6 defines a new advertisement interval option, used in router advertisement messages to advertise the interval at which the sending router sends unsolicited multicast router advertisements.

8.2.3.4 New HA Information Option MIPv6 defines a new HA information option, used in router advertisements sent by an HA to advertise information specific to this router's functionality as an HA.

8.2.3.5 Changes to Sending Router Advertisements The basic NDP specification limits routers to a minimum interval of 3s between sending unsolicited multicast router advertisement messages from any given network interface (limited by MinRtrAdvInterval and MaxRtrAdvInterval). This limitation, however, is not suitable to providing timely movement detection for MNs. MNs detect their own movement by learning the presence of new routers as the MN moves into wireless transmission range of them (or physically connects to a new wired network), and by learning that previous routers are no longer reachable. MNs must be able to quickly detect when they move to a link served by a new router, so that they can acquire a new CoA and send BUs to register this CoA with their HA and to notify CNs as needed. One method that can provide for faster movement detection is to increase the rate at which unsolicited router advertisements are sent. MIPv6 relaxes this limit such that routers may send unsolicited multicast router advertisements more frequently. This method can be applied where the router is expecting to provide service to visiting MNs (e.g., wireless network interfaces), or on which it is serving as an HA to one or more MNs (who may return home and need to hear its advertisements).

8.2.4 Requirements for Various IPv6 Nodes

MIPv6 imposes specific requirements on the functions provided by different types of IPv6 nodes (except for a generic IPv6 node acting as CN). These are summarized in Table 8.6.

8.2.5 Correspondent Node Operation

IPv6 nodes with route optimization support must maintain a binding cache of bindings for other nodes (as shown in Table 8.3); a separate Binding Cache is typically maintained by each IPv6 node for each of its unicast routable addresses. Specifically, CNs are required to support the following functionality:

- Processing mobility headers
- Packet processing
- Return-routability procedure
- Processing bindings
- Cache replacement policy

8.2.5.1 Processing Mobility Headers Mobility header processing follows the process of Figure 8.13. Subsequent checks depend on the particular mobility header.

TABLE 8.6 Requirements for Various IPv6 Nodes

Nodes	Requirement
IPv6 nodes	Any IPv6 node may at any time be a CN of an MN, either sending a packet to an MN or receiving a packet from an MN. There are no MIPv6-specific requirements for such nodes and basic IPv6 capabilities are sufficient. If an MN attempts to set up route optimization with a node with only basic IPv6 support, an ICMP error will signal that the node does not support such optimizations and communications will flow through the HA
IPv6 nodes with support for route optimization. Nodes that implement route optimization are a subset of all IPv6 nodes on the Internet. The ability of a CN to participate in route optimization is essential for the efficient operation of the IPv6 environment	The node must be able to validate a home address option using an existing binding cache entry The node must be able to insert a type 2 routing header into packets being sent to an MN Unless the CN is also acting as an MN, it must ignore type 2 routing headers and silently discard all packets that it has received with such headers The node should be able to interpret ICMP messages. The node must be able to send Binding Error messages. The node must be able to process Mobility Headers. The node must be able to participate in a return-routability procedure. The node must be able to process BU messages. The node must be able to return a BA. The node must be able to maintain a Binding Cache of the bindings received in accepted BUs. The node should allow route optimization to be administratively enabled or disabled. The default should be enabled.
IPv6 routers. All IPv6 routers, even those not serving as an HA for MIPv6, have an effect on how well MNs can communicate	Every IPv6 router should be able to send an advertisement interval option in each of its router advertisements, to aid movement detection by MNs. The use of this option in router advertisements should be configurable Every IPv6 router should be able to support sending unsolicited multicast router advertisements at a fast rate (the used rate should then be configurable) Each router should include at least one prefix with the router address (R) bit set and with its full IP address in its router advertisements Routers supporting filtering packets with routing headers should support different rules for type 0 and type 2 routing headers so that filtering of source routed packets (type 0) will not necessarily limit MIPv6 traffic which is delivered via type 2 routing headers

(*continued*)

TABLE 8.6 (*Continued*)

Nodes	Requirement
IPv6 routers that serve as an HA. In order for an MN to operate correctly while away from home, at least one IPv6 router on the MN's home link must function as an HA for the MN	Every HA must be able to maintain an entry in its binding cache for each MN for which it is serving as the HA Every HA must be able to intercept packets (using proxy neighbor discovery) addressed to an MN for which it is currently serving as the HA, on that MN's home link, while the MN is away from home Every HA must be able to encapsulate such intercepted packets in order to tunnel them to the primary CoA for the MN indicated in its binding in the HA's binding cache Every HA must support decapsulating reverse tunneled packets sent to it from an MN's home address. Every HA must also check that the source address in the tunneled packets corresponds to the currently registered location of the MN The node must be able to process mobility headers. Every HA must be able to return a BA in response to a BU Every HA must maintain a separate HA list for each link on which it is serving as an HA Every HA must be able to accept packets addressed to the MIPv6 HA anycast address for the subnet on which it is serving as an HA and must be able to participate in dynamic HAAD Every HA should support a configuration mechanism to allow a system administrator to manually set the value to be sent by this HA in the HA preference field of the HA information option in router advertisements that it sends Every HA should support sending ICMP mobile prefix advertisements and should respond to mobile prefix solicitations. If supported, this behavior must be configurable, so that HAs can be configured to avoid sending such prefix advertisements according to the needs of the network administration in the home domain Every HA must support IPsec encapsulating security payload (ESP) for protection of packets belonging to the return-routability procedure Every HA should support the multicast group membership control protocols. If this support is provided, the HA must be capable of using it to determine which multicast data packets to forward via the tunnel to the MN HAs may support stateful address autoconfiguration for MNs

TABLE 8.6 (*Continued*)

Nodes	Requirement
IPv6 MNs	The node must maintain a BU list
	The node must support sending packets containing a home address option and follow the required IPsec interaction
	The node must be able to perform IPv6 encapsulation and decapsulation
	The node must be able to process type 2 routing header
	The node must support receiving a binding error message
	The node must support receiving ICMP errors
	The node must support movement detection, CoA formation, and returning home
	The node must be able to process mobility headers
	The node must support the return-routability procedure
	The node must be able to send BUs
	The node must be able to receive and process BAs
	The node must support receiving a BRR by responding with a BU
	The node must support receiving mobile prefix advertisements and reconfiguring its home address based on the prefix information contained therein
	The node should support use of the dynamic HAAD mechanism
	The node must allow route optimization to be administratively enabled or disabled. The default should be enabled
	The node may support the multicast address listener part of a multicast group membership protocol. If this support is provided, the MN must be able to receive tunneled multicast packets from the HA
	The node may support stateful address autoconfiguration mechanisms such as dynamic host configuration protocol version 6 (DHCPv6) on the interface represented by the tunnel to the HA

8.2.5.2 Packet Processing Packet processing covers the following subactivities:

- Receiving packets with home address option
- Sending packets to an MN
- Sending binding error messages
- Receiving ICMP error messages

These subactivities are described next.

Receiving packets with home address option. The CN must process the option in a manner consistent with exchanging the home address field from the home address option into the IPv6 header and replacing the original value of the source address field there. After all IPv6 options have been processed, the upper layers can process the packet without the knowledge that it came originally from a CoA or that a home address option was used.

Packets containing a home address option must be dropped if the given home address is not a unicast routable address. MNs can include a home address destination

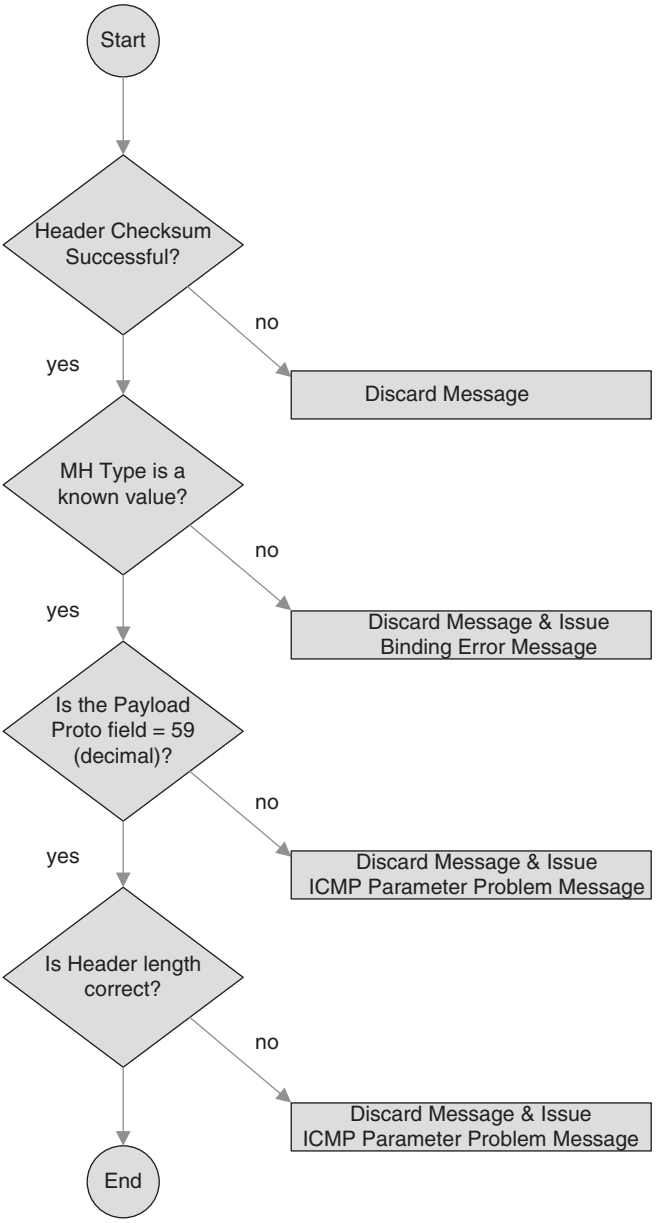


FIGURE 8.13 Mobility header processing.

option in a packet if they believe the CN has a binding cache entry for the home address of an MN. Packets containing a home address option must be dropped if there is no corresponding binding cache entry. A corresponding binding cache entry must have the same home address as appears in the home address destination option, and the currently registered CoA must be equal to the source address of the packet. These actions are not done for packets that contain a home address option and a BU. If the packet is dropped due to these conditions, the CN must send the binding error message.

Sending packets to an MN. Before sending any packet (except when sending an IPv6 neighbor discovery packet), the sending node should examine its binding cache for an entry for the destination address to which the packet is being sent. If the sending node has a binding cache entry for this address, the sending node should use a type 2 routing header to route the packet to this MN (the destination node) by way of its CoA. For example, if there are no additional routing headers in this packet beyond those needed by MIPv6, the CN could set the fields in the packet's IPv6 header and routing header as follows:

- The destination address in the packet's IPv6 header is set to the MN's home address (the original destination address to which the packet was being sent).
- The routing header is initialized to contain a single route segment, containing the MN's CoA copied from the binding cache entry. The segments left field is, however, temporarily set to zero.

If, on the other hand, the sending node has no binding cache entry for the destination address to which the packet is being sent, the sending node simply sends the packet normally, with no routing header. If the destination node is not an MN (or is an MN that is currently at home), the packet will be delivered directly to this node and processed normally by it. If, however, the destination node is an MN that is currently away from home, the packet will be intercepted by the MN's HA and tunneled to the MN's current primary CoA.

Sending binding error messages. A binding error message is sent directly to the address that appeared in the IPv6 source address field of the offending packet (if the source address field does not contain a unicast address, the binding error message must not be sent). The home address field in the binding error message is copied from the home address field in the home address destination option of the offending packet, or set to the unspecified address if no such option appeared in the packet.

Receiving ICMP error messages. When the CN has a binding cache entry for an MN, all traffic destined to the MN goes directly to the current CoA of the MN using a routing header. Any ICMP error message caused by packets on their way to the CoA will be returned in the normal manner to the CN. On the other hand, if the CN has no binding cache entry for the MN, the packet will be routed through the MN's home link. In all cases, any meaningful ICMP error messages caused by packets from a CN to an MN will be returned to the CN.

TABLE 8.7 Return-Routability Actions of the CN

Action	Description
Receiving HoTi messages	Upon receiving a HoTi message, the CN verifies that the packet does not include a home address destination option. Any packet carrying a HoTi message that fails to satisfy all of these tests must be silently ignored. Otherwise, in preparation for sending the corresponding HoT message, the CN checks that it has the necessary material to engage in a return-routability procedure. The CN must have a secret Kcn and a nonce; it does not have this material yet, it must produce it before continuing with the return-routability procedure
Receiving care-of test init messages	Upon receiving a HoTi message, the CN verifies that the packet does not include a home address destination option. Any packet carrying a care-of test init message that fails to satisfy all of these tests must be silently ignored. Otherwise, in preparation for sending the corresponding care-of test message, the CN checks that it has the necessary material to engage in a return-routability procedure
Sending HoT messages	The CN creates a home keygen token and uses the current nonce index as the home nonce index; it then creates a HoT message and sends it to the MN at the latter's home address
Sending care-of test messages	The CN creates a care-of keygen token and uses the current nonce index as the care-of nonce index; it then creates a care-of test message and sends it to the MN at the latter's CoA

8.2.5.3 Return-Routability Procedure Actions taken by a CN during the return-routability procedure are listed in Table 8.7.

8.2.5.4 Processing Bindings Messages related to bindings are as follows:

- **Receiving BUs**. Before accepting a BU, the receiving node must validate the BU. This validation entails the following: the packet must contain a unicast routable home address, either in the home address option or in the source address if the home address option is not present; also, the sequence number field in the BU is greater than the sequence number received in the previous valid BU for this home address, if any (if the receiving node has no BINDING CACHE entry for the indicated home address, it must accept any sequence number value in a received BU from this MN); also, other tests must pass.
- **Requests to cache a binding**. There is a need to process a valid BU that requests a node to cache a binding, for which the home registration (H) bit is not set in the BU. In this case, the receiving node should create a new entry in its binding cache for this home address, or update its existing binding cache entry for this home address, if such an entry already exists. The lifetime for the binding cache entry is initialized from the lifetime field specified in the BU, although this lifetime may be reduced by the node caching the binding; the lifetime for the binding cache entry cannot be greater than the lifetime value specified in the

BU. Any binding cache entry must be deleted after the expiration of its lifetime. The CN may refuse to accept a new binding cache entry if it does not have sufficient resources.

- **Requests to delete a binding**. There is a need to process a valid BU that requests a node to delete a binding when the home registration (H) bit is not set in the BU. Any existing binding for the given home address must be deleted. A binding cache entry for the home address must not be created in response to receiving the BU. If the binding cache entry was created by use of return-routability nonces, the CN must ensure that the same nonces are not used again with the particular home and CoA. If both nonces are still valid, the CN has to remember the particular combination of nonce indexes, addresses, and sequence number as illegal until at least one of the nonces has become too old.
- **Sending BAs**. A BA may be sent to indicate receipt of a BU. If the node accepts the BU and creates or updates an entry for this binding, the status field in the BA must be set to a value less than 128. Otherwise, the status field must be set to a value greater than or equal to 128.
- **Sending binding refresh requests (BRRs).** If a binding cache entry being deleted is still in active use when sending packets to an MN, then the next packet sent to the MN will be routed normally to the MN's home link. Communication with the MN continues, but the tunneling from the home network creates additional overhead and latency in delivering packets to the MN. If the sender is aware that the binding cache entry is still in active use, it may send a BRR message to the MN in an attempt to avoid this overhead and latency due to deleting and recreating the binding cache entry. This message is always sent to the home address of the MN. The CN may retransmit BRR messages as long as the rate limitation is applied. The CN must stop retransmitting when it receives a BU.

8.2.5.5 Cache Replacement Policy A node may maintain a separate timer for each entry in its binding cache. When creating or updating a binding cache entry in response to a received and accepted BU, the node sets the timer for this entry to the specified lifetime period; entries in a node's binding cache are deleted after the expiration of the lifetime specified in the BU from which the entry was created or last updated. A node may also opt to drop any entry already in its binding cache in order to make space for a new entry. If the node sends a packet to a destination for which it has dropped the entry from its binding cache, the packet will be routed through the MN's home link; the MN can detect this and establish a new binding if necessary.

8.2.6 HA Node Operation

HA operations entail the following functions:

- Maintaining the binding cache and the HA list
- Processing mobility headers

- Processing bindings
  - Primary CoA registration
  - Primary CoA de-registration
- Packet processing
  - Intercepting packets for an MN
  - Processing intercepted packets
  - Multicast membership control
  - Stateful Address autoconfiguration
  - Handling reverse tunneled packets
  - Protecting return-routability packets
- Dynamic HAAD
- Sending prefix information to the MN

We have generally described this (or comparable) functionality earlier in this chapter; hence we will not discuss it further herewith.

8.2.7 Mobile Node Operation

MN operations entail the following functions:

- Maintaining the BU list
- Processing bindings
  - Sending BUs to the HA
  - Correspondent registration
  - Receiving BAs
  - Receiving BRRs
- Processing mobility headers
- Packet processing
  - Sending packets while away from home
  - Interaction with outbound IPsec processing
  - Receiving packets while away from home
  - Routing multicast packets
  - Receiving ICMP error messages
  - Receiving binding error messages
- HA and prefix management
  - Dynamic HAAD
  - Sending mobile prefix solicitations
  - Receiving mobile prefix advertisements
- Movement support
  - Movement detection

- Forming new CoA
- Using multiple CoA
- Returning home

- Return-routability procedure
  - Sending test init messages
  - Receiving test messages
  - Protecting return-routability packets
- Retransmissions and rate limiting

The BU list records information for each BU sent by this MN, in which the lifetime of the binding has not yet expired. The BU list includes all bindings sent by the MN either to its HA or to remote CNs; it also contains BUs which are waiting for the completion of the return-routability procedure before they can be sent. However, for multiple BUs sent to the same destination address, the BU list contains only the most recent BU (i.e., with the greatest sequence number value) sent to that destination.

Other aspects of the MN operations are covered next; however, only some key highlights are covered here; for additional details, consult RFC 3775 (2).

8.2.7.1 Packet Processing For packets sent by an MN while it is at home, no special MIPv6 processing is required.

While an MN is away from home, it can continue to use its home address or it can use one or more CoAs as the source of the packet (thus eliminating the use of a home address option in the packet.) Using the MN's CoA as the source generally has a lower overhead than using the MN's home address, given that no extra options need be used. Such packets can be routed normally, that is, directly between their source and destination without relying on MIPv6 mechanisms. Summarizing this, if the MN uses an address other than one of its home addresses as the source of a packet sent while away from home, no special MIPv6 processing is required: packets are simply addressed and transmitted in the same way as any normal IPv6 packet.

For packets sent by the MN while away from home using the MN's home address as the source, MIPv6 processing of the packet is required. As we noted, this can be done in one of two ways:

- *Route optimization*: This approach to the delivery of packets does not require going through the home network, and such, typically enables faster and more reliable transmission. The MN needs to ensure that a binding cache entry exists for its home address so that the CN can process the packet. An MN should arrange to supply the home address in a home address option and must set the IPv6 header's source address field to the CoA which the MN has registered to be used with this CN. The CN will then use the address supplied in the home address option to serve the function traditionally done by the source IP address

in the IPv6 header. The MN's home address is then supplied to higher protocol layers and applications.

- *Reverse tunneling*. This is the mechanism that tunnels the packets via the HA, being needed if there is no binding yet with the CN; as such, it is not as efficient as the route optimization mechanism. This mechanism is used for packets that have the MN's home address as the source address in the IPv6 header, or with multicast control protocol. The process is as follows: (i) the packet is sent to the HA using IPv6 encapsulation; (ii) the source address in the tunnel packet is the primary CoA as registered with the HA; (iii) the destination address in the tunnel packet is the HA's address. Then, the HA will pass the encapsulated packet to the CN.

During packet processing, there will be an interaction between outbound MIPv6 processing and outbound IPsec processing for packets sent by an MN while away from home. This interaction is shown in Figure 8.14; in Figure 8.14, it is assumed that IPsec is being used in transport mode and that the MN is using its home address as the source for the packet. Note that the treatment of destination options (in RFC 2402) is extended as follows: the authentication header (AH) authentication data must be calculated as if the following were true: (i) the IPv6 source address in the IPv6 header contains the MN's home address; (ii) the home address field of the home address destination option contains the new CoA.

While away from home, an MN will receive packets addressed to its home address, by one of two methods:

- Packets sent by a CN, which does not have a binding cache entry for the MN, will be sent to the home address, captured by the HA, and tunneled to the MN. Here the MN must check that the IPv6 source address of the tunneled packet is the IP address of its HA. In this method, the MN may also send a BU to the original sender of the packet and subject to rate-limiting processes. The MN must also process the received packet in the manner defined for IPv6 encapsulation, which will result in the encapsulated (inner) packet being processed normally by upper-layer protocols within the MN as if it had been addressed (only) to the MN's home address.
- Packets sent by a CN that has a binding cache entry for the MN that contains the MN's current CoA will be sent by the CN using a type 2 routing header. The packet will be addressed to the MN's CoA, with the final hop in the routing header directing the packet to the MN's home address; the processing of this last hop of the routing header is entirely internal to the MN, since the CoA and home address are both addresses within the MN.

8.2.7.2 Home Agent Address Discovery Sometimes when the MN needs to send a BU to its HA to register its new primary CoA, the MN may not know the address of any router on its home link that can serve as an HA for it. In this case, the MN may attempt to discover the address of a suitable HA on its home link. To do so,

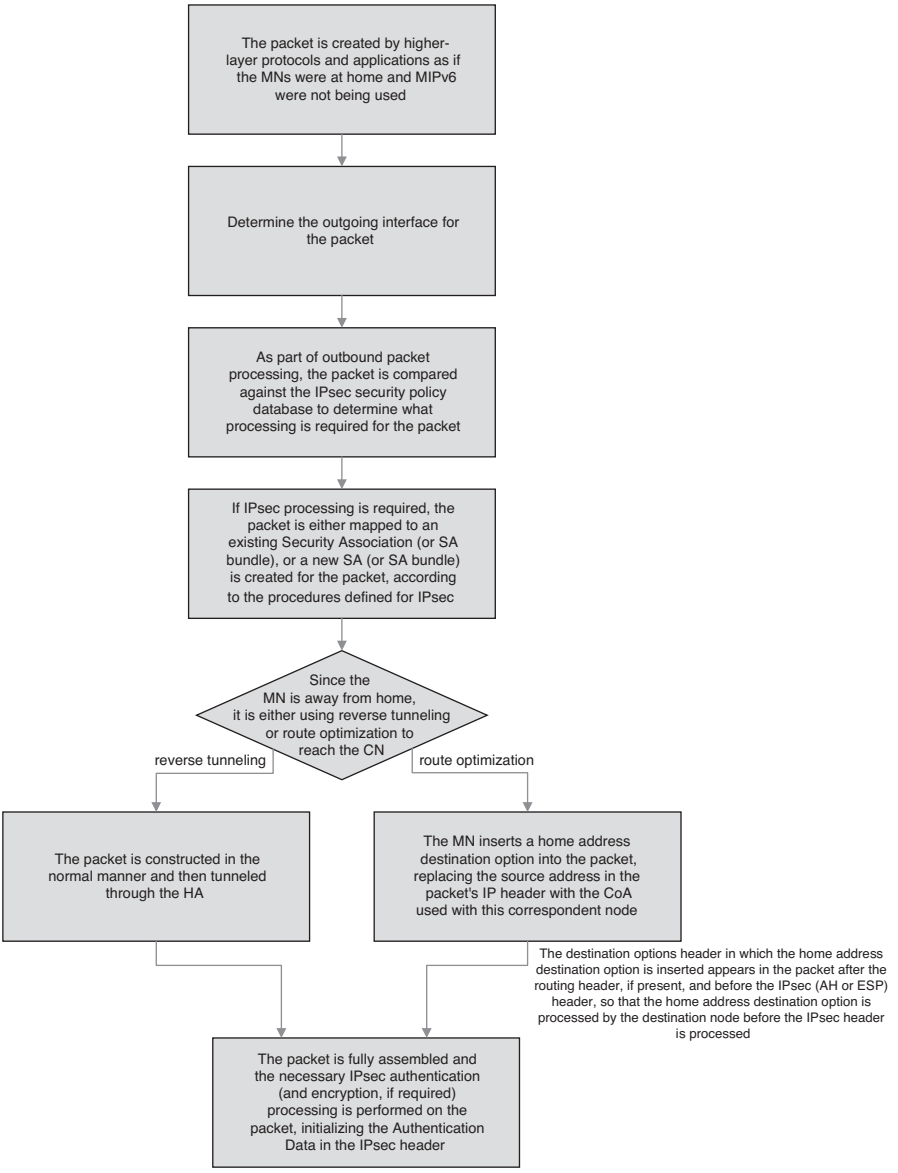


FIGURE 8.14 Interaction with outbound IPsec processing.

the MN sends an ICMP HAAD request message to the MIPv6 HA anycast address for its home subnet prefix. The HA on its home link that receives this request message will return an ICMP HAAD reply message. This message gives the addresses for the HAs operating on the home link. The MN, upon receiving this HAAD reply message, may then send its home registration BU to any of the unicast IP addresses listed in the HA addresses field in the reply.

8.2.7.3 Movement Support The goal of movement detection is to detect Layer 3 handovers. While full-function roaming mechanisms might be useful in this context, as a minimum, one needs some generic method of detecting handoffs. Methods that make use of the facilities of IPv6 neighbor discovery, including router discovery and neighbor unreachability detection, may be of interest. Table 8.8 depicts some mechanisms for movement support. Due to the temporary packet flow disruption and signaling overhead involved in updating mobility bindings, the MN should avoid performing an L3 handover until it is strictly necessary.

TABLE 8.8 Basic Mechanisms for Movement Support

Activity	Description
Movement detection	Generic movement detection can use neighbor unreachability detection to detect when the default router is no longer bidirectionally reachable, in which case the MN must discover a new default router. However, this detection only occurs when the MN has packets to send, and in the absence of frequent router advertisements or indications from the link layer, the MN might become unaware of an L3 handover that occurred. Hence, the MN should supplement this method with other information whenever it is available to the MN (e.g., from lower protocol layers)
	When the MN detects an L3 handover, it selects a new default router as a consequence of router discovery and then performs prefix discovery with that new router to form new CoA(es). It then registers its new primary CoA with its HA. After updating its home registration, the MN then updates associated mobility bindings in CNs that it is performing route optimization
Forming new CoA	After detecting that it has moved an MN is expected to generate a new primary CoA using normal IPv6 mechanisms. This should also be done when the current primary CoA becomes deprecated
	After selecting a new primary CoA, the MN must send a BU containing that CoA to its HA. The BU must have the home registration (H) and acknowledge (A) bits set its HA. In order to form a new CoA, an MN may use either stateless or stateful (e.g., DHCPv6) address autoconfiguration
Using multiple CoAs	An MN may use more than one CoA at a time. To assist with smooth handovers, an MN should retain its previous primary CoA as a (non-primary) CoA and should still accept packets at this address, even after registering its new primary CoA with its HA
	Whenever an MN determines that it is no longer reachable through a given link, it should invalidate all CoAs associated with address prefixes that it discovered from routers on the unreachable link which are not in the current set of address prefixes advertised by the (possibly new) current default router

8.2.8 Relationship to IPV4 Mobile IPv4 (MIP)

A question might be "what is the relationship of MIPv6 to IPV4 MIPv4 defined in RFC 3344 (9)?" RFC 3775 (2) notes that the design of MIPv6 benefits both from the experiences gained from the development of MIP and also from the opportunities provided by IPv6. Therefore, MIPv6 shares many features with MIP, but is integrated into IPv6 and offers other improvements. The notable differences between MIP and MIPv6 are as follows:

- There is no need to deploy special routers as "foreign agents," as in MIP. MIPv6 operates in any location without any special support required from the local router.
- Support for route optimization is a fundamental part of the protocol, rather than a nonstandard set of extensions.
- MIPv6 route optimization can operate securely even without prearranged SAs. It is expected that route optimization can be deployed on a global scale between all MNs and CNs.
- Support is also integrated into MIPv6 for allowing route optimization to coexist efficiently with routers that perform "ingress filtering."
- The IPv6 neighbor unreachability detection assures symmetric reachability between the MN and its default router in the current location.
- Most packets sent to an MN while away from home in MIPv6 are sent using an IPv6 routing header rather than IP encapsulation, reducing the amount of resulting overhead compared to MIP.
- MIPv6 is decoupled from any particular link layer, as it uses IPv6 neighbor discovery instead of Address Resolution Protocol (ARP); this also improves the robustness of the protocol.
- The use of IPv6 encapsulation (and the routing header) removes the need in MIPv6 to manage "tunnel soft state."
- The dynamic HAAD mechanism in MIPv6 returns a single reply to the MN. The directed broadcast approach used in IPv4 returns separate replies from each HA.

MIPv6 offers a number of improvements over MIPv4 principally due to capabilities inherited from IPv6. For example, route optimization and dynamic HA discovery can only be achieved with MIPv6. One of the advantages of the large address space provided by IPv6 is that it allows MNs to obtain a globally unique CoA wherever they are; therefore, there is no need for network address translator (NAT) traversal techniques designed for MIPv4. This allows MIPv6 to be a significantly simpler and more bandwidth-efficient mobility management protocol. At the same time, during the transition toward IPv6, NAT traversal for existing private IPv4 networks needs to be considered (10).

REFERENCES

1. Minoli D. *Mobile Video with Mobile IPv6*. New York: Wiley; 2012.
2. Johnson D, Perkins C, Arkko J. Mobility Support in IPv6. RFC 3775, June 2004.
3. Arkko J, Vogt C, Haddad W. Enhanced Route Optimization for Mobile IPv6. RFC 4866, May 2007.
4. Korhonen J, editor. Bournelle J, Giaretta G, NakhjiriM. Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction. February 2010, RFC 5778.
5. 6deploy.org. IPv6 Workshop – IPv6 Mobility Module. October 2008.
6. Giaretta G, Devarapalli V. Mobile IPv6 Bootstrapping in Split Scenario, RFC 5026, October 2007.
7. Arkko J, Devarapalli V, Dupont F. Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents. RFC 3776, June 2004.
8. Narten T, Nordmark E, Simpson W. Neighbor Discovery for IP Version 6 (IPv6). RFC 2461, December 1998.
9. Perkins C. editor. IP Mobility Support for IPv4. RFC 3344, August 2002.
10. Soliman H, editor. Mobile IPv6 Support for Dual Stack Hosts and Routers. RFC 5555, June 2009.