IETF Mobile IP Working Group
INTERNET-DRAFT

David B. Johnson
Rice University
Charles E. Perkins
Nokia Research Center
Jari Arkko
Ericsson
29 Oct 2002

Mobility Support in IPv6

<draft-ietf-mobileip-ipv6-19.txt>

Status of This Memo

This document specifies the operation of the IPv6 Internet with mobile computers. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about the mobile node's current location. IPv6 packets addressed to a mobile node's home address are transparently routed to its care-of address. The protocol enables IPv6 nodes to cache the binding of a mobile node's home address with its care-of address, and to then send any packets destined for the mobile node directly to it at this care-of address. To support this operation, Mobile IPv6 defines a new IPv6 protocol and a new destination option. All IPv6 nodes, whether mobile or stationary can communicate with mobile nodes.

Contents

1. Introduction

This document specifies how the IPv6 Internet operates with mobile computers. Without specific support for mobility in IPv6 [11], packets destined to a mobile node would not be able to reach it while the mobile node is away from its home link. In order to continue communication in spite of its movement, a mobile node could change its IP address each time it moves to a new link, but the mobile node would then not be able to maintain transport and higher-layer connections when it changes location. Mobility support in IPv6 is particularly important, as mobile computers are likely to account for a majority or at least a substantial fraction of the population of the Internet during the lifetime of IPv6.

The protocol defined in this document, known as Mobile IPv6, allows a mobile node to move from one link to another without changing the mobile node's "home address". Packets may be routed to the mobile node using this address regardless of the mobile node's current point of attachment to the Internet. The mobile node may also continue to communicate with other nodes (stationary or mobile) after moving to a new link. The movement of a mobile node away from its home link is thus transparent to transport and higher-layer protocols and applications.

The Mobile IPv6 protocol is just as suitable for mobility across homogeneous media as for mobility across heterogeneous media. For example, Mobile IPv6 facilitates node movement from one Ethernet segment to another as well as it facilitates node movement from an Ethernet segment to a wireless LAN cell, with the mobile node's IP address remaining unchanged in spite of such movement.

One can think of the Mobile IPv6 protocol as solving the network-layer mobility management problem. Some mobility management applications -- for example, handover among wireless transceivers, each of which covers only a very small geographic area -- have been solved using link-layer techniques. For example, in many current wireless LAN products, link-layer mobility mechanisms allow a "handover" of a mobile node from one cell to another, re-establishing link-layer connectivity to the node in each new location.

Mobile IPv6 does not attempt to solve all general problems related to the use of mobile computers or wireless networks. In particular, this protocol does not attempt to solve:

- Handling links with partial reachability, or unidirectional connectivity, such as are often found in wireless networks (but see Section 11.5.1).

- Access control on a link being visited by a mobile node.

- Local or hierarchical forms of mobility management (similar to many current link-layer mobility management solutions).

- Assistance for adaptive applications

- Mobile routers

- Service Discovery

- Distinguishing between packets lost due to bit errors vs. network congestion

2. Comparison with Mobile IP for IPv4

The design of Mobile IP support in IPv6 (Mobile IPv6) benefits both from the experiences gained from the development of Mobile IP support in IPv4 (Mobile IPv4) [20, 21, 22], and from the opportunities provided by IPv6. Mobile IPv6 thus shares many features with Mobile IPv4, but is integrated into IPv6 and offers many other improvements. This section summarizes the major differences between Mobile IPv4 and Mobile IPv6:

- There is no need to deploy special routers as "foreign agents", as in Mobile IPv4. Mobile IPv6 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.

- Mobile IPv6 route optimization can operate securely even without pre-arranged security associations. It is expected that route optimization can be deployed on a global scale between all mobile nodes and correspondent nodes.

- Support is also integrated into Mobile IPv6 for allowing route optimization to coexist efficiently with routers that perform "ingress filtering" [23].

- In Mobile IPv6, the mobile node does not have to tunnel multicast packets to its home agent.

- The movement detection mechanism in Mobile IPv6 provides bidirectional confirmation of a mobile node's ability to communicate with its default router in its current location.

- Most packets sent to a mobile node while away from home in Mobile IPv6 are sent using an IPv6 routing header rather than IP encapsulation, reducing the amount of resulting overhead compared to Mobile IPv4.

- Mobile IPv6 is decoupled from any particular link layer, as it uses IPv6 Neighbor Discovery [12] instead of ARP. This also improves the robustness of the protocol.

- The use of IPv6 encapsulation (and the routing header) removes the need in Mobile IPv6 to manage "tunnel soft state".

- The dynamic home agent address discovery mechanism in Mobile IPv6 returns a single reply to the mobile node. The directed broadcast approach used in IPv4 returns separate replies from each home agent.

3. Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [2].

3.1. General Terms

IP
: Internet Protocol Version 6 (IPv6).

node
: A device that implements IP.

router
: A node that forwards IP packets not explicitly addressed to itself.

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. Accordingly, a unicast routable address must have either a global or site-local scope (but not link-local).

host
: Any node that is not a router.

link
: A communication facility or medium over which nodes can communicate at the link layer, such as an Ethernet (simple or bridged). A link is the layer immediately below IP.

interface
: A node's attachment to a link.

subnet prefix
: A bit string that consists of some number of initial bits of an IP 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.

link-layer address
A link-layer identifier for an interface, such as IEEE 802 addresses on Ethernet links.

packet
An IP header plus payload.

security association
A security object shared between two nodes which includes the data mutually agreed on for operation of some cryptographic algorithm (typically including a key).

security policy database
A database of rules that describe what security associations should be applied for different kinds of packets.

destination option
Destination options are carried by the IPv6 Destination Options extension header. Destination options include optional information that need be examined only by the IPv6 node given as the destination address in the IPv6 header, not by other intermediate routing nodes. Mobile IPv6 defines one new destination option, the Home Address destination option (see Section 6.3).

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. In this document, use of the term "routing header" typically refers to use of a type 2 routing header, as specified in Section 6.4.

'|' (concatenation)
Some formulas in this specification use the symbol '|' indicate bytewise concatenation, as in A | B. This concatenation requires that all of the bytes of the datum A appear first in the result, followed by all of the bytes of the datum B.

First (size, input)
Some formulas in this specification use a functional

form "First (size, input)" to indicate truncation of the "input" data so that only the first "size" bits remain to be used.

3.2. Mobile IPv6 Terms

home address
A unicast routable address assigned to a mobile node, used as the permanent address of the mobile node. This address is within the mobile node's home link. Standard IP routing mechanisms will deliver packets destined for a mobile node's home address to its home link.

home subnet prefix
The IP subnet prefix corresponding to a mobile node's home address.

home link
The link on which a mobile node's home subnet prefix is defined.

mobile node
A node that can change its point of attachment from one link to another, while still being reachable via its home address.

movement
A change in a mobile node's point of attachment to the Internet such that it is no longer connected to the same link as it was previously. If a mobile node is not currently attached to its home link, the mobile node is said to be "away from home".

correspondent node
A peer node with which a mobile node is communicating. The correspondent node may be either mobile or stationary.

foreign subnet prefix
Any IP subnet prefix other than the mobile node's home subnet prefix.

foreign link
Any link other than the mobile node's home link.

care-of address
A unicast routable address associated with a mobile node while visiting a foreign link; the subnet prefix of this IP address is a foreign subnet prefix. Among the multiple care-of addresses that a mobile node may

have at any given time (e.g., with different subnet prefixes), the one registered with the mobile node's home agent is called its "primary" care-of address.

home agent
A router on a mobile node's home link with which the mobile node has registered its current care-of address. While the mobile node is away from home, the home agent intercepts packets on the home link destined to the mobile node's home address, encapsulates them, and tunnels them to the mobile node's registered care-of address.

binding
The association of the home address of a mobile node with a care-of address for that mobile node, along with the remaining lifetime of that association.

registration
The process during which a mobile node sends a Binding Update to its home agent or a correspondent node, causing a binding for the mobile node to be registered.

mobility message
A message containing a Mobility Header (see Section 6.1).

binding procedure
A binding procedure is initiated by the mobile node to inform either a correspondent node or the mobile node's home agent of the current binding of the mobile node.

binding authorization
Binding procedure needs to be authorized to allow the recipient to believe that the sender has the right to specify a new binding.

return routability procedure
The return routability procedure authorizes binding procedures by the use of a cryptographic token exchange.

correspondent binding procedure
A return routability procedure followed by a binding procedure, run between the mobile node and a correspondent node.

home binding procedure
A binding procedure between the mobile node and its home agent, authorized by the use of IPsec.

nonce
Nonces are random numbers used internally by the

correspondent node in the creation of keygen tokens
related to the return routability procedure. The nonces

are not specific to a mobile node, and are kept secret within the correspondent node.

nonce index
A nonce index is used to indicate which nonces have been used when creating keygen token values, without revealing the nonces themselves.

cookie
A cookie is a random number used by a mobile nodes to prevent spoofing by a bogus correspondent node in the return routability procedure.

care-of init cookie
A cookie sent to the correspondent node in the Care-of Test Init message, to be returned in the Care-of Test message.

home init cookie
A cookie sent to the correspondent node in the Home Test Init message, to be returned in the Home Test message.

keygen token
A keygen token is a number supplied by a correspondent node in the return routability procedure to enable the mobile node to compute the necessary binding management key for authorizing a Binding Update.

care-of keygen token
A keygen token sent by the correspondent node in the Care-of Test message.

home keygen token
A keygen token sent by the correspondent node in the Home Test message.

binding management key (Kbm)
A binding management key (Kbm) is a key used for authorizing a binding cache management message (e.g., Binding Update or Binding Acknowledgement). Return routability provides a way to create a binding management key.

4. Overview of Mobile IPv6

4.1. Basic Operation

A mobile node is always expected to be 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 mobile node within its home subnet prefix on its home link. While a mobile node is at home, packets addressed to its home address are routed to the mobile node's home link, using conventional Internet routing mechanisms.

While a mobile node is attached to some foreign link away from home, it is also addressable at one or more care-of addresses. A care-of address is an IP address associated with a mobile node that has the subnet prefix of a particular foreign link. The mobile node can acquire its care-of address through conventional IPv6 stateless or stateful auto-configuration mechanisms. As long as the mobile node stays in this location, packets addressed to this care-of address will be routed to the mobile node. The mobile node may also accept packets from several care-of addresses, such as when it is moving but still reachable at the previous link.

The association between a mobile node's home address and care-of address is known as a "binding" for the mobile node. While away from home, a mobile node registers its primary care-of address with a router on its home link, requesting this router to function as the "home agent" for the mobile node. The mobile node performs this binding registration by sending a "Binding Update" message to the home agent. The home agent replies to the mobile node by returning a "Binding Acknowledgement" message. The operation of the mobile node and the home agent is specified in Sections 11 and 10, respectively.

Any node communicating with a mobile node is referred to in this document as a "correspondent node" of the mobile node, and may itself be either a stationary node or a mobile node. Mobile nodes can provide information about their current location to correspondent nodes. This happens through the correspondent binding procedure. As a part of this procedure, a return routability test is performed in order to authorize the establishment of the binding. The operation of the correspondent node is specified in Section 9.

There are two possible modes for communications between the mobile node and a correspondent node. The first mode, bidirectional tunneling, does not require Mobile IPv6 support from the correspondent node and is available even if the mobile node has not registered its current binding with the correspondent node. Packets from the correspondent node are routed to the home agent and then tunneled to the mobile node. Packets to the correspondent node are tunneled from the mobile node to the home agent ("reverse tunneled") and then routed normally from the home network to the correspondent node. In this mode, the home agent uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the mobile node's home address (or home addresses) on the home link. Each intercepted packet is tunneled to the mobile node's primary care-of address. This tunneling is performed using IPv6 encapsulation [15].

The second mode, "route optimization", requires the mobile node to register its current binding at the correspondent node. Packets from the correspondent node can be routed directly to the care-of address of the mobile node. When sending a packet to any IPv6 destination, the correspondent node checks its cached bindings for an entry for 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 [11] (see Section 6.4) to route the packet to the mobile node by way of the care-of address indicated in this binding.

Routing packets directly to the mobile node's care-of address allows the shortest communications path to be used. It also eliminates congestion at the mobile node's home agent and home link. In addition, the impact of any possible failure of the home agent or networks on the path to or from it is reduced.

When routing packets directly to the mobile node, the correspondent node sets the Destination Address in the IPv6 header to the care-of address of the mobile node. A new type of IPv6 routing header (see Section 6.4) is also added to the packet to carry the desired home address. Similarly, the mobile node sets the Source Address in the packet's IPv6 header to its current care-of addresses. The mobile node adds a new IPv6 "Home Address" destination option (see Section 6.3) to carry its home address. The inclusion of home addresses in these packets makes the use of the care-of address transparent above the network layer (e.g., at the transport layer).

Mobile IPv6 also provides support for multiple home agents, and the reconfiguration of the home network. In these cases, the mobile node may not know the IP address of its own home agent, and even the home subnet prefixes may change over time. A mechanism, known as "dynamic home agent address discovery" allows a mobile node to dynamically discover the IP address of a home agent on its home link, even when the mobile node is away from home. Mobile nodes can also learn new information about home subnet prefixes through the "prefix discovery" mechanism. These mechanisms are described in Sections 6.5 through 6.8.

4.2. New IPv6 Protocol

Mobile IPv6 defines a new IPv6 protocol, using the Mobility Header (see Section 6.1). This Header is used to carry the following messages:

Home Test Init
Home Test
Care-of Test Init
Care-of Test
These four messages are used to initiate the return

routability procedure from the mobile node to a correspondent node. This ensures authorization of subsequent Binding Updates, as described in Section 5.2.5.

The format of the messages are defined in Sections 6.1.3 through 6.1.6.

Binding Update
A Binding Update is used by a mobile node to notify a correspondent node or the mobile node's home agent of its current binding. The Binding Update sent to the mobile node's home agent to register its primary care-of address is marked as a "home registration". The Binding Update message is described in detail in Section 6.1.7.

Binding Acknowledgement
A Binding Acknowledgement is used to acknowledge receipt of a Binding Update, if an acknowledgement was requested in the Binding Update. The Binding Acknowledgement is described in detail in Section 6.1.8.

Binding Refresh Request
A Binding Refresh Request is used to request a mobile node to re-establish its binding with the correspondent node. This message is typically used when the cached binding is in active use but the binding's lifetime is close to expiration. The correspondent node may use, for instance, recent traffic and open transport layer connections as an indication of active use. The Binding Refresh Request is described in detail in Section 6.1.2.

Binding Error
The Binding Error 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. This message is described in detail in Section 6.1.9.

4.3. New IPv6 Destination Option

Mobile IPv6 defines a new IPv6 destination option, the Home Address destination option. This option is described in detail in Section 6.3.

4.4. New IPv6 ICMP Messages

Mobile IPv6 also introduces four new ICMP message types, two for use in the dynamic home agent address discovery mechanism, and two for renumbering and mobile configuration mechanisms. As described in Sections 10.5 and 11.4.1, the following two new ICMP message types are used for home agent address discovery:

- Home Agent Address Discovery Request, described in Section 6.5.

- Home Agent Address Discovery Reply, described in Section 6.6.

The next two message types are used for network renumbering and address configuration on the mobile node, as described in Section 10.6:

- Mobile Prefix Solicitation, described in Section 6.7.

- Mobile Prefix Advertisement, described in Section 6.8.

4.5. Conceptual Data Structure Terminology

This document describes the Mobile IPv6 protocol in terms of the following conceptual data structures:

Binding Cache

A cache of bindings for other nodes. This cache is maintained by home agents and correspondent nodes. The cache contains both "correspondent registration" entries (see Section 9.1) and "home registration" entries (see Section 10.1).

Binding Update List

This list is maintained by each mobile node. The list has an item for every binding that the mobile node 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 sent in the Binding Update expires. See Section 11.1.

Home Agents List

Home agents need to know which other home agents are on the same link. This information is stored in the Home Agents List, as described in more detail in Section 10.1. The list is used for informing mobile nodes during dynamic home agent address discovery.

4.6. Site-Local Addressability

Mobile nodes are free to move from site to site, but the use of site-local addresses must be carefully managed. When a mobile node or home agent address is site-local, then packets that use those address need to stay within the site. The mobile node SHOULD use such addresses only when it somehow has a guarantee - for instance, by configuration - that it is safe to do so. Thus, a mobile node MAY use a site-local home address for roaming within a site, but not for roaming to another site. This is true even though the mobile node may be able to obtain a globally addressable care-of address at the new site.

If a mobile node or home agent has a global IPv6 address available, it SHOULD be selected for use with Mobile IP signaling, in order to make the greatest chance for success in case the mobile node might move to a different site.

Operations affecting multi-sited IPv6 nodes are not completely understood, especially when mobility management is involved. For this reason, home agents SHOULD NOT be multi-sited. Similarly, a mobile node that uses site-local home, care-of, or home agent addresses SHOULD NOT be multi-sited.

5. Overview of Mobile IPv6 Security

This specification provides a number of security features. These include the protection of Binding Updates both to home agents and correspondent nodes, and the protection of tunnels, home address information, and routing instructions in data packets.

Binding Updates 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.

5.1. Binding Updates to Home Agents

The mobile node and the home agent must have a security association to protect this signaling. Authentication Header (AH) or Encapsulating Security Payload (ESP) MUST be used. For ESP, a non-null authentication algorithm MUST be applied.

In order to protect messages exchanged between the mobile node and the home agent with IPsec, appropriate security policy database entries must be created. A mobile node must be prevented from using its security association to send a Binding Update on behalf of another mobile node using the same home agent. This MUST be achieved by checking that the given home address has been used with the right security association. Such a check can be provided in IPsec processing, by having the security policy database entries unequivocally identify a single security association for any given home address and home agent. The check may also be provided as a part of Mobile IPv6 processing, if information about the used security association is available in there. In any case, it is necessary that the home address of the mobile node is visible in the Binding Updates and Acknowledgements. The home address is used in these packets as a source or destination, or in the Home Address Destination option or the type 2 routing header.

As with all IPsec security associations in this specification, manual configuration of security associations MUST be supported. Automatic key management with IKE [9] MAY be supported. When dynamic keying is used, either the security policy database entries or the MIPv6 processing MUST unequivocally identify the IKE phase 1 credentials which can be used to create security associations for a particular home address.

Reference [24] is an informative description and example of using IPsec to protect the communications between the mobile node and the home agent.

5.2. Binding Updates to Correspondent Nodes

Binding Updates to correspondent nodes can be protected by using a binding management key, Kbm. Kbm may be established using data exchanged during the return routability procedure. The data exchange is accomplished by use of node keys, nonces, cookies, tokens, and certain cryptographic functions. Section 5.2.5 outlines the basic return routability procedure. Section 5.2.6 shows how the results of this procedure are used to authorize a Binding Update to a correspondent node. Finally, Sections 5.2.7 and 5.2.8 discuss some additional issues.

5.2.1. Node Keys

Each correspondent node has a secret key, Kcn, called the "node key", which it uses to produce the keygen tokens sent to the mobile nodes. The node key MUST be a random number, 20 octets in length. The node key allows the correspondent node to verify that the keygen tokens used by the mobile node in authorizing a Binding Update are indeed its own. This key MUST NOT be shared with any other entity.

A correspondent node MAY generate a fresh node key at any time; this avoid the need for secure persistent key storage. Procedures for optionally updating the node key are discussed later in Section 5.2.7.

5.2.2. Nonces

Each correspondent node also generates nonces at regular intervals. The nonces should be generated by using a random number generator that is known to have good randomness properties [1].

A correspondent node may use the same Kcn and nonce with all the mobiles it is in communication with.

Each nonce is identified by a nonce index. When a new nonce is generated, it must be associated with a new nonce index; this may be done, for example, by incrementing the value of the previous nonce index, if the nonce index is used as an array pointer into a linear array of nonces. However, there is no requirement that nonces be stored that way, or that the values of subsequent nonce indices have any particular relationship to each other. The index value is communicated in the protocol, so that if a nonce is replaced by new nonce during the run of a protocol, the correspondent node can distinguish messages that should be checked against the old nonce from messages that should be checked against the new nonce. Strictly speaking, indices are not necessary in the authentication, but allow the correspondent node to efficiently find the nonce value that it used in creating a keygen token.

Correspondent nodes keep both the current nonce and a small set of valid previous nonces whose lifetime has not yet expired. Expired values MUST be discarded, and messages using stale or unknown indices will be rejected.

The specific nonce index values cannot be used by mobile nodes to determine the validity of the nonce. Expected validity times for the nonces values and the procedures for updating them are discussed later in Section 5.2.7.

A nonce is an octet string of any length. The recommended length is 64 bits.

5.2.3. Cookies and Tokens

The return routability address test procedure uses cookies and keygen tokens as opaque values within the test init and test messages, respectively.

- The "home init cookie" and "care-of init cookie" are 64 bit values sent to the correspondent node from the mobile node, and later returned to the mobile node. The home init cookie is sent in the Home Test Init message, and returned in the Home Test message. The care-of init cookie is sent in the Care-of Test Init message, and returned in the Care-of Test message.

- The "home keygen token" and "care-of keygen token" are 64-bit values sent by the correspondent node to the mobile node via the home agent (via the Home Test message) and the care-of address (by the Care-of Test message), respectively.

The mobile node should use a newly generated random number for each request that carries a home init or care-of init cookie. The cookies are used to verify that the Home Test or Care-of Test message matches the Home Test Init or Care-of Test Init message, respectively. These cookies also serve to ensure that parties who have not seen the request cannot spoof responses.

Home and care-of keygen tokens are produced by the correspondent node based on its currently active secret key (Kcn) and nonces, as well as the home or care-of address (respectively). A keygen token is valid as long as both the secret key (Kcn) and the nonce used to create it are valid.

5.2.4. Cryptographic Functions

In this specification, the function used to compute hash values is SHA1 [19]. Message Authentication Codes (MACs) are computed using HMAC_SHA1 [25, 19]. HMAC_SHA1(K,m) denotes such a MAC computed on message m with key K.

5.2.5. Return Routability Procedure

The Return Routability Procedure enables the correspondent node to obtain some reasonable assurance that the mobile node is in fact addressable at its claimed care-of address as well as at its home address. Only with this assurance is the correspondent node able to accept Binding Updates from the mobile node which would then instruct the correspondent node to direct that mobile node's data traffic to its claimed care-of address.

This is done by testing whether packets addressed to the two claimed addresses are routed to the mobile node. The mobile node can pass the test only if it is able to supply proof that it received certain data (the "keygen tokens") which the correspondent node sends to those addresses. These data are combined by the mobile node into a binding management key, denoted Kbm.

Figure 1 shows the message flow for the return routability procedures.

The Home and Care-of Test Init messages are sent at the same time. The procedure requires very little processing at the correspondent node, and the Home and Care-of Test messages can be returned quickly, perhaps nearly simultaneously. These four messages form the return routability procedure.

Home Test Init

A mobile node sends a Home Test Init message to the correspondent node to acquire the home keygen token. The contents of the message can be summarized as follows:

Source Address = home address

```
     Mobile node                 Home agent          Correspondent node
          |                                                  |
          |  Home Test Init (HoTI)   |                       |
          |------------------------->|------------------------->|
          |                          |                       |
          |  Care-of Test Init (CoTI)                        |
          |------------------------------------------------->|
          |                                                  |
          |                          |  Home Test (HoT)      |
          |<-------------------------|<-------------------------|
          |                          |                       |
          |                             Care-of Test (CoT)   |
          |<-------------------------------------------------|
          |                                                  |
```

Figure 1: Message Flow for Return Routability Address Testing

```
        Destination Address = correspondent
        Parameters:
          - home init cookie
```

The Home Test Init message conveys the mobile node's home address to the correspondent node. The mobile node also sends along a home init cookie that the correspondent node must return later. The Home Test Init message is reverse tunneled through the home agent. The mobile node remembers these cookie values to obtain some assurance that its protocol messages are being processed by the desired correspondent node.

Care-of Test Init

The mobile node sends a Care-of Test Init message to the correspondent node to acquire the care-of keygen token. The contents of this message can be summarized as follows:

```
        Source Address = care-of address
        Destination Address = correspondent
        Parameters:
          - care-of init cookie
```

The Care-of Test Init message conveys the mobile node's care-of address to the correspondent node. The mobile node also sends along a care-of init cookie that the correspondent node must return later. The Care-of Test Init message is sent directly to the correspondent node.

Home Test

The Home Test message is sent in response to a Home Test Init message. The contents of the message are:

```
Source Address = correspondent
Destination Address = home address
Parameters:
  - home init cookie
  - home keygen token
  - home nonce index
```

When the correspondent node receives the Home Test Init message, it generates a home keygen token as follows:

```
home keygen token :=
     First (64, HMAC_SHA1 (Kcn, (home address | nonce | 0)))
```

where | denotes concatenation. The final "0" inside the HMAC_SHA1 function is a single zero octet, used to distinguish home and care-of cookies from each other.

The home keygen token is formed from the first 64 bits of the MAC. The home keygen token tests that the mobile can receive messages sent to its home address. Kcn is used in the production of home keygen token in order to allow the correspondent node to verify that it generated the home and care-of nonces, without forcing the correspondent node to remember a list of all tokens it has handed out.

The Home Test message is sent to the mobile node via the home network, where it is presumed that the home agent will tunnel the message to the mobile node. This means that the mobile node needs to already have sent a Binding Update to the home agent, so that the home agent will have received and authorized the new care-of address for the mobile node before the return routability procedure. For improved security, it is important that the data passed between the home agent and the mobile node be immune from inspection and passive attack. Such protection can be gained by encrypting the home keygen token as it is tunneled from the home agent to the mobile node.

The home init cookie from the mobile node is returned in the Home Test message, to ensure that the message comes from a node on the route between the home agent and the correspondent node.

The home nonce index is delivered to the mobile node to later allow the correspondent node to efficiently find the nonce value that it used in creating the home keygen token.

Care-of Test

This message is sent in response to a Care-of Test Init message. The contents of the message are:

```
Source Address = correspondent
Destination Address = care-of address
Parameters:
  - care-of init cookie
  - care-of keygen token
  - care-of nonce index
```

The correspondent node sends a challenge also to the mobile's care-of address. When the correspondent node receives the Care-of Test Init message, it generates a care-of keygen token as follows:

```
care-of keygen token :=
   First (64, HMAC_SHA1 (Kcn, (care-of address | nonce | 1)))
```

Here, the final "1" inside the HMAC_SHA1 function is a single octet containing the hex value 0x01, and is used to distinguish home and care-of cookies from each other. The keygen token is formed from the first 64 bits of the MAC, and sent directly to the mobile node at its care-of address. The care-of init cookie from the from Care-of Test Init message is returned to ensure that the message comes from a node on the route to the correspondent node.

The care-of nonce index is provided to identify the nonce used for the care-of keygen token. The home and care-of nonce indices MAY be the same, or different, in the Home and Care-of Test messages.

When the mobile node has received both the Home and Care-of Test messages, the return routability procedure is complete. As a result of the procedure, the mobile node has the data it needs to send a Binding Update to the correspondent node. The mobile node hashes the tokens together to form a 20 octet binding key Kbm:

```
Kbm = SHA1 (home keygen token | care-of keygen token)
```

A Binding Update may also be used to delete a previously established binding by setting the care-of address equal to the home address (Section 6.1.7). In this case, the care-of keygen token is not used. Instead, the binding management key is generated as follows:

```
Kbm = SHA1(home keygen token)
```

Note that the correspondent node does not create any state specific to the mobile node, until it receives the Binding Update from that mobile node. The correspondent node does not maintain the value for the binding management key Kbm; it creates Kbm when given the nonce indices and the mobile node's addresses.

5.2.6. Authorizing Binding Management Messages

After the mobile node has created the binding management key (Kbm), it can supply a verifiable Binding Update to the correspondent node. This section provides an overview of this binding procedure. Figure 2 shows the message flow. The Binding Update creates a binding, and the Binding Acknowledgement is optional.

```
  Mobile node                               Correspondent node
       |                                                |
       |             Binding Update (BU)                |
       |----------------------------------------------->|
       |  (MAC, seq#, nonce indices, care-of address)   |
       |                                                |
       |                                                |
       |    Binding Acknowledgement (BA) (if sent)      |
       |<-----------------------------------------------|
       |              (MAC, seq#, status)               |
```

Figure 2: Message Flow for Establishing Binding at the Correspondent Node

Binding Update

To authorize a Binding Update, the mobile node creates a binding management key Kbm from the keygen tokens as described in the previous section. The contents of the Binding Update include the following:

```
    Source Address = care-of address
    Destination Address = correspondent
    Parameters:
      - home address (within the Home Address destination
        option or in the Source Address)
      - sequence number (within the Binding Update message
        header)
      - home nonce index (within the Nonce Indices option)
      - care-of nonce index (within the Nonce Indices option)
      - HMAC_SHA1 (Kbm, (care-of address | CN address | BU))
```

The Binding Update may contain a Nonce Indices option, indicating to the correspondent node which home and care-of nonces to use to recompute Kbm, the binding management key.

The MAC is computed as described in Section 6.2.6, using the correspondent node's address as the destination address and the Binding Update message itself as the Mobility Header Data.

Once the correspondent node has verified the MAC, it can create a Binding Cache entry for the mobile.

Binding Acknowledgement

The Binding Update is optionally acknowledged by the correspondent node. The contents of the message are as follows:

```
Source Address = correspondent
Destination Address = care-of address
Parameters:
  - sequence number (within the Binding Update message
    header)
  - HMAC_SHA1 (Kbm, (care-of address | CN address | BA))
```

The Binding Acknowledgement contains the same sequence number as the Binding Update. The MAC is computed as described in Section 6.2.6, using the correspondent node's address as the destination address and the message itself as the Mobility Header Data.

Bindings established with correspondent nodes using keys created by way of the return routability procedure MUST NOT exceed MAX_RR_BINDING_LIFE seconds (see Section 12).

The value in the Source Address field in the IPv6 header carrying the Binding Update is normally also the care-of address which is used in the binding. However, a different care-of address MAY be specified by including an Alternate Care-of Address mobility option in the Binding Update (see Section 6.2.4). When such a message is sent to the correspondent node and the return routability procedure is used as the authorization method, the Care-of Test Init and Care-of Test messages MUST have been performed for the address in the Alternate Care-of Address option (not the Source Address). The nonce indices and MAC value MUST be based on information gained in this test.

The care-of address may be set equal to the home address in order to delete a previously established binding In this case, generation of the binding management key depends exclusively on the home keygen token (Section 5.2.5).

5.2.7. Updating Node Keys and Nonces

Correspondent nodes generate nonces at regular intervals. It is recommended to keep each nonce (identified by a nonce index) acceptable for at least MAX_TOKEN_LIFE seconds (see Section 12) after it has been first used in constructing a return routability message response. However, the correspondent node MUST NOT accept nonces beyond MAX_NONCE_LIFE seconds (see Section 12) after the first use. As the difference between these two constants is 30 seconds, a convenient way to enforce the above lifetimes is to generate a new nonce every 30 seconds. The node can then continue to accept tokens that have been based on the last 8 (MAX_NONCE_LIFE / 30) nonces. This results in tokens being acceptable MAX_TOKEN_LIFE to MAX_NONCE_LIFE seconds after they have been sent to the mobile node, depending on whether the token was sent at the beginning or end of the first 30 second period. Note that the correspondent node may also attempt to generate new nonces on demand, or only if the old nonces have been used. This is possible, as long as the correspondent node keeps track of how long time ago the nonces were used for the first time, and does not generate new nonces on every return routability request.

Due to resource limitations, rapid deletion of bindings, or reboots the correspondent node may not in all cases recognize the nonces that the tokens were based on. If a nonce index is unrecognized, the correspondent node replies with an an error code in the Binding Acknowledgement (either 136, 137, or 138 as discussed in Section 6.1.8). The mobile node can then retry the return routability procedure.

An update of Kcn SHOULD be done at the same time as an update of a nonce, so that nonce indices can identify both the nonce and the key. Old Kcn values have to be therefore remembered as long as old nonce values.

Given that the tokens are normally expected to be usable for MAX_TOKEN_LIFE seconds, the mobile node MAY use them beyond a single run of the return routability procedure until MAX_TOKEN_LIFE expires. After this the mobile node SHOULD NOT use the tokens. A fast moving mobile node may reuse a recent home keygen token from a correspondent node when moving to a new location, and just acquire a new care-of keygen token to show routability in the new location.

While this does not save the number of round-trips due to the simultaneous processing of home and care-of return routability tests, there are fewer messages being exchanged, and a potentially long round-trip through the home agent is avoided. Consequently, this optimization is often useful. A mobile node that has multiple home addresses, may also use the same care-of keygen token for Binding Updates concerning all of these addresses.

5.2.8. Preventing Replay Attacks

The return routability procedure also protects the participants against replayed Binding Updates through the use of the sequence number and a MAC. Care must be taken when removing bindings at the correspondent node, however. Correspondent nodes must retain bindings and the associated sequence number information at least as long as the nonces used in the authorization of the binding are still valid. The correspondent node can, for instance, change the nonce often enough to ensure that the nonces used when removed entries were created are no longer valid. If many such deletions occur the correspondent node can batch them together to avoid having to increment the nonce index too often.

5.3. Dynamic Home Agent Address Discovery

No security is required for dynamic home agent address discovery.

5.4. Prefix Discovery

The mobile node and the home agent must have a security association to protect prefix discovery. IPsec AH or ESP SHOULD be supported and used for integrity protection. For ESP, a non-null authentication algorithm MUST be applied.

5.5. Payload Packets

Payload packets exchanged with mobile nodes can be protected in the usual manner, in the same way as stationary hosts can protect them. However, Mobile IPv6 introduces the Home Address destination option, a routing header, and tunneling headers in the payload packets. In the following we define the security measures taken to protect these, and to prevent their use in attacks against other parties.

This specification limits the use of the Home Address destination option to the situation where the correspondent node already has a Binding Cache entry for the given home address. This avoids the use of the Home Address option in attacks described in Section 14.1.

Mobile IPv6 uses a Mobile IPv6 specific type of a routing header. This type provides the necessary functionality but does not open vulnerabilities discussed in Section 14.1.

Tunnels between the mobile node and the home agent are protected by ensuring proper use of source addresses, and optional cryptographic protection. The mobile node verifies that the outer IP address corresponds to its home agent. The home agent verifies that the outer IP address corresponds to the current location of the mobile node (Binding Updates sent to the home agents are secure). These measures protect the tunnels against vulnerabilities discussed in Section 14.1.

For traffic tunneled via the home agent, additional IPsec AH or ESP encapsulation MAY be supported and used.

6. New IPv6 Protocol, Message Types, and Destination Option

6.1. Mobility Header

The Mobility Header is an extension header used by mobile nodes, correspondent nodes, and home agents 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.

6.1.1. Format

The Mobility Header is identified by a Next Header value of TBD <To be assigned by IANA> in the immediately preceding header, and has the following format:

```
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | Payload Proto |  Header Len   |   MH Type     |   Reserved    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |           Checksum            |                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
 |                                                               |
 .                                                               .
 .                        Message Data                           .
 .                                                               .
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Payload Proto

8-bit selector. Identifies the type of header immediately following the Mobility Header. Uses the same values as the IPv6 Next Header field [11].

This field is intended to be used by a future specification of piggybacking binding messages on payload packets (see Section B.1).

Implementations conforming to this specification SHOULD set the payload protocol type to IPPROTO_NONE (59 decimal).

Header Len

8-bit unsigned integer, representing the length of the Mobility Header in units of 8 octets, excluding the first 8 octets.

The length of the Mobility Header MUST be a multiple of 8 octets.

MH Type

8-bit selector. Identifies the particular mobility message in question. Current values are specified in Sections 6.1.2 to 6.1.9. An unrecognized MH Type field causes an error indication to be sent.

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. The checksum is calculated from the octet string consisting of a "pseudo-header" followed by the entire Mobility Header starting with the Payload Proto field. The checksum is the 16-bit one's complement of the one's complement sum of this string.

The pseudo-header contains IPv6 header fields, as specified in Section 8.1 of [11]. The Next Header value used in the pseudo-header is TBD <To be assigned by IANA>. The addresses used in the pseudo-header are the addresses that appear in the Source and Destination Address fields in the IPv6 packet carrying the Mobility Header.

Note that the procedures described in Section 11.3.1 apply even for the Mobility Header. If a mobility message has a Home Address destination option, then the checksum calculation uses the home address in this option as the value of the IPv6 Source Address field. The type 2 routing header is treated as explained in [26].

The Mobility Header is considered as the upper layer protocol for the purposes of calculating the pseudo-header. The Upper-Layer Packet Length field in the pseudo-header MUST be set to the total length of the Mobility Header.

For computing the checksum, the checksum field is set to zero.

Message Data

A variable length field containing the data specific to the indicated Mobility Header type.

Mobile IPv6 also defines a number of "mobility options" for use within these messages; if included, any options MUST appear after the fixed portion of the message data specified in this document. The presence of such options will be indicated by the Header Len field within the message. When the Header Len value is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options. These options include padding options that can be used to ensure that other options are aligned properly, and that the total length of the message is divisible by 8. The encoding and format of defined options are described in Section 6.2.

Alignment requirements for the Mobility Header are the same as for any IPv6 protocol Header. That is, they MUST be aligned on an 8-octet boundary.

6.1.2. Binding Refresh Request Message

The Binding Refresh Request (BRR) message is used to request a mobile node's binding from the mobile node. It is sent according to the rules in Section 9.5.5. When a mobile node receives a packet containing a Binding Refresh Request message it processes the message according to the rules in Section 11.7.4.

The Binding Refresh Request message uses the MH Type value 0. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:

```
                                +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                |          Reserved             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                                                               .
.                        Mobility options                       .
.                                                               .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Reserved

16-bit field reserved for future use. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. Contains one or more TLV-encoded mobility options. The encoding and format of defined options are described in Section 6.2. The receiver MUST ignore and skip any options which it does not understand.

There MAY be additional information, associated with this Binding Refresh Request message, that need not be present in all Binding Refresh Request messages sent. Mobility options allow future extensions to the format of the Binding Refresh Request message to be defined. This specification does not define any options valid for the Binding Refresh Request message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 0.

6.1.3. Home Test Init Message

A mobile node uses the Home Test Init (HoTI) message to initiate the return routability procedure and request a home keygen token from a correspondent node (see Section 11.6.1). The Home Test Init message uses the MH Type value 1. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:

```
                                +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                |           Reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                       Home Init Cookie                        +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                                                               .
.                       Mobility Options                        .
.                                                               .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Reserved

16-bit field reserved for future use. This value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Home Init Cookie

64-bit field which contains a random value, the home init cookie.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. Contains one or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for the Home Test Init message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 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 home agent and the mobile node. This protection is indicated by the IPsec policy data base. The protection of Home Test Init messages is unrelated to the requirement to protect regular payload traffic, which MAY use such tunnels as well.

6.1.4. Care-of Test Init Message

A mobile node uses the Care-of Test Init (CoTI) message to initiate the return routability procedure and request a care-of keygen token from a correspondent node (see Section 11.6.1). The Care-of Test Init message uses the MH Type value 2. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:

```
                                +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                |           Reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                      Care-of Init Cookie                      +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                                                               .
.                        Mobility Options                       .
.                                                               .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Reserved

16-bit field reserved for future use. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Care-of Init Cookie

64-bit field which contains a random value, the care-of init cookie.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. Contains one or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for the Care-of Test Init message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 1.

6.1.5. Home Test Message

The Home Test (HoT) message is a response to the Home Test Init message, and is sent from the correspondent node to the mobile node (see Section 5.2.5). The Home Test message uses the MH Type value 3. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:

```
                                +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                |       Home Nonce Index        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                        Home Init Cookie                       +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                       Home Keygen Nonce                       +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                                                               .
.                        Mobility options                       .
.                                                               .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Home Nonce Index

This field will be echoed back by the mobile node to the correspondent node in a subsequent Binding Update.

Home Init Cookie

64-bit field which contains the home init cookie.

Home Keygen Nonce

This field contains the 64 bit home keygen token used in the return routability procedure.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. Contains one or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for the Home Test message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 2.

6.1.6. Care-of Test Message

The Care-of Test (CoT) message is a response to the Care-of Test Init message, and is sent from the correspondent node to the mobile node (see Section 11.6.2). The Care-of Test message uses the MH Type value 4. When this value is indicated in the MH Type field,

the format of the Message Data field in the Mobility Header is as follows:

```
                                +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                |      Care-of Nonce Index      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                      Care-of Init Cookie                      +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                     Care-of Keygen Nonce                      +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                                                               .
.                        Mobility Options                       .
.                                                               .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Care-of Nonce Index

This value will be echoed back by the mobile node to the correspondent node in a subsequent Binding Update.

Care-of Init Cookie

64-bit field which contains the care-of init cookie.

Care-of Keygen Nonce

This field contains the 64 bit care-of keygen token used in the return routability procedure.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. Contains one or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for the Care-of Test message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 2.

6.1.7. Binding Update Message

The Binding Update (BU) message is used by a mobile node to notify other nodes of a new care-of address for itself. Binding Updates are sent as described in Section 11.7.1 and 11.7.2.

The Binding Update uses the MH Type value 5. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:

```
                                +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                |          Sequence #           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|A|H|S|D|L|      Reserved       |            Lifetime           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                                                               .
.                        Mobility options                       .
.                                                               .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Acknowledge (A)

The Acknowledge (A) bit is set by the sending mobile node to request a Binding Acknowledgement (Section 6.1.8) be returned upon receipt of the Binding Update.

Home Registration (H)

The Home Registration (H) bit is set by the sending mobile node to request that the receiving node should act as this node's home agent. 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 mobile node in the binding.

Single Address Only (S)

If this bit is set, the mobile node requests that the home agent make no changes to any other Binding Cache entry except for the particular one containing the home address specified in the Home Address destination option. This disables home agent processing for other related addresses, as is described in Section 10.3.1.

Duplicate Address Detection (D)

The Duplicate Address Detection (D) bit is set by the sending mobile node to request that the receiving node (the mobile node's home agent) perform Duplicate Address Detection [13] on the mobile node's home link for the home address in this binding. This bit is only valid when the Home Registration (H) and Acknowledge (A) bits are also set, and MUST NOT be set otherwise.

Link-Local Address Compatibility (L)

The Link-Local Address Compatibility (L) bit is set when the home address reported by the mobile node has the same interface identifier (IID) as the mobile node's link-local address.

Reserved

These fields are unused. They MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Sequence #

A 16-bit number used by the receiving node to sequence Binding Updates and by the sending node to match a returned Binding Acknowledgement with this Binding Update.

Lifetime

16-bit unsigned integer. The number of time units remaining before the binding MUST be considered expired. A value of all one bits (0xffff) indicates infinity. A value of zero indicates that the Binding Cache entry for the mobile node MUST be deleted. One time unit is 4 seconds.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. Contains one or more TLV-encoded mobility options. The encoding and format of defined options are described in Section 6.2. The receiver MUST ignore and skip any options which it does not understand.

The following options are valid in a Binding Update:

- Binding Authorization Data option

- Nonce Indices option.

- Alternate Care-of Address option

If no options are present in this message, 4 bytes of padding is necessary and the Header Len field will be set to 1.

The care-of address MUST be a unicast routable address. Binding

Updates for a care-of address which is not a unicast routable address MUST be silently discarded.

The deletion of a binding can be indicated by setting the Lifetime field to 0 or by setting the care-of address equal to the home address. In either case, generation of the binding management key depends exclusively on the home keygen token (Section 5.2.5). Correspondent nodes SHOULD NOT expire the Binding Cache entry before the lifetime expires, if any application hosted by the correspondent node is still likely to require communication with the mobile node. A Binding Cache entry that is deallocated prematurely might cause subsequent packets to be dropped from the mobile node, if they contain the Home Address destination option. This situation is recoverable, since an Binding Error message is sent to the mobile node (see Section 6.1.9); however, it causes unnecessary delay in the communications.

6.1.8. Binding Acknowledgement Message

The Binding Acknowledgement is used to acknowledge receipt of a Binding Update (Section 6.1.7). This packet is sent as described in Sections 9.5.4 and 10.3.1.

The Binding Acknowledgement has the MH Type value 6. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:

```
                                 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                 |    Status     |   Reserved    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |           Sequence #          |            Lifetime           |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 .                                                               .
 .                        Mobility options                       .
 .                                                               .
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 Binding Update. Values of the Status field less than 128 indicate that the Binding Update was accepted by the receiving node. Values greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following Status values are currently defined:

0	Binding Update accepted
128	Reason unspecified
129	Administratively prohibited
130	Insufficient resources
131	Home registration not supported
132	Not home subnet
133	Not home agent for this mobile node
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

Up-to-date values of the Status field are to be specified in the IANA registry of assigned numbers [18].

Sequence #

The Sequence Number in the Binding Acknowledgement is copied from the Sequence Number field in the Binding Update. It is used by the mobile node in matching this Binding Acknowledgement with an outstanding Binding Update.

Lifetime

The granted lifetime, in time units of 4 seconds, for which this node SHOULD retain the entry for this mobile node in its Binding Cache. A value of all one bits (0xffff) indicates infinity.

The value of this field is undefined if the Status field indicates that the Binding Update was rejected.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. Contains one or more TLV-encoded mobility options. The encoding and format of defined options are described in Section 6.2. The receiver MUST ignore and skip any options which it does not understand.

There MAY be additional information, associated with this Binding Acknowledgement, that need not be present in all Binding Acknowledgements sent. Mobility options allow future extensions to the format of the Binding Acknowledgement to be defined. The following options are valid for the Binding Acknowledgement:

- Binding Authorization Data option

- Binding Refresh Advice option

If no options are present in this message, 4 bytes of padding is necessary and the Header Len field will be set to 1.

6.1.9. Binding Error Message

The Binding Error (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; see Section 9.3.3 for details.

The Binding Error message uses the MH Type value 7. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:

```
                                 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                 |     Status    |   Reserved    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                          Home Address                         +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.                                                               .
.                        Mobility Options                       .
.                                                               .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Status

8-bit unsigned integer indicating the reason for this message. The following values are currently defined:

1 Unknown binding for Home Address destination option

2 Unrecognized MH Type value

Reserved

A 8-bit field reserved for future use. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Home Address

The home address that was contained in the Home Address destination option. The mobile node uses this information to determine which binding does not exist, in cases where the mobile node has several home addresses.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. Contains one or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand.

There MAY be additional information, associated with this Binding Error message, that need not be present in all Binding Error messages sent. Mobility options allow future extensions to the format of the format of the Binding Error message to be defined. The encoding and format of defined options are described in Section 6.2. This specification does not define any options valid for the Binding Error message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 2.

6.2. Mobility Options

Mobility messages can include one 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 specified in the message subsections of Section 6.1.

The presence of such options will be indicated by the Header Len of the Mobility Header. If included, the Binding Authorization Data option (Section 6.2.6) MUST be the last option and MUST NOT have trailing padding. Otherwise, options can be placed in any order.

6.2.1. Format

Mobility options are encoded within the remaining space of the Message Data field of a mobility message, using a type-length-value (TLV) format as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Option Type  | Option Length |   Option Data...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Option Type

8-bit identifier of the type of mobility option. When processing a Mobility Header containing an option for which the Option Type value is not recognized by the receiver, the receiver MUST quietly ignore and skip over the option, correctly handling any remaining options in the message.

Option Length

8-bit unsigned integer, representing the length in octets of the mobility option, not including the Option Type and Option Length fields.

Option Data

A variable length field that contains data specific to the option.

The following subsections specify the Option types which are currently defined for use in the Mobility Header.

Implementations MUST silently ignore any mobility options that they do not understand.

6.2.2. Pad1

The Pad1 option does not have any alignment requirements. Its format is as follows:

```
 0
 0 1 2 3 4 5 6 7
+-+-+-+-+-+-+-+-+
|   Type = 0    |
+-+-+-+-+-+-+-+-+
```

NOTE! the format of the Pad1 option is a special case - it has neither Option Length nor Option Data fields.

The Pad1 option is used to insert one octet of padding in the Mobility Options area of a Mobility Header. If more than one octet of padding is required, the PadN option, described next, should be used rather than multiple Pad1 options.

6.2.3. PadN

The PadN option does not have any alignment requirements. Its format is as follows:

```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -
|   Type = 1    | Option Length | Option Data
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -
```

The PadN option is used to insert two or more octets of padding in the Mobility Options area of a mobility message. For N octets of padding, the Option Length field contains the value N-2, and the Option Data consists of N-2 zero-valued octets. Option data MUST be ignored by the receiver.

6.2.4. Alternate Care-of Address

The Alternate Care-of Address option has an alignment requirement of 8n+6. Its format is as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                |   Type = 3    |  Length = 16  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                   Alternate Care-of Address                   +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The Alternate Care-of Address option is valid only in Binding Update. The Alternate Care-of Address field contains an address to use as the care-of address for the binding, rather than using the Source Address of the packet as the care-of address.

6.2.5. Nonce Indices

The Nonce Indices option has an alignment requirement of 2n. Its format is as follows:

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                   |   Type = 4    |   Length = 4  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Home Nonce Index      |     Care-of Nonce Index       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The Nonce Indices option is valid only in the Binding Update message, and only when present together with an Binding Authorization Data option.

The Home Nonce Index field tells the correspondent node that receives the message which of its stored random nonce values is to be used to produce the home keygen token to authorize the Binding Update.

The Care-of Nonce Index field tells the correspondent node that receives the message which of its stored random nonce values is to be used to produce the care-of keygen token to authorize the Binding Update.

6.2.6. Binding Authorization Data

The Binding Authorization Data option has an alignment requirement of 8n+2. Its format is as follows:

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                   |   Type = 5    | Option Length |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   +                                                               +
   |                         Authenticator                         |
   +                                                               +
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The Binding Authorization Data option is valid in the Binding Update and Binding Acknowledgment.

The Option Length field contains the length of the authenticator in octets.

The Authenticator field contains a cryptographic value which can be used to determine that the message in question comes from the right authority. Rules for calculating this value depend on the used authorization procedure.

For the return routability procedure, this option can appear in the Binding Update and Binding Acknowledgements. Rules for calculating the Authenticator value are the following:

```
Mobility Data = care-of address | final dest | Mobility Header Data
Authenticator = First (96, HMAC_SHA1 (Kbm, Mobility Data))
```

Where | denotes concatenation and "final dest" is the IPv6 address of the final destination of the packet. "Mobility Header Data" is the content of the Mobility Header, excluding the Authenticator field itself. The Authenticator value is calculated as if the Checksum field in the Mobility Header was zero. The Checksum in the transmitted packet is still calculated in the usual manner, with the calculated Authenticator being a part of the packet protected by the Checksum. Kbm is the binding management key, which is typically created using nonces provided by the correspondent node (see Section 9.4).

The first 96 bits from the MAC result are used as the Authenticator field. Note that, if the message is sent to a destination which is itself mobile, the "final dest" address may not be the address found in the Destination Address field of the IPv6 header; instead the address of the true destination (e.g., its home address) should be used.

6.2.7. Binding Refresh Advice

The Binding Refresh Advice option has an alignment requirement of 2n. Its format is as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                |   Type = 6    |   Length = 2  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Refresh Interval        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The Binding Refresh Advice option is only valid in the Binding Acknowledgement, and only on Binding Acknowledgements sent from the mobile node's home agent in reply to a home registration. The Refresh Interval is measured in units of four seconds, and indicates how long before the mobile node SHOULD send a new home registration to the home agent. The Refresh Interval MUST be set to indicate a smaller time interval than the Lifetime value of the Binding Acknowledgement.

6.3. 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 a mobile node while away from home, to inform the recipient of the mobile node's home address.

The Home Address option is encoded in type-length-value (TLV) format as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Header | Header Ext Len  |  Option Type  | Option Length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                          Home Address                         +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Option Type

201 = 0xC9

Option Length

8-bit unsigned integer. Length of the option, in octets, excluding the Option Type and Option Length fields. This field MUST be set to 16.

Home Address

The home address of the mobile node sending the packet. This address MUST be a unicast routable address.

IPv6 requires that options appearing in a Hop-by-Hop Options header or Destination Options header be aligned in a packet so that multi-octet values within the Option Data field of each option fall on natural boundaries (i.e., fields of width n octets are placed at an integer multiple of n octets from the start of the header, for n = 1, 2, 4, or 8) [11]. The alignment requirement [11] for the Home

Address option is 8n+6.

The three highest-order bits of the Option Type field are encoded to indicate specific processing of the option [11]; for the Home Address option, these three bits are set to 110. This indicates the following processing requirements:

- Any IPv6 node that does not recognize the Option Type must discard the packet.

- If the packet's Destination Address was not a multicast address, return an ICMP Parameter Problem, Code 2, message to the packet's Source Address; otherwise, for multicast addresses, the ICMP message MUST NOT be sent.

- The data within the option cannot change en-route to the packet's final destination.

The Home Address option MUST be placed as follows:

- After the routing header, if that header is present

- Before the Fragment Header, if that header is present

- Before the AH Header or ESP Header, if either one of those headers is present

For each IPv6 packet header, the Home Address Option MUST NOT appear more than once. However, an encapsulated packet [15] MAY contain a separate Home Address option associated with each encapsulating IP header.

The inclusion of a Home Address destination option in a packet affects the receiving node's processing of only this single packet. No state is created or modified in the receiving node as a result of receiving a Home Address option in a packet. In particular, the presence of a Home Address option in a received packet MUST NOT alter the contents of the receiver's Binding Cache and MUST NOT cause any changes in the routing of subsequent packets sent by this receiving node.

6.4. Type 2 Routing Header

Mobile IPv6 defines a new routing header variant, the type 2 routing header, to allow the packet to be routed directly from a correspondent to the mobile node's care-of address. The mobile node's care-of address is inserted into the IPv6 Destination Address field. Once the packet arrives at the care-of address, the mobile node retrieves its home address from the routing header, and this is used as the final destination address for the packet.

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 Mobile IPv6. This routing header type (type 2) is restricted to carry only one IPv6 address. All IPv6 nodes which 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, since it is the mobile node's home address, MUST be a unicast routable address. Furthermore, if the scope of the home address is smaller than the scope of the care-of address, the mobile node MUST discard the packet (see Section 4.6).

6.4.1. Format

The type 2 routing header has the following format:

```
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |  Next Header  | Hdr Ext Len=2 | Routing Type=2|Segments Left=1|
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                            Reserved                           |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 +                                                               +
 |                                                               |
 +                         Home Address                          +
 |                                                               |
 +                                                               +
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 [11].

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. Initialized to zero for transmission, and ignored on reception.

Home Address

The Home Address of the destination Mobile Node.

For a type 2 routing header, the Hdr Ext Len MUST be 2. The Segments Left value describes the number of route segments remaining; i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination. Segments Left MUST be 1. The ordering rules for extension headers in an IPv6 packet are described in Section 4.1 of [11]. The type 2 routing header defined for Mobile IPv6 follows the same ordering as other routing headers. If both a Type 0 and a type 2 routing header are present, the type 2 routing header should follow the other routing header.

In addition, the general procedures defined by IPv6 for routing headers suggest that a received routing header MAY be automatically "reversed" to construct a routing header for use in any response packets sent by upper-layer protocols, if the received packet is authenticated [6]. This MUST NOT be done automatically for type 2 routing headers.

6.5. ICMP Home Agent Address Discovery Request Message

The ICMP Home Agent Address Discovery Request message is used by a mobile node to initiate the dynamic home agent address discovery mechanism, as described in Section 11.4.1. The mobile node sends

the Home Agent Address Discovery Request message to the Mobile IPv6 Home-Agents anycast address for its own home subnet prefix [16].

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |            Checksum           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Identifier           |            Reserved           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

150 <To Be Assigned by IANA>

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching Home Agent Address Discovery Reply messages to this Home Agent Address Discovery Request message.

Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

The Source Address of the Home Agent Address Discovery Request message packet MUST be one of the mobile node's current care-of addresses. The home agent MUST then return the Home Agent Address Discovery Reply message directly to the Source Address chosen by the mobile node. Note that, at the time of performing this dynamic home agent address discovery procedure, it is likely that the mobile node is not registered with any home agent within the specified anycast group.

6.6. ICMP Home Agent Address Discovery Reply Message

The ICMP Home Agent Address Discovery Reply message is used by a home agent to respond to a mobile node that uses the dynamic home agent address discovery mechanism, as described in Section 10.5.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |            Checksum           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Identifier          |             Reserved          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
.                                                               .
.                      Home Agent Addresses                     .
.                                                               .
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

151 <To Be Assigned by IANA>

Code

0

Checksum

The ICMP checksum [14].

Identifier

The identifier from the invoking Home Agent Address Discovery Request message.

Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Home Agent Addresses

A list of addresses of home agents on the home link for the mobile node. The number of addresses present in the list is indicated by the remaining length of the IPv6 packet carrying the Home Agent Address Discovery Reply message.

6.7. ICMP Mobile Prefix Solicitation Message Format

The ICMP Mobile Prefix Solicitation Message is sent by a mobile node to its home agent while it is away from home. The purpose of the message is to solicit a Mobile Prefix Advertisement from the home agent, which will allow the mobile node 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 home agent.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |            Checksum           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Identifier          |             Reserved          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

IP Fields:

Source Address

The mobile node's care-of address.

Destination Address

The address of the mobile node's home agent. This home agent must be on the link which the mobile node wishes to learn prefix information about.

Hop Limit

Set to an initial hop limit value, similarly to any other unicast packet sent by the mobile node.

Destination Option:

A Home Address destination option MUST be included.

AH or ESP header:

IPsec headers SHOULD be supported and used as described in Section 5.4.

ICMP Fields:

Type

152 <To Be Assigned by IANA>

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching a future Mobile Prefix Advertisement to this Mobile Prefix Solicitation.

Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

6.8. ICMP Mobile Prefix Advertisement Message Format

A home agent will send a Mobile Prefix Advertisement to a mobile node to distribute prefix information about the home link while the mobile node is traveling away from the home network. This will occur in response to a Mobile Prefix Solicitation with an Advertisement, or by an unsolicited Advertisement sent according to the rules in Section 10.6.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Identifier           |   Options ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

IP Fields:

Source Address
: The home agent's address as the mobile node would expect to see it (i.e., same network prefix)

Destination Address
: If this message is a response to a Mobile Prefix Solicitation, this field contains the Source Address field from that packet. For unsolicited messages, the mobile node's care-of address SHOULD be used. Note that unsolicited messages can only be sent if the mobile node is currently registered with the home agent.

Routing header:

A type 2 routing header MUST be included.

AH or ESP header:

IPsec headers SHOULD be supported and used as described in Section 5.4.

ICMP Fields:

Type

153 <To Be Assigned by IANA>

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching this Mobile Prefix Advertisement to a previous Mobile Prefix Solicitation.

Options:

Prefix Information

Each message contains one or more Prefix Information options. Each option carries the prefix(es) that the mobile node should use to configure its home address(es). Section 10.6 describes which prefixes should be advertised to the mobile node.

The Prefix Information option is defined in Section 4.6.2 of [12], with modifications defined in Section 7.2 of this specification. The home agent MUST use this modified Prefix Information option to send the aggregate list of home network prefixes as defined in Section 10.6.1.

The Mobile Prefix Advertisement sent by the home agent MAY include the Source Link-layer Address option defined in RFC 2461 [12], or the Advertisement Interval option specified in Section 7.3.

Future versions of this protocol may define new option types. Mobile nodes MUST silently ignore any options they do not recognize and continue processing the message.

If the Advertisement is sent in response to a Mobile Prefix Solicitation, the home agent MUST copy the Identifier value from that message into the Identifier field of the Advertisement.

The home agent MUST NOT send more than one Mobile Prefix Advertisement message per second to any mobile node.

7. Modifications to IPv6 Neighbor Discovery

7.1. Modified Router Advertisement Message Format

Mobile IPv6 modifies the format of the Router Advertisement message [12] by the addition of a single flag bit to indicate that the router sending the Advertisement message is serving as a home agent on this link. The format of the Router Advertisement message is as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Cur Hop Limit |M|O|H| Reserved|       Router Lifetime         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Reachable Time                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Retrans Timer                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Options ...
+-+-+-+-+-+-+-+-+-+-+-+-+-
```

This format represents the following changes over that originally specified for Neighbor Discovery [12]:

Home Agent (H)

The Home Agent (H) bit is set in a Router Advertisement to indicate that the router sending this Router Advertisement is also functioning as a Mobile IPv6 home agent on this link.

Reserved

Reduced from a 6-bit field to a 5-bit field to account for the addition of the above bit.

7.2. Modified Prefix Information Option Format

Mobile IPv6 requires knowledge of a router's global address in building a Home Agents List as part of the dynamic home agent address discovery mechanism (Sections 10.5 and 11.4.1).

However, Neighbor Discovery [12] only advertises a router's link-local address, by requiring this address to be used as the IP Source Address of each Router Advertisement.

Mobile IPv6 extends Neighbor Discovery 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. The format of the Prefix Information option is as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     | Prefix Length |L|A|R|Reserved1|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Valid Lifetime                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Preferred Lifetime                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Reserved2                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                            Prefix                             +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

This format represents the following changes over that originally specified for Neighbor Discovery [12]:

Router Address (R)

1-bit router address flag. When set, indicates that the Prefix field, in addition to advertising the indicated prefix, contains a complete IP address assigned to the sending router. This router IP address has the same scope and conforms to the same lifetime values as the advertised prefix. This use of the Prefix field is compatible with its use in advertising the prefix itself, since Prefix Advertisement uses only the leading number Prefix bits specified by the Prefix Length field. Interpretation of this flag bit is thus independent of the processing required for the On-Link (L) and Autonomous Address-Configuration (A) flag bits.

Reserved1

Reduced from a 6-bit field to a 5-bit field to account for the addition of the above bit.

In a Router Advertisement, a home agent MUST, and all other routers MAY, include at least one Prefix Information option with the Router Address (R) bit set. Neighbor Discovery specifies that, if including all options in a Router Advertisement causes the size of the Advertisement to exceed the link MTU, multiple Advertisements can be sent, each containing a subset of the options [12]. In this case, at least one (not all) of these multiple Advertisements being sent needs to satisfy the above requirement.

7.3. New Advertisement Interval Option Format

Mobile IPv6 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. The format of the Advertisement Interval option is as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Length    |           Reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Advertisement Interval                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

7

Length

8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 octets. The value of this field MUST be 1.

Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Advertisement Interval

32-bit unsigned integer. The maximum time, in milliseconds, between successive unsolicited router Router Advertisement messages sent by this router on this network interface. Using the conceptual router configuration variables defined by Neighbor Discovery [12], this field MUST be equal to the value MaxRtrAdvInterval, expressed in milliseconds.

Routers MAY include this option in their Router Advertisements. A mobile node receiving a Router Advertisement containing this option SHOULD utilize the specified Advertisement Interval for that router in its movement detection algorithm, as described in Section 11.5.1.

This option MUST be silently ignored for other Neighbor Discovery messages.

7.4. New Home Agent Information Option Format

Mobile IPv6 defines a new Home Agent Information option, used in Router Advertisements sent by a home agent to advertise information specific to this router's functionality as a home agent. The format of the Home Agent Information option is as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |           Reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Home Agent Preference     |      Home Agent Lifetime      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

8

Length

8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 octets. The value of this field MUST be 1.

Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Home Agent Preference

16-bit signed, two's complement integer. The preference for the home agent sending this Router Advertisement, for use in ordering the addresses returned to a mobile node in the Home Agent Addresses field of a Home Agent Address Discovery Reply message. Higher values mean more preferable. If this option is not included in a Router Advertisement in which the Home Agent (H) bit is set, the preference value for this home agent SHOULD be considered to be 0. Values greater than 0 indicate a home agent more preferable than this default value, and values less than 0 indicate a less preferable home agent.

The manual configuration of the Home Agent Preference value is described in Section 8.4. In addition, the sending home agent MAY dynamically set the Home Agent Preference value, for example basing it on the number of mobile nodes it is currently serving or on its remaining resources for serving additional mobile nodes; such dynamic settings are beyond the scope of this document. Any such dynamic setting of the Home Agent Preference, however, MUST set the preference appropriately, relative to the default Home Agent Preference value of 0 that may be in use by some home agents on this link (i.e., a home agent not including a Home Agent Information option in its Router Advertisements will be considered to have a Home Agent Preference value of 0).

Home Agent Lifetime

16-bit unsigned integer. The lifetime associated with the home agent in units of seconds. The default value is the same as the Router Lifetime, as specified in the main body of the Router Advertisement. The maximum value corresponds to 18.2 hours. A value of 0 MUST NOT be used. The Home Agent Lifetime applies only to this router's usefulness as a home agent; it does not apply to information contained in other message fields or options.

Home agents MAY include this option in their Router Advertisements. This option MUST NOT be included in a Router Advertisement in which the Home Agent (H) bit (see Section 7.1) is not set. If this option is not included in a Router Advertisement in which the Home Agent (H) bit is set, the lifetime for this home agent MUST be considered to be the same as the Router Lifetime in the Router Advertisement. If multiple Advertisements are being sent instead of a single larger unsolicited multicast Advertisement, all of the multiple Advertisements with the Router Address (R) bit set MUST include this option with the same contents, otherwise this option MUST be omitted from all Advertisements.

This option MUST be silently ignored for other Neighbor Discovery messages.

If both the Home Agent Preference and Home Agent Lifetime are set to their default values specified above, this option SHOULD NOT be included in the Router Advertisement messages sent by this home agent.

7.5. Changes to Sending Router Advertisements

The Neighbor Discovery protocol specification [12] limits routers to a minimum interval of 3 seconds between sending unsolicited multicast Router Advertisement messages from any given network interface (limited by MinRtrAdvInterval and MaxRtrAdvInterval), stating that:

> "Routers generate Router Advertisements frequently enough that hosts will learn of their presence within a few minutes, but not frequently enough to rely on an absence of advertisements to detect router failure; a separate Neighbor Unreachability Detection algorithm provides failure detection."

This limitation, however, is not suitable to providing timely movement detection for mobile nodes. Mobile nodes detect their own movement by learning the presence of new routers as the mobile node 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. Mobile nodes MUST be able to quickly detect when they move to a link served by a new router, so that they can acquire a new care-of address and send Binding Updates to register this care-of address with their home agent and to notify correspondent nodes as needed.

Mobile IPv6 relaxes this limit such that routers MAY send unsolicited multicast Router Advertisements more frequently. This is important on network interfaces where the router is expecting to provide service to visiting mobile nodes (e.g., wireless network interfaces), or on which it is serving as a home agent to one or more mobile nodes (who may return home and need to hear its Advertisements). Such routers SHOULD be configured with a smaller MinRtrAdvInterval value and MaxRtrAdvInterval value, to allow sending of unsolicited multicast Router Advertisements more often. Recommended values for these limits are:

- MinRtrAdvInterval 0.05 seconds

- MaxRtrAdvInterval 1.5 seconds

Use of these modified limits MUST be configurable, and specific knowledge of the type of network interface in use SHOULD be taken into account in configuring these limits for each network interface. Note that multicast Router Advertisements are not always required in certain wireless networks that have limited bandwidth. Mobility detection or link changes in such networks may be done at lower layers. Router advertisements in such networks SHOULD be sent only when solicited. In such networks it SHOULD be possible to disable unsolicited multicast Router Advertisements on specific interfaces. The MaxRtrAdvInterval in such a case can be set to some high value.

When sending unsolicited multicast Router Advertisements more frequently than the standard limit on unsolicited multicast Advertisement frequency, the sending router need not include all options in each of these Advertisements, but it SHOULD include at least one Prefix Information option with the Router Address (R) bit set (Section 7.2) in each.

7.6. Changes to Sending Router Solicitations

In addition to the limit on routers sending unsolicited multicast Router Advertisement messages (Section 7.5), Neighbor Discovery defines limits on nodes sending Router Solicitation messages, such that a node SHOULD send no more than 3 Router Solicitations, and that these 3 transmissions SHOULD be spaced at least 4 seconds apart. However, these limits prevent a mobile node from finding a new default router (and thus a new care-of address) quickly as it moves about.

Mobile IPv6 relaxes this limit such that, while a mobile node is away from home, it MAY send Router Solicitations more frequently. The following limits for sending Router Solicitations are recommended for mobile nodes while away from home:

- A mobile node that is not configured with any current care-of address (e.g., the mobile node has moved since its previous care-of address was configured), MAY send more than the defined Neighbor Discovery limit of MAX_RTR_SOLICITATIONS Router Solicitations.

- The rate at which a mobile node sends Router Solicitations MUST be limited, although a mobile node MAY send Router Solicitations more frequently than the defined Neighbor Discovery limit of RTR_SOLICITATION_INTERVAL seconds. The minimum interval MUST be configurable, and specific knowledge of the type of network interface in use SHOULD be taken into account in configuring this limit for each network interface. A recommended minimum interval is 1 second.

- After sending at most MAX_RTR_SOLICITATIONS Router Solicitations, a mobile node MUST reduce the rate at which it sends subsequent Router Solicitations. Subsequent Router Solicitations SHOULD be sent using a binary exponential back-off mechanism, doubling the interval between consecutive Router Solicitations, up to a maximum interval. The maximum interval MUST be configurable and SHOULD be chosen appropriately based on the characteristics of the type of network interface in use.

- While still searching for a new default router and care-of address, a mobile node MUST NOT increase the rate at which it sends Router Solicitations unless it has received a positive indication (such as from lower network layers) that it has moved to a new link. After successfully acquiring a new care-of address, the mobile node SHOULD also increase the rate at which it will send Router Solicitations when it next begins searching for a new default router and care-of address.

- A mobile node that is currently configured with a care-of address SHOULD NOT send Router Solicitations to the default router on its current link, until its movement detection algorithm (Section 11.5.1) determines that it has moved and that its current care-of address might no longer be valid.

7.7. Changes to Duplicate Address Detection

Upon failing Duplicate Address Detection, [13] requires IPv6 nodes to stop using the address and wait for reconfiguration. In addition, if the failed address was a link-local address formed from an interface identifier, the interface should be disabled.

Mobile IPv6 extends this behavior as follows. Upon failing Duplicate Address Detection while away from home, the mobile node SHOULD stop using the address on this interface until the mobile node moves to another link. The mobile node SHOULD NOT wait for reconfiguration or disable the interface.

The mobile node MUST NOT discard the home address based on a failure of a link-local address with the same interface identifier. Instead, the mobile node SHOULD generate a new random interface identifier and use it for assigning itself a new link-local address. In order to do this, the mobile node applies to the link-local address the procedure described in [17] for global addresses. At most 5 consecutive attempts SHOULD be performed to generate such addresses and test them through Duplicate Address Detection. If after these attempts no unique address was found, the mobile node SHOULD log a system error and give up attempting to find a link-local address on that interface, until the node moves to a new link.

8. Requirements for Types of IPv6 Nodes

Mobile IPv6 places some special requirements on the functions provided by different types of IPv6 nodes. This section summarizes those requirements, identifying the functionality each requirement is intended to support.

The requirements are set for the following groups of nodes:

- All IPv6 nodes.

- All IPv6 nodes with support for route optimization.

- All IPv6 routers.

- All Mobile IPv6 home agents.

- All Mobile IPv6 mobile nodes.

It is outside the scope of this specification to specify which of these groups are mandatory in IPv6. We only describe what is mandatory for a node that supports, for instance, route optimization. Other specifications are expected to define the extent of IPv6.

8.1. All IPv6 Nodes

Any IPv6 node may at any time be a correspondent node of a mobile node, either sending a packet to a mobile node or receiving a packet from a mobile node. There are no Mobile IPv6 specific requirements for such nodes, and standard IPv6 techniques are sufficient.

8.2. 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 correspondent node to participate in route optimization is essential for the efficient operation of the IPv6 Internet, beneficial for robustness and reduction of jitter and latency, and necessary to avoid congestion in the home network. The following requirements apply to all correspondent nodes that support route optimization:

- The node MUST be able validate a Home Address option using an existing Binding Cache entry, as described in Section 9.3.1.

- The node MUST be able to insert a type 2 routing header into packets to be sent to a mobile node, as described in Section 9.3.2.

- Unless the correspondent node is also acting as a mobile node, it MUST ignore type 2 routing headers and drop all packets that it has received with such headers.

- The node SHOULD be able to interpret ICMP messages as described in Section 9.3.4.

- The node MUST be able to send Binding Error messages as described in Section 9.3.3.

- The node MUST be able to process Mobility Headers as described in Section 9.2.

- The node MUST be able to participate in a return routability procedure (Section 9.4).

- The node MUST be able to process Binding Update messages (Section 9.5).

- The node MUST be able to return a Binding Acknowledgement (Section 9.5.4).

- The node MUST be able to maintain a Binding Cache of the bindings received in accepted Binding Updates, as described in Sections 9.1 and 9.6.

8.3. All IPv6 Routers

All IPv6 routers, even those not serving as a home agent for Mobile IPv6, have an effect on how well mobile nodes can communicate:

- Every IPv6 router SHOULD be able to send an Advertisement Interval option (Section 7.3) in each of its Router Advertisements [12], to aid movement detection by mobile nodes (as in Section 11.5.1). The use of this option in Router Advertisements MUST be configurable.

- Every IPv6 router SHOULD be able to support sending unsolicited multicast Router Advertisements at the faster rate described in Section 7.5. The use of this faster rate MUST 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 (as described in Section 7.2).

- Filtering routers SHOULD support different rules for type 0 and type 2 routing headers (see Section 6.4) so that filtering of source routed packets (type 0) will not necessarily limit Mobile IPv6 traffic which is delivered via type 2 routing headers.

8.4. IPv6 Home Agents

In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

- Every home agent MUST be able to maintain an entry in its Binding Cache for each mobile node for which it is serving as the home agent (Sections 10.1 and 10.3.1).

- Every home agent MUST be able to intercept packets (using proxy Neighbor Discovery [12]) addressed to a mobile node for which it is currently serving as the home agent, on that mobile node's home link, while the mobile node is away from home

(Section 10.4.1).

- Every home agent MUST be able to encapsulate [15] such intercepted packets in order to tunnel them to the primary care-of address for the mobile node indicated in its binding in the home agent's Binding Cache (Section 10.4.2).

- Every home agent MUST support decapsulating [15] reverse tunneled packets sent to it from a mobile node's home address. Every home agent MUST also check that the source address in the tunneled packets corresponds to the currently registered location of the mobile node (Section 10.4.3).

- The node MUST be able to process Mobility Headers as described in Section 10.2.

- Every home agent MUST be able to return a Binding Acknowledgement in response to a Binding Update (Section 10.3.1).

- Every home agent MUST maintain a separate Home Agents List for each link on which it is serving as a home agent, as described in Sections 10.1 and 10.5.1.

- Every home agent MUST be able to accept packets addressed to the Mobile IPv6 Home-Agents anycast address for the subnet on which it is serving as a home agent [16], and MUST be able to participate in dynamic home agent address discovery (Section 10.5).

- Every home agent SHOULD support a configuration mechanism to allow a system administrator to manually set the value to be sent by this home agent in the Home Agent Preference field of the Home Agent Information Option in Router Advertisements that it sends (Section 7.4).

- Every home agent SHOULD support sending ICMP Mobile Prefix Advertisements (Section 6.8), and SHOULD respond to Mobile Prefix Solicitations (Section 6.7). This behavior MUST be configurable, so that home agents can be configured to avoid sending such Prefix Advertisements according to the needs of the network administration in the home domain.

- Every home agent MUST support IPsec ESP for protection of packets belonging to the return routability procedure (Section 10.4.4).

8.5. IPv6 Mobile Nodes

Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

- The node MUST maintain a Binding Update List (Section 11.1).

- The node MUST support sending packets containing a Home Address option (Section 11.3.1), and follow the required IPsec interaction (Section 11.3.2).

- The node MUST be able to perform IPv6 encapsulation and decapsulation [15].

- The node MUST be able to process type 2 routing header as defined in Sections 6.4 and 11.3.3.

- The node MUST support receiving a Binding Error message (Section 11.7.5).

- The node SHOULD support receiving ICMP errors (Section 11.3.4).

- The node MUST support movement detection, care-of address formation, and returning home (Section 11.5).

- The node MUST be able to process Mobility Headers as described in Section 11.2.

- The node MUST support the return routability procedure (Section 11.6).

- The node MUST be able to send Binding Updates, as specified in Sections 11.7.1 and 11.7.2.

- The node MUST be able to receive and process Binding Acknowledgements, as specified in Section 11.7.3.

- The node MUST support receiving a Binding Refresh Request (Section 6.1.2), by responding with a Binding Update.

- The node MUST support receiving Mobile Prefix Advertisements (Section 11.4.3) and reconfiguring its home address based on the prefix information contained therein.

- The node SHOULD support use of the dynamic home agent address discovery mechanism, as described in Section 11.4.1.

9. Correspondent Node Operation

9.1. Conceptual Data Structures

IPv6 nodes with route optimization support maintain a Binding Cache of bindings for other nodes. A separate Binding Cache SHOULD be maintained by each IPv6 node for each of its IPv6 addresses. The Binding Cache MAY be implemented in any manner consistent with the external behavior described in this document, for example by being combined with the node's Destination Cache as maintained by Neighbor Discovery [12]. When sending a packet, the Binding Cache is searched before the Neighbor Discovery conceptual Destination Cache [12]. That is, any Binding Cache entry for this destination SHOULD take precedence over any Destination Cache entry for the same destination.

Each Binding Cache entry conceptually contains the following fields:

- The home address of the mobile node 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. If the destination address of the packet matches the home address in the Binding Cache entry, this entry SHOULD be used in routing that packet.

- The care-of address for the mobile node indicated by the home address field in this Binding Cache entry. If the destination address of a packet being routed by a node matches the home address in this entry, the packet SHOULD be routed to this care-of address. This is described in Section 9.3.2 for packets originated by this node.

- A lifetime value, indicating the remaining lifetime for this Binding Cache entry. The lifetime value is initialized from the Lifetime field in the Binding Update that created or last modified this Binding Cache entry. Once the lifetime of this entry expires, the entry MUST be deleted from the Binding Cache.

- A flag indicating whether or not this Binding Cache entry is a home registration entry.

- The maximum value of the Sequence Number field received in previous Binding Updates for this mobile node home address. The Sequence Number field is 16 bits long. Sequence Number values MUST be compared modulo 2**16 as explained in Section 9.5.1.

- 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 Binding Refresh Request should be sent when the lifetime of this entry nears expiration.

Binding Cache entries not marked as home registrations MAY be replaced at any time by any reasonable local cache replacement policy but SHOULD NOT be unnecessarily deleted. The Binding Cache for any one of a node's IPv6 addresses may contain at most one entry for each mobile node home address. The contents of a node's Binding Cache MUST NOT be changed in response to a Home Address option in a received packet.

9.2. Processing Mobility Headers

Mobility Header processing MUST observe the following rules:

1. The MH Type field MUST have a known value (Section 6.1.1). Otherwise, the node MUST discard the message and SHOULD issue a Binding Error message as described in Section 9.3.3, with Status field set to 2 (unrecognized MH Type value).

2. The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST silently discard the message.

3. The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

Subsequent checks depend on the particular Mobility Header, as specified in Sections 9.4 and 9.5.

9.3. Packet Processing

This section describes how the correspondent node sends packets to the mobile node, and receives packets from it.

9.3.1. Receiving Packets with Home Address Destination Option

If the correspondent node has a Binding Cache entry for the home address of a mobile node, packets sent by the mobile node MAY include a Home Address destination option.

Packets containing a Home Address option MUST be dropped if the given home address is not a unicast routable address.

Packets containing a Home Address option MUST also be dropped if there is no corresponding Binding Cache entry for the given home address. A corresponding Binding Cache entry MUST have the currently registered care-of address equal to the source address of the packet. These tests MUST NOT be done for packets that contain a Binding Update and a Home Address option.

If the packet is dropped due the above tests, the correspondent node SHOULD send the Binding Error message as described in Section 9.3.3. The Status field in this message should be set to 1 (unknown binding for Home Address destination option).

The correspondent node 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, it MUST be possible to process the packet without the knowledge that it came originally from a care-of address or that a Home Address option was used.

No additional authentication of the Home Address option is required, except that if the IPv6 header of a packet is covered by authentication, then that authentication MUST also cover the Home Address option; this coverage is achieved automatically by the definition of the Option Type code for the Home Address option, since it indicates that the data within the option cannot change en-route to the packet's final destination, and thus the option is included in the authentication computation. By requiring that any authentication of the IPv6 header also cover the Home Address option, the security of the Source Address field in the IPv6 header is not compromised by the presence of a Home Address option. When attempting to verify authentication data in a packet that contains a Home Address option, the receiving node MUST make the calculation as if the care-of address were present in the Home Address option, and the home address were present in the source IPv6 address field of the IPv6 header. This conforms with the calculation specified in Section 11.3.2.

9.3.2. Sending Packets to a Mobile Node

Before sending any 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 mobile node (the destination node) by way of its care-of address. Assuming there are no additional routing headers in this packet beyond those needed by Mobile IPv6, the mobile node sets 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 mobile node'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 mobile node's care-of address copied from the Binding Cache entry. The Segments Left field is, however, temporarily set to zero.

The IP layer will insert the routing header before performing IPsec processing. The IPsec Security Policy Database will be consulted based on the IP source address and the destination address (which will be the mobile node's home address). Once all IPsec processing has been performed, the node swaps the IPv6 destination field with the Home Address field in the routing header, sets the Segments Left field to one, and sends the packet. This ensures the AH calculation is done on the packet in the form it will have on the receiver after advancing the routing header.

Following the definition of a type 2 routing header in Section 6.4, this packet will be routed to the mobile node's care-of address, where it will be delivered to the mobile node (the mobile node has associated the care-of address with its network interface).

Note that following the above conceptual model in an implementation creates some additional requirements for path MTU discovery since the layer that decides the packet size (e.g., TCP and applications using UDP) needs to be aware of the size of the headers added by the IP layer on the sending node.

If, instead, 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 a mobile node (or is a mobile node 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 a mobile node that is currently away from home, the packet will be intercepted by the mobile node's home agent and tunneled to the mobile node's current primary care-of address.

9.3.3. Sending Binding Error Messages

Sections 9.2 and 9.3.1 describe error conditions that lead to a need to send a Binding Error message.

A Binding Error message is sent 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 MUST be 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.

Binding Error messages are subject to rate limiting in the same manner as is done for ICMPv6 messages [14].

9.3.4. Receiving ICMP Error Messages

When the correspondent node has a Binding Cache entry for a mobile node, all traffic destined to the mobile node goes directly to the current care-of address of the mobile node using a routing header. Any ICMP error message caused by packets on their way to the care-of address will be returned in the normal manner to the correspondent node.

On the other hand, if the correspondent node has no Binding Cache entry for the mobile node, the packet will be routed through the mobile node's home link. Any ICMP error message caused by the packet on its way to the mobile node while in the tunnel, will be transmitted to the mobile node's home agent. By the definition of IPv6 encapsulation [15], the home agent MUST relay certain ICMP error messages back to the original sender of the packet, which in this case is the correspondent node.

Thus, in all cases, any meaningful ICMP error messages caused by packets from a correspondent node to a mobile node will be returned to the correspondent node. If the correspondent node receives persistent ICMP Destination Unreachable messages after sending packets to a mobile node based on an entry in its Binding Cache, the correspondent node SHOULD delete this Binding Cache entry.

9.4. Return Routability Procedure

This subsection specifies actions taken by a correspondent node during the return routability procedure.

9.4.1. Receiving Home Test Init Messages

Upon receiving a Home Test Init message, the correspondent node verifies the following:

- The Header Len field in the Mobility Header MUST NOT be less than the length specified in Section 6.1.3.

- The packet MUST NOT include a Home Address destination option.

Any packet carrying a Home Test Init message which fails to satisfy all of these tests MUST be silently ignored.

Otherwise, in preparation for sending the corresponding Home Test Message, the correspondent node checks that it has the necessary material to engage in a return routability procedure, as specified in Section 5.2. The correspondent node MUST have a secret Kcn and a nonce. If it does not have this material yet, it MUST produce it before continuing with the return routability procedure.

Section 9.4.3 specifies further processing.

9.4.2. Receiving Care-of Test Init Messages

Upon receiving a Care-of Test Init message, the correspondent node verifies the following:

- The Header Len field in the Mobility Header MUST NOT be less than the length specified in Section 6.1.4.

- The packet MUST NOT include a Home Address destination option.

Any packet carrying a Care-of Test Init message which fails to satisfy all of these tests MUST be silently ignored.

Otherwise, in preparation for sending the corresponding Care-of Test Message, the correspondent node checks that it has the necessary material to engage in a return routability procedure in the manner described in Section 9.4.1.

Section 9.4.4 specifies further processing.

9.4.3. Sending Home Test Messages

The correspondent node creates a home keygen token and uses the current nonce index as the Home Nonce Index. It then creates a Home Test message (Section 6.1.5) and sends it to the mobile node at the latter's home address. Note that the Home Test message is always sent to the home address of the mobile node, even when there is an existing binding for the mobile node.

9.4.4. Sending Care-of Test Messages

The correspondent node creates a care-of nonce and uses the current nonce index as the Care-of Nonce Index. It then creates a Care-of Test message (Section 6.1.6) and sends it to the mobile node at the latter's care-of address.

9.5. Processing Bindings

This section explains how the correspondent node processes messages related to bindings. These messages are:

- Binding Update

- Binding Refresh Request

- Binding Acknowledgement

- Binding Error

9.5.1. Receiving Binding Updates

Before accepting a Binding Update, the receiving node MUST validate the Binding Update according to the following tests:

- The packet MUST contain a Home Address option with a unicast routable home address, unless the Source Address is the home address of the mobile node

- The Header Len field in the Mobility Header is no less than the length specified in Section 6.1.7.

- The Sequence Number field in the Binding Update is greater than the Sequence Number received in the previous Binding Update for this home address, if any.

  This Sequence Number comparison MUST be performed modulo 2**16, i.e., the number is a free running counter represented modulo 65536. A Sequence Number in a received Binding Update is considered less than or equal to the last received number if its value lies in the range of the last received number and the preceding 32767 values, inclusive. For example, if the last received sequence number was 15, then messages with sequence numbers 0 through 15, as well as 32784 through 65535, would be considered less than or equal.

When the return routability procedure is used to enable the establishment of nonce indices as inputs to the creation of the binding key Kbm, the following are also required:

- A Nonce Indices mobility option MUST be present, and the Home and Care-of Nonce Index values in this option MUST be recent enough to be recognized by the correspondent node.

- The correspondent node MUST re-generate the home keygen token and the care-of keygen token from the information contained in the packet. It then generates the binding management key Kbm and uses it to verify the authenticator field in the Binding Update as specified in Section 6.1.7.

When using Kbm for validating the Binding Update, the following are required:

- The Binding Authorization Data mobility option MUST be present,

and its contents MUST satisfy rules presented in Section 5.2.6.
Note that a care-of address different from the Source Address MAY

have been specified by including an Alternate Care-of Address mobility option in the Binding Update. When such message is received and the return routability procedure is used as an authorization method, the correspondent node MUST verify the authenticator by using the address within the Alternate Care-of Address in the calculations.

- The Binding Authorization Data mobility option MUST be the last option and MUST NOT have trailing padding.

- The Home Registration (H) bit MUST NOT be set.

If the mobile node sends a sequence number which is not greater than the sequence number from the last successful Binding Update, then the receiving node MUST send back a Binding Acknowledgement with status code 135, and the last accepted sequence number in the Sequence Number field of the Binding Acknowledgement.

If the receiving node no longer recognizes the Home Nonce Index value, Care-of Nonce Index value, or both values from the Binding Update, then the receiving node MUST send back a Binding Acknowledgement with status code 136, 137, or 138, respectively.

Packets carrying Binding Updates that fail to satisfy all of these tests for any reason other than insufficiency of the Sequence Number or expired nonce index values MUST be silently discarded.

If the Binding Update is valid according to the tests above, then the Binding Update is processed further as follows:

- If the Lifetime specified in the Binding Update is nonzero and the specified care-of address is not equal to the home address for the binding, then this is a request to cache a binding for the mobile node. If the Home Registration (H) bit is set in the Binding Update, the Binding Update is processed according to the procedure specified in Section 10.3.1; otherwise, it is processed according to the procedure specified in Section 9.5.2.

- If the Lifetime specified in the Binding Update is zero or the specified care-of address matches the home address for the binding, then this is a request to delete the mobile node's cached binding. The update MUST include a valid home nonce index (the care-of nonce index MUST be ignored by the correspondent node). In this case, generation of the binding management key depends exclusively on the home keygen token (Section 5.2.5). If the Home Registration (H) bit is set in the Binding Update, the Binding Update is processed according to the procedure specified in Section 10.3.2; otherwise, it is processed according to the procedure specified in Section 9.5.3.

The specified care-of address MUST be determined as follows:

- If the Alternate Care-of Address option is present, the care-of address is the address in that option.

- Otherwise, the care-of address is the Source Address field in the packet's IPv6 header.

The home address for the binding MUST be determined as follows:

- If the Home Address destination option is present, the home address is the address in that option.

- Otherwise, the home address is the Source Address field in the packet's IPv6 header. This implies that the mobile node is at home and is about to perform de-registration.

9.5.2. Requests to Cache a Binding

This section describes the processing of a valid Binding Update that requests a node to cache a mobile node's binding, for which the Home Registration (H) bit is not set in the Binding Update.

In this case, the receiving node SHOULD create a new entry in its Binding Cache for this mobile node, or update its existing Binding Cache entry for this mobile node, if such an entry already exists. The lifetime for the Binding Cache entry is initialized from the Lifetime field specified in the Binding Update, although this lifetime MAY be reduced by the node caching the binding; the lifetime for the Binding Cache entry MUST NOT be greater than the Lifetime value specified in the Binding Update. Any Binding Cache entry MUST be deleted after the expiration of its lifetime.

The Sequence Number value received from a mobile node in a Binding Update is stored by a correspondent node in its Binding Cache entry for that mobile node. If the receiving correspondent node has no Binding Cache entry for the sending mobile node, it MUST accept any Sequence Number value in a received Binding Update from this mobile node.

The correspondent node MAY refuse to accept a new Binding Cache entry, if it does not have sufficient resources. A new entry MAY also be refused if the correspondent node believes its resources are utilized more efficiently in some other purpose, such as serving another mobile node with higher amount of traffic. In both cases the correspondent node SHOULD return a Binding Acknowledgement with status value 130.

9.5.3. Requests to Delete a Binding

This section describes the processing of a valid Binding Update that requests a node to delete a mobile node's binding from its Binding Cache, for which the Home Registration (H) bit is not set in the Binding Update.

Any existing binding for the mobile node MUST be deleted. A Binding Cache entry for the mobile node MUST NOT be created in response to receiving the Binding Update.

If the Binding Cache entry was created by use of return routability nonces, the correspondent node MUST ensure that the same nonces are not used again with the particular home and care-of address. If both nonces are still valid, the correspondent node 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.

9.5.4. Sending Binding Acknowledgements

A Binding Acknowledgement may be sent to indicate receipt of a Binding Update as follows:

- If the Binding Update was silently discarded as described in Section 9.5.1, a Binding Acknowledgement MUST NOT be sent.

- Otherwise, if the Acknowledge (A) bit set is set in the Binding Update, a Binding Acknowledgement MUST be sent.

- Otherwise, if the node rejects the Binding Update, a Binding Acknowledgement MUST be sent.

- Otherwise, if the node accepts the Binding Update, a Binding Acknowledgement SHOULD NOT be sent.

If the node accepts the Binding Update and creates or updates an entry for this binding, the Status field in the Binding Acknowledgement 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. Values for the Status field are described in Section 6.1.8 and in the IANA registry of assigned numbers [18].

If the Status field in the Binding Acknowledgement contains the value 136 (expired home nonce index), 137 (expired care-of nonce index), or 138 (expired nonces), then the message MUST NOT include the Binding Authorization Data mobility option. Otherwise, the Binding Authorization Data mobility option MUST be included, and MUST meet the specific authentication requirements for Binding Acknowledgements as defined in Section 5.2.

If the Source Address field of the IPv6 header that carried the Binding Update does not contain a unicast address, the Binding Acknowledgement MUST NOT be sent, and the Binding Update packet MUST be silently discarded. Otherwise, the acknowledgement MUST be sent to the Source Address. Unlike the treatment of regular packets, this addressing procedure does not use information from the Binding Cache.

If the Source Address is the home address of the mobile node, i.e., the Binding Update did not contain a Home Address destination option, then the Binding Acknowledgement MUST be sent to that address, and the routing header MUST NOT be used. Otherwise, the Binding Acknowledgement MUST be sent using a type 2 routing header which contains the mobile node's home address.

Entries in a node's Binding Cache MUST be deleted when their lifetime expires.

9.5.5. Sending Binding Refresh Requests

If a Binding Cache entry being deleted is still in active use in sending packets to a mobile node, the next packet sent to the mobile node will be routed normally to the mobile node's home link. Communication with the mobile node continues, but the tunneling from the home network creates additional overhead and latency in delivering packets to the mobile node.

If the sender knows that the Binding Cache entry is still in active use, it MAY send a Binding Refresh Request message to the mobile node in an attempt to avoid this overhead and latency due to deleting and recreating the Binding Cache entry. The Binding Refresh Request message is sent in the same way as any packet addressed to the mobile node (Section 9.3.2).

The correspondent node MAY retransmit Binding Refresh Request messages provided that rate limitation is applied. The correspondent node SHOULD stop retransmitting when it receives a Binding Update.

9.6. Cache Replacement Policy

Conceptually, a node maintains 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 Binding Update, the node sets the timer for this entry to the specified Lifetime period. Any entry in a node's Binding Cache MUST be deleted after the expiration of the Lifetime specified in the Binding Update from which the entry was created or last updated.

Each node's Binding Cache will, by necessity, have a finite size. A node MAY use any reasonable local policy for managing the space within its Binding Cache, except that any entry marked as a home registration (Section 10.3.1) MUST NOT be deleted from the cache until the expiration of its lifetime period. When such home registration entries are deleted, the home agent MUST also cease intercepting packets on the mobile node's home link addressed to the mobile node (Section 10.4.1), just as if the mobile node had de-registered its primary care-of address (see Section 10.3.2).

When attempting to add a new home registration entry in response to a Binding Update with the Home Registration (H) bit set, if no sufficient space can be found, the home agent MUST reject the Binding Update. Furthermore, the home agent MUST return a Binding Acknowledgement to the sending mobile node, in which the Status field is set to 130 (insufficient resources).

A node MAY choose to drop any entry already in its Binding Cache, other than home registration entries, in order to make space for a new entry. For example, a "least-recently used" (LRU) strategy for cache entry replacement among entries not marked as home registrations is likely to work well unless the size of the Binding Cache is substantially insufficient.

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 mobile node's home link. The mobile node can detect this, and establish a new binding if necessary.

10. Home Agent Operation

10.1. Conceptual Data Structures

Each home agent MUST maintain a Binding Cache and Home Agents List.

The rules for maintaining a Binding Cache are same for home agents and correspondent nodes, and have already been described in Section 9.1.

The Home Agents List is maintained by each home agent, recording information about each router on the same link which is acting as a home agent; this list is used by the dynamic home agent address discovery mechanism. A router is known to be acting as a home agent, if it sends a Router Advertisement in which the Home Agent (H) bit is set. When the lifetime for a list entry (defined below) expires, that entry is removed from the Home Agents List. The Home Agents List is thus similar to the Default Router List conceptual data structure maintained by each host for Neighbor Discovery [12]. The Home Agents List MAY be implemented in any manner consistent with the external behavior described in this document.

Each home agent maintains a separate Home Agents List for each link on which it is serving as a home agent. A new entry is created or an existing entry is updated in response to receipt of a valid Router Advertisement in which the Home Agent (H) bit is set. Each Home Agents List entry conceptually contains the following fields:

- The link-local IP address of a home agent on the link. This address is learned through the Source Address of the Router Advertisements received from the router [12].

- One or more global IP addresses for this home agent. Global addresses are learned through Prefix Information options with the Router Address (R) bit set, received in Router Advertisements from this link-local address. Global addresses for the router in a Home Agents List entry MUST be deleted once the prefix associated with that address is no longer valid [12].

- The remaining lifetime of this Home Agents List entry. If a Home Agent Information Option is present in a Router Advertisement received from a home agent, the lifetime of the Home Agents List entry representing that home agent is initialized from the Home Agent Lifetime field in the option; otherwise, the lifetime is initialized from the Router Lifetime field in the received Router Advertisement. If Home Agents List entry lifetime reaches zero, the entry MUST be deleted from the Home Agents List.

- The preference for this home agent; higher values indicate a more preferable home agent. The preference value is taken from the Home Agent Preference field in the received Router Advertisement, if the Router Advertisement contains a Home Agent Information Option, and is otherwise set to the default value of 0. A home agent uses this preference in ordering the Home Agents List when it sends an ICMP Home Agent Address Discovery message.

10.2. Processing Mobility Headers

All IPv6 home agents MUST observe the rules described in Section 9.2 when processing Mobility Headers.

10.3. Processing Bindings

10.3.1. Primary Care-of Address Registration

When a node receives a Binding Update, it MUST validate it and determine the type of Binding Update according to the steps described in Section 9.5.1. Furthermore, it MUST authenticate the Binding Update as described in Section 5.1. This includes authorization of the particular node to control a particular home address, as the home address unequivocally identifies the security association that must be used.

This section describes the processing of a valid and authorized Binding Update, when it requests the registration of the mobile node's primary care-of address.

To begin processing the Binding Update, the home agent MUST perform the following sequence of tests:

- If the node is not a router that implements home agent functionality, then the node MUST reject the Binding Update and MUST return a Binding Acknowledgement to the mobile node, in which the Status field is set to 131 (home registration not supported).

- Else, if the home address for the binding (the Home Address field in the packet's Home Address option) is not an on-link IPv6 address with respect to the home agent's current Prefix List, then the home agent MUST reject the Binding Update and SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to 132 (not home subnet).

- Else, if the home agent chooses to reject the Binding Update for any other reason (e.g., insufficient resources to serve another mobile node as a home agent), then the home agent SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to an appropriate value to indicate the reason for the rejection.

- A Home Address destination option MUST be present in the message.

- Finally, if the Duplicate Address Detection (D) bit is set in the Binding Update, this home agent MUST perform Duplicate Address Detection [13] on the mobile node's home link for the link-local address associated with the home address in this binding, before returning the Binding Acknowledgement. This ensures that no other node on the home link was using the mobile node's home address when the Binding Update arrived.

If home agent accepts the Binding Update, it MUST then create a new entry in its Binding Cache for this mobile node, or update its existing Binding Cache entry, if such an entry already exists. The Home Address field as received in the Home Address option provides the home address of the mobile node.

The home agent MUST mark this Binding Cache entry as a home registration to indicate that the node is serving as a home agent for this binding. Binding Cache entries marked as a home registration

MUST be excluded from the normal cache replacement policy used for the Binding Cache (Section 9.6) and MUST NOT be removed from the Binding Cache until the expiration of the Lifetime period.

Normal processing for Duplicate Address Detection specifies that, in certain cases, the node SHOULD delay sending the initial Neighbor Solicitation of Duplicate Address Detection by a random delay between 0 and MAX_RTR_SOLICITATION_DELAY [12, 13]. However, when the Duplicate Address Detection (D) bit instructs the home agent to perform Duplicate Address Detection, the home agent SHOULD NOT perform such a delay. If this Duplicate Address Detection fails, then the home agent MUST reject the Binding Update and MUST return a Binding Acknowledgement to the mobile node, in which the Status field is set to 134 (Duplicate Address Detection failed). When the home agent sends a successful Binding Acknowledgement to the mobile node, the home agent assures to the mobile node that its home address will continue to be kept unique by the home agent at least as long as the lifetime granted for that home address binding is not over.

If the Single Address Only (S) bit in the Binding Update is zero, the home agent creates Binding Cache entries for each of possibly several home addresses. The set of such home addresses is formed by replacing the routing prefix for the given home address with all other routing prefixes on the mobile node's home link that are supported by the home agent processing the Binding Update. The home agent creates such a separate primary care-of address registration for each such home address. Note that the same considerations for Duplicate Address Detection apply for each affected home address. The value of the Single Address Only (S) bit field is examined only for new registrations. Its value is ignored on de-registrations and re-registrations of the same addresses.

The specific addresses which are to be tested before accepting the Binding Update, and later to be defended by performing Duplicate Address Detection, depend on the settings of the Single Address Only (S) and Link-Local Address Compatibility (L) bits, as follows:

- L=0: Defend the given address. The Single Address Only (S) bit is ignored in this case since we cannot derive other on-link addresses without knowing the interface identifier.

- L=1 and S=0: Defend all non link-local unicast addresses possible on link and the derived link-local.

- L=1 and S=1: Defend both the given non link-local unicast (home) address and the derived link-local.

The lifetime of the Binding Cache entry depends on a number of factors:

- The lifetime for the Binding Cache entry MUST NOT be greater than the Lifetime value specified in the Binding Update.

- The lifetime for the Binding Cache entry MUST NOT be greater than the remaining valid lifetime for the subnet prefix in the mobile node's home address specified with the Binding Update. The remaining valid lifetime for this prefix is determined by the home agent based on its own Prefix List entry for this prefix [12].

- However, if the Single Address Only (S) bit field in the Binding Update is zero, the lifetime for that Binding Cache entry MUST NOT be greater than the minimum remaining valid lifetime for all subnet prefixes on the mobile node's home link. If the value of the Lifetime field specified by the mobile node in its Binding Update is greater than this prefix lifetime, the home agent MUST decrease the binding lifetime to less than or equal to the prefix valid lifetime.

- The home agent MAY further decrease the specified lifetime for the binding, for example based on a local policy. The resulting lifetime is stored by the home agent in the Binding Cache entry, and this Binding Cache entry MUST be deleted by the home agent after the expiration of this lifetime.

Regardless of the setting of the Acknowledge (A) bit in the Binding Update, the home agent MUST return a Binding Acknowledgement to the mobile node, constructed as follows:

- The Status field MUST be set to a value 0, indicating success.

- The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.

- The Lifetime field MUST be set to the remaining lifetime for the binding as set by the home agent in its home registration Binding Cache entry for the mobile node, as described above.

- If the home agent stores the Binding Cache entry in nonvolatile storage, then the Binding Refresh Advice mobility option MUST be omitted. Otherwise, the home agent MAY include this option to suggest that the mobile node refreshes its binding sooner than the actual lifetime of the binding ends.

  If the Binding Refresh Advice mobility option is present, the Refresh Interval field in the option MUST be set to a value less than the Lifetime value being returned in the Binding Update. This indicates that the mobile node SHOULD attempt to refresh its home registration at the indicated shorter interval. The home agent MUST still retain the registration for the Lifetime period, even if the mobile node does not refresh its registration within the Refresh period.

The rules for selecting the Destination IP address (and possibly routing header construction) for the Binding Acknowledgement to the mobile node are the same as in Section 9.5.4.

In addition, the home agent MUST follow the procedure defined in Section 10.4.1 to intercept packets on the mobile node's home link addressed to the mobile node, while the home agent is serving as the home agent for this mobile node. The home agent MUST also be prepared to accept reverse tunneled packets from the new care-of address of the mobile node, as described in Section 10.4.3. Finally, the home agent MUST also propagate new home network prefixes, as described in Section 10.6.

10.3.2. Primary Care-of Address De-Registration

A Binding Update is validated and authorized in the manner described in the previous section. This section describes the processing of a valid Binding Update that requests the receiving node to no longer serve as its home agent, de-registering its primary care-of address.

To begin processing the Binding Update, the home agent MUST perform the following test:

- If the receiving node has no entry marked as a home registration in its Binding Cache for this mobile node, then this node MUST reject the Binding Update and SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to 133 (not home agent for this mobile node).

If the home agent does not reject the Binding Update as described above, then it MUST delete any existing entry in its Binding Cache for this mobile node. Then, the home agent MUST return a Binding Acknowledgement to the mobile node, constructed as follows:

- The Status field MUST be set to a value 0, indicating success.

- The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.

- The Lifetime field MUST be set to zero.

- The Binding Refresh Advice mobility option MUST be omitted.

In addition, the home agent MUST stop intercepting packets on the mobile node's home link that are addressed to the mobile node (Section 10.4.1).

The rules for selecting the Destination IP address (and, if required, routing header construction) for the Binding Acknowledgement to the mobile node are the same as in the previous section. When the Status field in the Binding Acknowledgement is greater than or equal to 128 and the Source Address of the Binding Update is on the home link, the home agent MUST send it to the same link-layer address as the Binding Update came from.

10.4. Packet Processing

10.4.1. Intercepting Packets for a Mobile Node

While a node is serving as the home agent for mobile node it MUST attempt to intercept packets on the mobile node's home link that are addressed to the mobile node, and MUST tunnel each intercepted packet to the mobile node using IPv6 encapsulation [15].

In order to do this, when a node begins serving as the home agent it MUST multicast onto the home link a Neighbor Advertisement message [12] on behalf of the mobile node. Specifically, the home agent performs the following steps:

1. The home agent examines the value of the Single Address Only (S) bit in the received Binding Update. If this bit is nonzero, the next step is carried out only for the individual home address specified for this binding. If, instead, this bit is zero, then the next step is carried out for one address for each one of the subnet prefixes currently considered by the home agent to be on-link the mobile node. Each address is formed by replacing, in turn, the configured subnet prefix in the mobile node's home address. For this purpose, the set of on-link prefixes includes both the link-local and site-local prefix.

2. For each specific IP address for the mobile node determined in the first step above, the home agent sends a Neighbor Advertisement message [12] to the all-nodes multicast address on the home link, to advertise the home agent's own link-layer address for this IP address on behalf of the mobile node.

   All fields in each such Neighbor Advertisement message SHOULD be set in the same way they would be set by the mobile node itself if sending this Neighbor Advertisement while at home [12], with the following exceptions:

   - The Target Address in the Neighbor Advertisement MUST be set to the specific IP address for the mobile node.

   - The Advertisement MUST include a Target Link-layer Address option specifying the home agent's link-layer address.

   - The Router (R) bit in the Advertisement MUST be set to zero.

- The Solicited Flag (S) in the Advertisement MUST NOT be set, since it was not solicited by any Neighbor Solicitation.

- The Override Flag (O) in the Advertisement MUST be set, indicating that the Advertisement SHOULD override any existing Neighbor Cache entry at any node receiving it.

Any node on the home link receiving one of the Neighbor Advertisement messages described above will thus update its Neighbor Cache to associate the mobile node's address with the home agent's link layer address, causing it to transmit any future packets normally destined to the mobile node to the mobile node's home agent. Since multicasting on the local link (such as Ethernet) is typically not guaranteed to be reliable, the home agent MAY retransmit this Neighbor Advertisement message up to MAX_ADVERT_REXMIT (see Section 12) times to increase its reliability. It is still possible that some nodes on the home link will not receive any of these Neighbor Advertisements, but these nodes will eventually be able to detect the link-layer address change for the mobile node's home address, through use of Neighbor Unreachability Detection [12].

While a node is serving as a home agent for some mobile node, the home agent uses IPv6 Neighbor Discovery [12] to intercept unicast packets on the home link addressed to the mobile node's home address. In order to intercept packets in this way, the home agent MUST act as a proxy for this mobile node, and reply to any received Neighbor Solicitations for it. When a home agent receives a Neighbor Solicitation, it MUST check if the Target Address specified in the message matches the home address of any mobile node for which it has a Binding Cache entry marked as a home registration. Note that Binding Update with the Single Address Only (S) bit set to zero will result in multiple Binding Cache entries, so checks on all these entries necessarily include all possible home addresses for the mobile node.

If such an entry exists in the home agent's Binding Cache, the home agent MUST reply to the Neighbor Solicitation with a Neighbor Advertisement, giving the home agent's own link-layer address as the link-layer address for the specified Target Address. In addition, the Router (R) bit in the Advertisement MUST be set to zero. Acting as a proxy in this way allows other nodes on the mobile node's home link to resolve the mobile node's IPv6 home address, and allows the home agent to defend these addresses on the home link for Duplicate Address Detection [12].

10.4.2. Tunneling Intercepted Packets to a Mobile Node

For any packet sent to a mobile node from the mobile node's home agent (for which the home agent is the original sender of the packet), the home agent is operating as a correspondent node of the mobile node for this packet and the procedures described in Section 9.3.2 apply. The home agent then uses a routing header to route the packet to the mobile node by way of the primary care-of address in the home agent's Binding Cache.

While the mobile node is away from home, the home agent intercepts any packets on the home link addressed to the mobile node's home address (including addresses formed from other on-link prefixes, if the Single Address Only (S) bit was zero in the Binding Update), as described in Section 10.4.1. In order to forward each intercepted packet to the mobile node, the home agent MUST tunnel the packet to the mobile node using IPv6 encapsulation [15]. When a home agent encapsulates an intercepted packet for forwarding to the mobile node, the home agent sets the Source Address in the new tunnel IP header to the home agent's own IP address, and sets the Destination Address in the tunnel IP header to the mobile node's primary care-of address. When received by the mobile node, normal processing of the tunnel header [15] will result in decapsulation and processing of the original packet by the mobile node.

However, packets addressed to the mobile node's link-local address MUST NOT be tunneled to the mobile node. Instead, such a packet MUST be discarded, and the home agent SHOULD return an ICMP Destination Unreachable, Code 3, message to the packet's Source Address (unless this Source Address is a multicast address). Packets addressed to the mobile node's site-local address SHOULD be tunneled to the mobile node by default, but this behavior MUST be configurable to disable it; currently, the exact definition and semantics of a "site" and a site-local address are incompletely defined in IPv6, and this default behavior might change at some point in the future.

Tunneling of multicast packets to a mobile node follows similar limitations to those defined above for unicast packets addressed to the mobile node's link-local and site-local addresses. Multicast packets addressed to a multicast address with link-local scope [3], to which the mobile node is subscribed, MUST NOT be tunneled to the mobile node; such packets SHOULD be silently discarded (after delivering to other local multicast recipients). Multicast packets addressed to a multicast address with scope larger than link-local but smaller than global (e.g., site-local and organization-local [3]), to which the mobile node is subscribed, SHOULD be tunneled to the mobile node by default. This behavior MUST be configurable to allow changing or disabling it. Note that this default behavior might change at some point in the future as the definition of these scopes become more completely defined in IPv6.

Before tunneling a packet to the mobile node, the home agent MUST perform any IPsec processing as indicated by the security policy data base.

10.4.3. Handling Reverse Tunneled Packets from a Mobile Node

Unless a binding has been established between the mobile node and a correspondent node, traffic from the mobile node to the correspondent node goes through a reverse tunnel. Home agents MUST support reverse tunneling as follows:

- The tunneled traffic arrives to the home agent using IPv6 encapsulation [15].

- The tunnel entry point is the primary care-of address as registered with the home agent and the tunnel exit point is the home agent.

- When a home agent decapsulates a tunneled packet from the mobile node, the home agent MUST verify that the Source Address in the tunnel IP header is the mobile node's primary care-of address. Otherwise any node in the Internet could send traffic through the home agent and escape ingress filtering limitations.

Reverse tunneled packets MAY be discarded unless accompanied by a valid AH or ESP header, depending on the security policies used by the home agent. The support for authenticated reverse tunneling allows the home agent to protect the home network and correspondent nodes from malicious nodes masquerading as a mobile node, even if they know the current location of the real mobile node.

10.4.4. Protecting Return Routability Packets

The return routability procedure described in Section 5.2.5 assumes that the confidentiality of the Home Test Init and Home Test messages is protected as they are tunneled between the home agent to the mobile node. Therefore, the home agent MUST support tunnel mode IPsec ESP for the protection of packets belonging to the return routability procedure. Support for a non-null encryption transform and authentication algorithm MUST be available. It isn't necessary to distinguish between different kinds of packets within the return routability procedure.

The security association between the home agent and the mobile node MUST change its destination address (tunnel gateway address) when the care-of address for the mobile node changes [24].

The above protection SHOULD be used with all mobile nodes. The use is controlled by configuration of the IPsec security policy database both at the mobile node and at the home agent.

As described earlier, the Binding Update and Binding Acknowledgement messages require protection between the home agent and the mobile node. These messages and the return routability messages employ the same protocol from the point of view of the security policy database, the Mobility Header. The security policy database entries MUST be defined as if they were specifically for the tunnel interface between the mobile node and the home agent. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters the tunnel. This makes use of per-interface security policy database entries [4], specific to the tunnel interface (the node's attachment to the tunnel [11]).

10.5. Dynamic Home Agent Address Discovery

This section describes how a home agent can help mobile nodes to discover the addresses of the home agents. The home agent keeps track of the other home agents on the same link, and responds to queries sent by the mobile node.

10.5.1. Receiving Router Advertisement Messages

For each link on which a router provides service as a home agent, the router maintains a Home Agents List recording information about all other home agents on that link. This list is used in the dynamic home agent address discovery mechanism, described in Section 10.5. The information for the list is learned through receipt of the periodic unsolicited multicast Router Advertisements, in a manner similar to the Default Router List conceptual data structure maintained by each host for Neighbor Discovery [12]. In the construction of the Home Agents List, the Router Advertisements are from each other home agent on the link, and the Home Agent (H) bit is set in them.

On receipt of a valid Router Advertisement, as defined in the processing algorithm specified for Neighbor Discovery [12], the home agent performs the following steps, in addition to any steps already required of it by Neighbor Discovery:

- If the Home Agent (H) bit in the Router Advertisement is not set, check to see if the sending node has an entry in the current Home Agents List. If it does, delete the corresponding entry. In any case all of the following steps are skipped.

- Otherwise, extract the Source Address from the IP header of the Router Advertisement. This is the link-local IP address on this link of the home agent sending this Advertisement [12].

- Determine the preference for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the preference is taken from the Home Agent Preference field in the option; otherwise, the default preference of 0 MUST be used.

- Determine the lifetime for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the lifetime is taken from the Home Agent Lifetime field in the option; otherwise, the lifetime specified by the Router Lifetime field in the Router Advertisement SHOULD be used.

- If the link-local address of the home agent sending this Advertisement is already present in this home agent's Home Agents List and the received home agent lifetime value is zero, immediately delete this entry in the Home Agents List.

- Otherwise, if the link-local address of the home agent sending this Advertisement is already present in the receiving home agent's Home Agents List, reset its lifetime and preference to the values determined above.

- If the link-local address of the home agent sending this Advertisement is not already present in the Home Agents List maintained by the receiving home agent, and the lifetime for the sending home agent is non-zero, create a new entry in the list, and initialize its lifetime and preference to the values determined above.

- If the Home Agents List entry for the link-local address of the home agent sending this Advertisement was not deleted as described above, determine any global address(es) of the home agent based on each Prefix Information option received in this Advertisement in which the Router Address (R) bit is set (Section 7.2). Add all such global addresses to the list of global addresses in this Home Agents List entry.

A home agent SHOULD maintain an entry in its Home Agents List for each valid home agent address until that entry's lifetime expires, after which time the entry MUST be deleted.

As described in Section 11.4.1, a mobile node attempts dynamic home agent address discovery by sending an ICMP Home Agent Address Discovery Request message to the Mobile IPv6 Home-Agents anycast address [16] for its home IP subnet prefix. A home agent receiving such a Home Agent Address Discovery Request message that is serving this subnet SHOULD return an ICMP Home Agent Address Discovery Reply message to the mobile node, with the Source Address of the Reply packet set to one of the global unicast addresses of the home agent. The Home Agent Addresses field in the Reply message is constructed as follows:

- The Home Agent Addresses field SHOULD contain one global IP address for each home agent currently listed in this home agent's own Home Agents List (Section 10.1). However, if this home agent's own global IP address would be placed as the first entry in the list (as described below), then this home agent SHOULD NOT include its own address in the Home Agent Addresses field in the Reply message. Not placing this home agent's own IP address in the list will cause the receiving mobile node to consider this home agent as the most preferred home agent; otherwise, this home agent will be considered to be preferred in its order given by its place in the list returned.

- The IP addresses in the Home Agent Addresses field SHOULD be listed in order of decreasing preference values, based either on the respective advertised preference from a Home Agent Information option or on the default preference of 0 if no preference is advertised (or on the configured home agent preference for this home agent itself).

- Among home agents with equal preference, their IP addresses in the Home Agent Addresses field SHOULD be listed in an order randomized with respect to other home agents with equal preference, each time a Home Agent Address Discovery Reply message is returned by this home agent.

- For each entry in this home agent's Home Agents List, if more than one global IP address is associated with this list entry, then one of these global IP addresses SHOULD be selected to include in the Home Agent Addresses field in the Reply message.

  The selected global IP address for each home agent to include in forming the Home Agent Addresses field in the Reply message MUST be the global IP address of the respective home agent sharing a prefix with the Destination IP address of the Request message. If no such global IP address is known for some home agent, an entry for that home agent MUST NOT be included in the Home Agent Addresses field in the Reply message.

- The home agent SHOULD reduce the number of home agent IP addresses so that the packet fits within the minimum IPv6 MTU [11]. The home agent addresses selected for inclusion in the packet SHOULD be those from the complete list with the highest preference. This limitation avoids the danger of the Reply message packet being fragmented (or rejected by an intermediate router with an ICMP Packet Too Big message [14]).

- If the Reply message packet must be truncated to fit within the minimum IPv6 MTU, and the home agent sending the message is not the highest priority, then its address MUST appear in the list sent to avoid implying that it is the highest priority. Therefore, if this home agent would not appear in the truncated list because it is of lower priority than the last entry, this home agent's address must be substituted for the last entry.

10.6. Sending Prefix Information to the Mobile Node

10.6.1. Aggregate List of Home Network Prefixes

Mobile IPv6 arranges to propagate relevant prefix information to the mobile node when it is away from home, so that it may be used in mobile node home address configuration, and in network renumbering. In this mechanism, mobile nodes away from home receive Mobile Prefix Advertisements messages with Prefix Information Options, which give the valid lifetime and preferred lifetime for available prefixes on the home link.

A mobile node on a remote network SHOULD autoconfigure all of the global IP addresses, which it would autoconfigure if it were attached to its home network and which are from prefixes served by home agents. Site-local addresses MAY be autoconfigured if the mobile node is roaming in a network on the same site as its home addresses. Site-local addresses and addresses not served by a home agent MUST NOT be autoconfigured, since they are unusable in the remote network.

To support this, the home agent monitors prefixes advertised by itself and other home agents routers on the home link, and passes this aggregated list of relevant subnet prefixes on to the mobile node in Mobile Prefix Advertisements.

The home agent SHOULD construct the aggregate list of home subnet prefixes as follows:

- Copy prefix information defined in the home agent's AdvPrefixList on the home subnet's interfaces to the aggregate list. Also apply any changes made to the AdvPrefixList on the home agent to the aggregate list.

- Check valid prefixes received in Router Advertisements from the home network for consistency with the home agent's AdvPrefixList, as specified in Section 6.2.7 of RFC 2461 [12]. Do not update the aggregate list with any information from received prefixes that fail this check.

- For Router Advertisements which have the Home Agent (H) bit set, check valid prefixes that are not yet in the aggregate list. If a Prefix Information option has the autonomous address configuration (A) flag set and the prefix length is valid for address autoconfiguration on the home subnet, add these advertisements and preserve the on-link (L) flag value. Clear the Router Address (R) flag and zero the interface-id portion of the prefix field to prevent mobile nodes from treating another router's interface address as belonging to the home agent. Treat the lifetimes of these prefixes as decrementing in real time, as defined in Section 6.2.7 of RFC 2461 [12].

- Do not perform consistency checks on valid prefixes received in Router Advertisements on the home network that do not exist in the home agent's AdvPrefixList. Instead, if the prefixes already exist in the aggregate list, update the prefix lifetime fields in the aggregate list according to the rules specified for hosts in Section 6.3.4 of RFC 2461 [12] and Section 5.5.3 of RFC 2462 [13].

- If the L flag is set on valid prefixes received in a Router Advertisement, and that prefix already exists in the aggregate list, set the flag in the aggregate list. Ignore the flag if it is clear.

- Delete prefixes from the aggregate list when their valid lifetimes expire.

The home agent uses the information in the aggregate list to construct Mobile Prefix Advertisements. It may be possible to construct an aggregate list by combining information contained in the home agent's AdvPrefixList and its Home Agents List used for Dynamic Home Agent Address Discovery (Section 11.4.1).

10.6.2. Scheduling Prefix Deliveries to the Mobile Node

A home agent serving a mobile node will schedule the delivery of new prefix information to that mobile node when any of the following conditions occur:

MUST:

- The valid or preferred lifetime or the state of the flags changes for the prefix of the mobile node's registered home address.

- The mobile node requests the information with a Mobile Prefix Solicitation (see Section 11.4.2).

MAY:

- A new prefix is added to the aggregate list.

- The valid or preferred lifetime or the state of the flags changes for a prefix which is not used in any Binding Cache entry for this mobile node.

The home agent uses the following algorithm to determine when to send prefix information to the mobile node.

- If the mobile node has not received the prefix information within the last HomeRtrAdvInterval (see Section 12) seconds, then transmit the prefix information. This MAY be done according to a periodically scheduled transmission.

- If a mobile node sends a solicitation, answer right away.

- If a prefix in the aggregate list that matches the mobile node's home registration is added, or if its information changes in any way that does not cause the mobile node's address to go deprecated, ensure that a transmission is scheduled (as described below), and calculate RAND_ADV_DELAY in order to randomize the time at which the transmission is scheduled.

- If a home registration expires, cancel any scheduled advertisements to the mobile node.

The aggregate list is sent in its entirety in all cases.

Suppose that the home agent already has scheduled the transmission of a Mobile Prefix Advertisement to the mobile node. The home agent deletes the previously scheduled transmission event and schedules another advertisement to the mobile node.

Otherwise, the home agent computes a fresh value for RAND_ADV_DELAY, the offset from the current time for the scheduled transmission as follows. First calculate the maximum delay for the scheduled Advertisement:

```
MaxScheduleDelay = min (MaxMobPfxAdvInterval, Preferred Lifetime),
```

where MaxMobPfxAdvInterval is as defined in Section 12. Then compute the final delay for the advertisement:

```
RAND_ADV_DELAY = MinMobPfxAdvInterval +
      (rand() % abs(MaxScheduleDelay - MinMobPfxAdvInterval))
```

This computation is expected to alleviate bursts of advertisements when prefix information changes. In addition, a home agent MAY further reduce the rate of packet transmission by further delaying individual advertisements, if needed to avoid overwhelming local network resources. The home agent SHOULD periodically continue to retransmit an unsolicited Advertisement to the mobile node, until it is acknowledged by the receipt of a Mobile Prefix Solicitation from the mobile node.

The home agent MUST wait PREFIX_ADV_TIMEOUT (see Section 12) before the first retransmission, and double the retransmission wait time for every succeeding retransmission, up until a maximum of PREFIX_ADV_RETRIES attempts (see Section 12). If the mobile node's bindings expire before the matching Binding Update has been received, then the home agent MUST NOT attempt any more retransmissions, even if not all PREFIX_ADV_RETRIES have been retransmitted. If the mobile node sends another Binding Update without returning home in the meantime, the home agent SHOULD again begin transmitting the unsolicited Advertisement.

If some condition as described above occurs on the home link causes another Prefix Advertisement to be sent to the mobile node, before the mobile node acknowledges a previous transmission the home agent SHOULD combine any Prefix Information options in the unacknowledged Mobile Prefix Advertisement into a new Advertisement. The home agent discards the old Advertisement.

10.6.3. Sending Advertisements to the Mobile Node

When sending a Mobile Prefix Advertisement to the mobile node, the home agent MUST construct the packet as follows:

- The Source Address in the packet's IPv6 header MUST be set to the home agent's IP address to which the mobile node addressed its current home registration, or its default global home agent address if no binding exists.

- If the advertisement was solicited, it MUST be destined to the source address of the solicitation. If it was triggered by prefix changes or renumbering, the advertisement's destination will be the mobile node's home address in the binding which triggered the rule.

- A type 2 routing header MUST be included with the mobile node's home address.

- IPsec headers SHOULD be supported and used.

- The home agent MUST send the packet as it would any other unicast IPv6 packet that it originates.

10.6.4. Lifetimes for Changed Prefixes

As described in Section 10.3.1, the lifetime returned by the home agent in a Binding Acknowledgement MUST be no greater than the remaining valid lifetime for the subnet prefix in the mobile node's home address. This limit on the binding lifetime serves to prohibit use of a mobile node's home address after it becomes invalid.

11. Mobile Node Operation

11.1. Conceptual Data Structures

Each mobile node MUST maintain a Binding Update List.

The Binding Update List records information for each Binding Update sent by this mobile node, for which the Lifetime sent in that Binding Update has not yet expired. The Binding Update List includes all bindings sent by the mobile node either to its home agent or correspondent nodes. It also contains Binding Updates which are waiting for the completion of the return routability procedure before they can be sent. However, for multiple Binding Updates sent to the same destination address, the Binding Update List contains only the most recent Binding Update (i.e., with the greatest Sequence Number value) sent to that destination. The Binding Update List MAY be implemented in any manner consistent with the external behavior described in this document.

Each Binding Update List entry conceptually contains the following fields:

- The IP address of the node to which a Binding Update was sent. If the Binding Update was successfully received by that node (e.g., not lost by the network), a Binding Cache entry may have been created or updated based on this Binding Update. The Binding Cache entry may still exist, if that node has not deleted the entry before its expiration for some reason.

- The home address for which that Binding Update was sent.

- The care-of address sent in that Binding Update. This value is necessary for the mobile node to determine if it has sent a Binding Update giving its new care-of address to this destination after changing its care-of address.

- The initial value of the Lifetime field sent in that Binding Update.

- The remaining lifetime of that binding. This lifetime is initialized from the Lifetime value sent in the Binding Update and is decremented until it reaches zero, at which time this entry MUST be deleted from the Binding Update List.

- The maximum value of the Sequence Number field sent in previous Binding Updates to this destination. The Sequence Number field is 16 bits long, and all comparisons between Sequence Number values MUST be performed modulo 2**16 (see Section 9.5.1).

- The time at which a Binding Update was last sent to this destination, as needed to implement the rate limiting restriction for sending Binding Updates.

- The state of any retransmissions needed for this Binding Update, if the Acknowledge (A) bit was set in this Binding Update. This state includes the time remaining until the next retransmission attempt for the Binding Update, and the current state of the exponential back-off mechanism for retransmissions.

- A flag specifying whether or not future Binding Updates should be sent to this destination. The mobile node sets this flag in the Binding Update List entry when it receives an ICMP Parameter Problem, Code 1, error message in response to a return routability message or Binding Update sent to that destination, as described in Section 11.3.4.

The Binding Update list also conceptually contains the following data related to running the return routability procedure. This data is relevant only for Binding Updates sent to correspondent nodes.

- The time at which a Home Test Init or Care-of Test Init message was last sent to this destination, as needed to implement the rate limiting restriction for the return routability procedure.

- The state of any retransmissions needed for this return routability procedure. This state includes the time remaining until the next retransmission attempt and the current state of the exponential back-off mechanism for retransmissions.

- Cookie values used the Home Test Init and Care-of Test Init messages.

- Home and care-of keygen tokens received from the correspondent node.

- Home and care-of nonce indices received from the correspondent node.

- The time at which each of the tokens and nonces was received from this correspondent node, as needed to implement reuse while moving.

11.2. Processing Mobility Headers

All IPv6 mobile nodes MUST observe the rules described in Section 9.2 when processing Mobility Headers.

11.3. Packet Processing

11.3.1. Sending Packets While Away from Home

While a mobile node is away from home, it continues to use its home address, as well as also using one or more care-of addresses. When sending a packet while away from home, a mobile node MAY choose among these in selecting the address that it will use as the source of the packet, as follows:

- Protocols layered over IP will generally treat the mobile node's home address as its IP address for most packets. For packets sent that are part of transport-level connections established while the mobile node was at home, the mobile node MUST use its home address. Likewise, for packets sent that are part of transport-level connections that the mobile node may still be using after moving to a new location, the mobile node SHOULD use its home address in this way. If a binding exists, the mobile node SHOULD send the packets directly to the correspondent node. Otherwise, if a binding does not exist, the mobile node MUST use reverse tunneling. Detailed operation for both of these cases is described later in this section.

- The mobile node MAY choose to directly use one of its care-of addresses as the source of the packet, not requiring the use of a Home Address option in the packet. This is particularly useful for short-term communication that may easily be retried if it fails. An example of this type of communication might be DNS queries sent by the mobile node [27, 28]. Using the mobile node's care-of address as the source for such queries will generally have a lower overhead than using the mobile node's home address, since no extra options need be used in either the query or its reply. Such packets can be routed normally, directly between their source and destination without relying on Mobile IPv6. If application running on the mobile node has no particular knowledge that the communication being sent fits within this general type of communication, however, the mobile node SHOULD NOT use its care-of address as the source of the packet in this way.

  The mobile node may send packets to the correspondent node that includes the home address destination option directly to the correspondent node only if the mobile node is aware that the correspondent node already has a Binding Cache entry for the mobile node's home address. Section 9.3.1 specifies the rules for Home Address Destination Option Processing at a correspondent node. The mobile node needs to ensure that there exists a Binding Cache entry for its home address so that the correspondent node can process the packet.

- While not at its home link, the mobile node MUST NOT use its home address (or the home address destination option) in Neighbor Discovery messages on the visited link. The mobile node also MUST NOT use its home address when communicating with link-local or site-local peers on the visited link, if the scope of the home address is larger than the scope of the peer's address.

For packets sent by a mobile node while it is at home, no special Mobile IPv6 processing is required. Likewise, if the mobile node uses any address other than any of its home addresses as the source of a packet sent while away from home no special Mobile IPv6 processing is required. In either case, the packet is simply addressed and transmitted in the same way as any normal IPv6 packet.

For packets sent by the mobile node sent while away from home using the mobile node's home address as the source, special Mobile IPv6 processing of the packet is required. This can be done in the following two ways:

direct delivery

This is manner of delivering packets does not require going through the home network, and typically will enable faster and more reliable transmission. A mobile node SHOULD arrange to supply the home address in a Home Address option, and allowing the IPv6 header's Source Address field to be set to one of the mobile node's care-of addresses; the correspondent node 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 mobile node's home address is then supplied to higher protocol layers and applications.

Specifically:

- Construct the packet using the mobile node's home address as the packet's Source Address, in the same way as if the mobile node were at home. This includes the calculation of upper layer checksums using the home address as the value of the source.

- Insert a Home Address option into the packet, with the Home Address field copied from the original value of the Source Address field in the packet.

- Change the Source Address field in the packet's IPv6 header to one of the mobile node's care-of addresses. This will typically be the mobile node's current primary care-of address, but MUST be a care-of address with a subnet prefix that is on-link on the network interface on which the mobile node will transmit the packet.

By using the care-of address as the Source Address in the IPv6 header, with the mobile node's home address instead in the Home Address option, the packet will be able to safely pass through any router implementing ingress filtering [23].

reverse tunneling

This is the mechanism which tunnels the packets via the home agent. It isn't as efficient as the above mechanism, but is needed if there is no binding yet with the correspondent node. Specifically:

- The packet is sent to the home agent using IPv6 encapsulation [15].

- The Source Address in the tunnel packet is the primary care-of address as registered with the home agent.

- The Destination Address in the tunnel packet is the home agent's address.

Reverse tunneled packets MAY be protected using a AH or ESP header, depending on the security policies used by the home agent. The support for encrypted reverse tunneling allows mobile nodes to defeat certain kinds of traffic analysis, and provides a mechanism by which routers on the home network can distinguish authorized traffic from other possibly malicious traffic.

11.3.2. Interaction with Outbound IPsec Processing

This section sketches the interaction between outbound Mobile IPv6 processing and outbound IP Security (IPsec) processing for packets sent by a mobile node while away from home. Any specific implementation MAY use algorithms and data structures other than those suggested here, but its processing MUST be consistent with the effect of the operation described here and with the relevant IPsec specifications. In the steps described below, it is assumed that IPsec is being used in transport mode [4] and that the mobile node is using its home address as the source for the packet (from the point of view of higher protocol layers or applications, as described in Section 11.3.1):

- The packet is created by higher layer protocols and applications (e.g., by TCP) as if the mobile node were at home and Mobile IPv6 were not being used.

- As part of outbound packet processing in IP, the packet is compared against the IPsec security policy database to determine what processing is required for the packet [4].

- If IPsec processing is required, the packet is either mapped to an existing Security Association (or SA bundle), or a new SA (or SA bundle) is created for the packet, according to the procedures defined for IPsec.

- Since the mobile node is away from home, the mobile is either using reverse tunneling or route optimization to reach the correspondent node.

  If reverse tunneling is used, the packet is constructed in the normal manner and then tunneled through the home agent.

  If route optimization is in use, the mobile node inserts a Home Address destination option into the packet, replacing the Source Address in the packet's IP header with a care-of address suitable for the link on which the packet is being sent, as described in Section 11.3.1. The Destination Options header in which the Home Address destination option is inserted MUST appear in the packet after the routing header, if present, and before the IPsec (AH [5] or ESP [6]) header, so that the Home Address destination option is processed by the destination node before the IPsec header is processed.

  Finally, once the packet is fully assembled, the necessary IPsec authentication (and encryption, if required) processing is performed on the packet, initializing the Authentication Data in the IPsec header. The AH authentication data MUST be calculated as if the following were true:

  * the IPv6 source address in the IPv6 header contains the mobile node's home address,

  * the Home Address field of the Home Address destination option (Section 6.3) contains the new care-of address.

- This allows, but does not require, the receiver of the packet containing a Home Address destination option to exchange the two fields of the incoming packet, simplifying processing for all subsequent packet headers. However, such an exchange is not required, as long as the result of the authentication calculation remains the same.

When an automated key management protocol is used to create new security associations towards a peer, it is important to ensure that the peer can send the key management protocol packets to the mobile node. This may not be possible if the peer is the home agent of the mobile node, and the purpose of the security associations would be to send a Binding Update to the home agent. Packets addressed to the home address of the mobile node cannot be used before the Binding

Update has been processed. For the default case of using IKE as the automated key management protocol [9, 4], such problems can be avoided by the following requirements:

- When the mobile node is away from home, it MUST use its care-of address as the Source Address of all packets it sends as part of the key management protocol (without use of Mobile IPv6 for these packets, as suggested in Section 11.3.1).

- In addition, for all security associations bound to the mobile node's home address established by IKE, the mobile node MUST include an ISAKMP Identification Payload [8] in the IKE exchange, giving the mobile node's home address as the initiator of the Security Association [7].

11.3.3. Receiving Packets While Away from Home

While away from home, a mobile node will receive packets addressed to its home address, by one of three methods:

- Packets sent by a correspondent node that does not have a Binding Cache entry for the mobile node, will be tunneled to the mobile node via its home agent.

- Packets sent by a correspondent node that has a Binding Cache entry for the mobile node that contains the mobile node's current care-of address, will be sent by the correspondent node using a type 2 routing header. The packet will be addressed to the mobile node's care-of address, with the final hop in the routing header directing the packet to the mobile node's home address; the processing of this last hop of the routing header is entirely internal to the mobile node, since the care-of address and home address are both addresses within the mobile node.

For packets received by the first of these methods, the mobile node MUST check that the IPv6 source address of the tunneled packet is the IP address of its home agent.

For packets received by either the first or last of these three methods, the mobile node SHOULD send a Binding Update to the original sender of the packet, as described in Section 11.7.2, subject to the rate limiting defined in Section 11.8. The mobile node MUST also process the received packet in the manner defined for IPv6 encapsulation [15], which will result in the encapsulated (inner) packet being processed normally by upper-layer protocols within the mobile node, as if it had been addressed (only) to the mobile node's home address.

For packets received by the second method above (using a type 2 routing header), the following rules will result in the packet being processed normally by upper-layer protocols within the mobile node, as if it had been addressed to the mobile node's home address.

A node receiving a packet addressed to itself (i.e., one of the node's addresses is in the IPv6 destination field) follows the next header chain of headers and processes them. When it encounters a type 2 routing header during this processing it performs the following checks. If any of these checks fail the node MUST silently discard the packet.

- The length field in the routing header is exactly 2.

- The segments left field in the routing header is either 0 or 1. (Values on the wire are always 1. But implementations may process the routing header so that the value may become 0 after the routing header has been processed, but before the rest of the packet is processed.)

- The Home Address field in the routing header is one of the node's home addresses, if the segments left field was 1. Thus, in particular the address field is required to be a unicast routable address.

Once the above checks have been performed, the node swaps the IPv6 destination field with the Home Address field in the routing header, decrements segments left, and resubmits the packet to IP for processing the next header. Conceptually this follows the same model as in RFC 2460. However, in the case of type 2 routing header this can be simplified since it is known that the packet will not be forwarded to a different node.

The definition of AH requires the sender to calculate the AH integrity check value of a routing header in a way as it appears in the receiver after it has processed the header. Since IPsec headers follow the routing header, any IPsec processing will operate on the packet with the home address in the IP destination field and segments left being zero. Thus, the AH calculations at the sender and receiver will have an identical view of the packet.

11.3.4. Receiving ICMP Error Messages

Any node that doesn't recognize the Mobility header will return an ICMP Parameter Problem, Code 1, message to the sender of the packet. If the mobile node receives such an ICMP error message in response to a return routability procedure or Binding Update, it SHOULD record in its Binding Update List that future Binding Updates SHOULD NOT be sent to this destination.

Correspondent nodes who have participated in the return routability procedure MUST implement the ability to correctly process received packets containing a Home Address destination option. Therefore, correctly implemented correspondent nodes should always be able to recognize Home Address options. If a mobile node receives an ICMP Parameter Problem, Code 2, message from some node indicating that it does not support the Home Address option, the mobile node SHOULD log the error and then discard the ICMP message.

11.3.5. Routing Multicast Packets

A mobile node that is connected to its home link functions in the same way as any other (stationary) node. Thus, when it is at home, a mobile node functions identically to other multicast senders and receivers. This section therefore describes the behavior of a mobile node that is not on its home link.

In order to receive packets sent to some multicast group, a mobile node must join that multicast group. One method by which a mobile node MAY join the group is via a (local) multicast router on the foreign link being visited. The mobile node SHOULD use one of its care-of addresses that shares a subnet prefix with the multicast router, as the source IPv6 address of its multicast group membership control messages. The mobile node MUST NOT use the Home Address destination option when sending MLD packets [29]

Alternatively, a mobile node MAY join multicast groups via a bi-directional tunnel to its home agent. The mobile node tunnels its multicast group membership control packets to its home agent, and the home agent forwards multicast packets down the tunnel to the mobile node.

A mobile node that wishes to send packets to a multicast group also has two options:

1. Send directly on the foreign link being visited.

   The application is aware of the care-of address and uses it for multicast traffic just like any other stationary address. The mobile node MUST NOT use Home Address destination option in such traffic.

2. Send via a tunnel to its home agent.

   Because multicast routing in general depends upon the Source Address used in the IPv6 header of the multicast packet, a mobile node that tunnels a multicast packet to its home agent MUST use its home address as the IPv6 Source Address of the inner multicast packet.

Note that direct sending from the foreign link is only applicable while the mobile node is at that foreign link. This is because the associated multicast tree is specific to that source location and any change of location and source address will invalidate the source specific tree or branch and the application context of the other multicast group members.

This specification does not provide mechanisms to enable such local multicast session to survive hand-off, and to seamlessly continue from a new CCoA on each new foreign link. Any such mechanism, developed as an extension to this specification, needs to take into account the impact of fast moving mobile nodes on the Internet multicast routing protocols and their ability to maintain the integrity of source specific multicast trees and branches.

While the use of reverse tunnelling can ensure that multicast trees are independent of the mobile nodes movement, in some case such tunnelling can have adverse affects. The latency of specific types of multicast applications such as multicast based discovery protocols will be affected when the round-trip time between the foreign subnet and the home agent is significant compared to that of the topology to be discovered. In addition, the delivery tree from the home agent in such circumstances relies on unicast encapsulation from the agent to the mobile node and is therefore bandwidth inefficient compared to the native multicast forwarding in the foreign multicast system.

11.4. Home Agent and Prefix Management

11.4.1. Dynamic Home Agent Address Discovery

Sometimes, when the mobile node needs to send a Binding Update to its home agent to register its new primary care-of address, as described in Section 11.7.1, the mobile node may not know the address of any router on its home link that can serve as a home agent for it. For example, some nodes on its home link may have been reconfigured while the mobile node has been away from home, such that the router that was operating as the mobile node's home agent has been replaced by a different router serving this role.

In this case, the mobile node MAY attempt to discover the address of a suitable home agent on its home link. To do so, the mobile node sends an ICMP Home Agent Address Discovery Request message to the Mobile IPv6 Home-Agents anycast address [16] for its home subnet prefix. As described in Section 10.5, the home agent on its home link that receives this Request message will return an ICMP Home Agent Address Discovery Reply message, giving this home agent's own global unicast IP address along with a list of the global unicast IP address of each other home agent operating on the home link.

The mobile node, upon receiving this Home Agent Address Discovery

Reply message, MAY then send its home registration Binding Update to the home agent address given as the IP Source Address of the packet carrying the Reply message or to any of the unicast IP addresses listed in the Home Agent Addresses field in the Reply. For example, if necessary, the mobile node MAY attempt its home registration with each of these home agents, in turn, by sending each a Binding Update and waiting for the matching Binding Acknowledgement, until its registration is accepted by one of these home agents. The mobile node MUST, however, wait at least 1.5 times longer than (RetransTimer * DupAddrDetectTransmits) before sending a Binding Update to the next home agent. In trying each of the returned home agent addresses, the mobile node SHOULD try each in the order listed in the Home Agent Addresses field in the received Home Agent Address Discovery Reply message. If the home agent identified by the Source Address field in the IP header of the packet carrying the Home Agent Address Discovery Reply message is not listed in the Home Agent Addresses field in the Reply, it SHOULD be tried before the first address given in the list; otherwise, it SHOULD be tried in its listed order.

If the mobile node has a current registration with some home agent on its home link (the Lifetime for that registration has not yet expired), then the mobile node MUST attempt any new registration first with that home agent. If that registration attempt fails (e.g., times out or is rejected), the mobile node SHOULD then reattempt this registration with another home agent on its home link. If the mobile node knows of no other suitable home agent, then it MAY attempt the dynamic home agent address discovery mechanism described above.

If, after a mobile node transmits a Home Agent Address Discovery Request message to the Home Agents Anycast address, it does not receive a corresponding Home Agent Address Discovery Reply message within INITIAL_DHAAD_TIMEOUT (see Section 12) seconds, the mobile node MAY retransmit the same Request message to the same anycast address. This retransmission MAY be repeated up to a maximum of DHAAD_RETRIES (see Section 12) attempts. Each retransmission MUST be delayed by twice the time interval of the previous retransmission.

11.4.2. Sending Mobile Prefix Solicitations

When a mobile node has a home address that is about to become invalid, it sends a Mobile Prefix Solicitation to its home agent in an attempt to acquire fresh routing prefix information. The new information also enables the mobile node to participate in renumbering operations affecting the home network, as described in Section 10.6.

The mobile node MUST use the Home Address destination option to carry its home address and SHOULD use IPsec to protect the solicitation.

The mobile node SHOULD send a Solicitation to the home agent when its home address will become invalid within MaxRtrAdvInterval seconds, where this value is acquired in a previous Mobile Prefix Advertisement from the home agent. If no such value is known, the value MAX_PFX_ADV_DELAY seconds is used instead (see Section 12).

This solicitation follows the same retransmission rules specified for Router Solicitations [12], except that the initial retransmission interval is specified to be INITIAL_SOLICIT_TIMER (see Section 12).

As described in Section 11.7.2, Binding Updates sent by the mobile node to other nodes MUST use a lifetime no greater than the remaining lifetime of its home registration of its primary care-of address. The mobile node SHOULD further limit the lifetimes that it sends on any Binding Updates to be within the remaining valid lifetime (see Section 10.6.2) for the prefix in its home address.

When the lifetime for a changed prefix decreases, and the change would cause cached bindings at correspondent nodes in the Binding Update List to be stored past the newly shortened lifetime, the mobile node MUST issue a Binding Update to all such correspondent nodes.

These limits on the binding lifetime serve to prohibit use of a mobile node's home address after it becomes invalid.

11.4.3. Receiving Mobile Prefix Advertisements

Section 10.6 describes the operation of a home agent to support boot time configuration and renumbering a mobile node's home subnet while the mobile node is away from home. The home agent sends Mobile Prefix Advertisements to the mobile node while away from home, giving "important" Prefix Information options that describe changes in the prefixes in use on the mobile node's home link.

The Mobile Prefix Solicitation is similar to the Router Solicitation used in Neighbor Discovery [12], except it is routed from the mobile node on the visited network to the home agent on the home network by usual unicast routing rules.

When a mobile node receives a Mobile Prefix Advertisement, it MUST validate it according to the following test:

- The Source Address of the IP packet carrying the Mobile Prefix Advertisement is the same as the home agent address to which the mobile node last sent an accepted home registration Binding Update to register its primary care-of address. Otherwise, if no such registrations have been made, it SHOULD be the mobile node's stored home agent address, if one exists. Otherwise, if the mobile node has not yet discovered its home agent's address, it MUST NOT accept Mobile Prefix Advertisements.

- The packet MUST have a type 2 routing header and SHOULD be protected by an IPsec header as described in Sections 5.4 and 6.8.

Any received Mobile Prefix Advertisement not meeting this test MUST be silently discarded. For advertisements that do not contain the same ICMP Identifier value as in a recently sent solicitation, the mobile node MUST send a solicitation and expect an advertisement with a matching Identifier before further processing.

For an accepted Mobile Prefix Advertisement, the mobile node MUST process the Prefix Information Options as if they arrived in a Router Advertisement on the mobile node's home link [12]. Such processing may result in the mobile node configuring a new home address, although due to separation between preferred lifetime and valid lifetime, such changes should not affect most communication by the mobile node, in the same way as for nodes that are at home. In this case, the mobile node MUST return a Binding Update, which will be viewed by the home agent as an acknowledgement of the corresponding Mobile Prefix Advertisement, which it can cease transmitting. In addition, if the method used for this new home address configuration would require the mobile node to perform Duplicate Address Detection [13] for the new address if the mobile node were located at home, then the mobile node MUST set the Duplicate Address Detection (D) bit in this Binding Update to its home agent, to request the home agent to perform this Duplicate Address Detection on behalf of the mobile node.

11.5. Movement

11.5.1. Movement Detection

The primary movement detection mechanism for Mobile IPv6 defined in this section uses the facilities of IPv6 Neighbor Discovery, including Router Discovery and Neighbor Unreachability Detection. The mobile node SHOULD supplement this mechanism with other information whenever it is available to the mobile node (e.g., from lower protocol layers). The description here is based on the conceptual model of the organization and data structures defined by Neighbor Discovery [12].

Mobile nodes SHOULD use Router Discovery to discover new routers and on-link subnet prefixes; a mobile node MAY send Router Solicitations, or MAY wait for unsolicited (periodic) multicast Router Advertisements, as specified for Router Discovery [12]. Based on received Router Advertisements, a mobile node maintains an entry in its Default Router List for each router, and an entry in its

Prefix List for each subnet prefix that it currently considers to be on-link. Each entry in these lists has an associated invalidation timer value. While away from home, a mobile node typically selects one default router and one subnet prefix to use as the subnet prefix in its primary care-of address. A mobile node MAY also have associated additional care-of addresses, using other subnet prefixes from its Prefix List. The method by which a mobile node selects and forms a care-of address from the available subnet prefixes is described in Section 11.5.2. The mobile node registers its primary care-of address with its home agent, as described in Section 11.7.1.

While a mobile node is away from home, it is important for the mobile node to quickly detect when its default router becomes unreachable. When this happens, the mobile node SHOULD switch to a new default router and potentially to a new primary care-of address. If, on the other hand, the mobile node becomes unreachable from its default router, it should attempt to become reachable through some other router. To detect when its default router becomes unreachable, a mobile node SHOULD use Neighbor Unreachability Detection.

For a mobile node to detect when it has become unreachable from its default router, the mobile node cannot efficiently rely on Neighbor Unreachability Detection alone, since the network overhead would be prohibitively high in many cases. Instead, when a mobile node receives any IPv6 packets from its current default router at all, irrespective of the source IPv6 address, it SHOULD use that as an indication that it is still reachable from the router.

Since the router SHOULD be sending periodic unsolicited multicast Router Advertisements, the mobile node will have frequent opportunity to check if it is still reachable from its default router, even in the absence of other packets to it from the router. If Router Advertisements that the mobile node receives include an Advertisement Interval option, the mobile node MAY use its Advertisement Interval field as an indication of the frequency with which it SHOULD expect to continue to receive future Advertisements from that router. This field specifies the minimum rate (the maximum amount of time between successive Advertisements) that the mobile node SHOULD expect. If this amount of time elapses without the mobile node receiving any Advertisement from this router, the mobile node can be sure that at least one Advertisement sent by the router has been lost. It is thus possible for the mobile node to implement its own policy for determining the number of Advertisements from its current default router it is willing to tolerate losing before deciding to switch to a different router from which it may currently be correctly receiving Advertisements.

On some types of network interfaces, the mobile node MAY also supplement this monitoring of Router Advertisements, by setting its network interface into "promiscuous" receive mode, so that it is able to receive all packets on the link, including those not addressed to it at the link layer (i.e., disabling link-level address filtering). The mobile node will then be able to detect any packets sent by the router, in order to detect reachability from the router. This use of promiscuous mode may be useful on very low bandwidth (e.g., wireless) links, but its use MUST be configurable on the mobile node since it is likely to consume additional energy resources.

If the above means do not provide indication that the mobile node is still reachable from its current default router (for instance, the mobile node receives no packets from the router for a period of time), then the mobile node SHOULD attempt to actively probe the router with Neighbor Solicitations, even if it is not otherwise actively sending packets to the router. If it receives a solicited Neighbor Advertisement in response from the router, then the mobile node can deduce that it is still reachable. It is expected that the mobile node will in most cases be able to determine its reachability from the router by listening for packets from the router as described above, and thus, such extra Neighbor Solicitation probes should rarely be necessary.

With some types of networks, indications about link-layer mobility might be obtained from lower-layer protocol or device driver software within the mobile node. However, all link-layer mobility indications from lower layers do not necessarily indicate a movement of the mobile node to a new link, such that the mobile node would need to switch to a new default router and primary care-of address. For example, movement of a mobile node from one cell to another in many wireless LANs can be made transparent to the IP level through use of a link-layer "roaming" protocol, as long as the different wireless LAN cells all operate as part of the same IP link with the same subnet prefix. Upon lower-layer indication of link-layer mobility, the mobile node MAY send Router Solicitations to determine if additional on-link subnet prefixes are available on its new link.

Such lower-layer information might also be useful to a mobile node in deciding to switch its primary care-of address to one of the other care-of addresses it has formed from the on-link subnet prefixes currently available through different routers from which the mobile node is reachable. For example, a mobile node MAY use signal strength or signal quality information (with suitable hysteresis) for its link with the available routers to decide when to switch to a new primary care-of address using that router rather than its current default router (and current primary care-of address). Even though the mobile node's current default router may still be reachable in terms of Neighbor Unreachability Detection, the mobile node MAY use such lower-layer information to determine that switching to a new default router would provide a better connection.

11.5.2. Forming New Care-of Addresses

After detecting that it has moved from one link to another (i.e., its current default router has become unreachable and it has discovered a new default router), a mobile node SHOULD form a new primary care-of address using one of the on-link subnet prefixes advertised by the new router. A mobile node MAY form a new primary care-of address at any time, except that it MUST NOT do so too frequently. Specifically, a mobile node MUST NOT send a Binding Update about a new care-of address to its home agent (which is required to register the new address as its primary care-of address) more often than once per MAX_UPDATE_RATE seconds.

In addition, after discovering a new on-link subnet prefix, a mobile node MAY form a new (non-primary) care-of address using that subnet prefix, even when it has not switched to a new default router. A mobile node can have only one primary care-of address at a time (which is registered with its home agent), but it MAY have an additional care-of address for any or all of the prefixes on its current link. Furthermore, since a wireless network interface may actually allow a mobile node to be reachable on more than one link at a time (i.e., within wireless transmitter range of routers on more than one separate link), a mobile node MAY have care-of addresses on more than one link at a time. The use of more than one care-of address at a time is described in Section 11.5.3.

As described in Section 4, in order to form a new care-of address, a mobile node MAY use either stateless [13] or stateful (e.g., DHCPv6 [30]) Address Autoconfiguration. If a mobile node needs to send packets as part of the method of address autoconfiguration, it MUST use an IPv6 link-local address rather than its own IPv6 home address as the Source Address in the IPv6 header of each such autoconfiguration packet.

In some cases, a mobile node may already know a (constant) IPv6 address that has been assigned to it for its use only while visiting a specific foreign link. For example, a mobile node may be statically configured with an IPv6 address assigned by the system administrator of some foreign link, for its use while visiting that link. If so, rather than using Address Autoconfiguration to form a new care-of address using this subnet prefix, the mobile node MAY use its own pre-assigned address as its care-of address on this link.

A mobile node, after forming a new care-of address, MAY begin using the new care-of address without performing Duplicate Address Detection. Furthermore, the mobile node MAY continue using the address without performing Duplicate Address Detection, although it SHOULD in most cases. begin Duplicate Address Detection asynchronously when it begins use of the address. This allows the Duplicate Address Detection procedure to complete in parallel with normal communication using the address, avoiding major delays for some applications.

In addition, normal processing for Duplicate Address Detection specifies that, in certain cases, the node SHOULD delay sending the initial Neighbor Solicitation message of Duplicate Address Detection by a random delay between 0 and MAX_RTR_SOLICITATION_DELAY [12, 13]; however, in this case, the mobile node SHOULD NOT perform such a delay in its use of Duplicate Address Detection, unless the mobile node is initializing after rebooting.

11.5.3. Using Multiple Care-of Addresses

As described in Section 11.5.2, a mobile node MAY use more than one care-of address at a time. Particularly in the case of many wireless networks, a mobile node effectively might be reachable through multiple links at the same time (e.g., with overlapping wireless cells), on which different on-link subnet prefixes may exist. A mobile node SHOULD select a primary care-of address from among those care-of addresses it has formed using any of these subnet prefixes, based on the movement detection mechanism in use, as described in Section 11.5.1. After selecting a new primary care-of address, the mobile node MUST send a Binding Update containing that care-of address to its home agent. The Binding Update MUST have the Home Registration (H) and Acknowledge (A) bits set its home agent, as described on Section 11.7.1.

To assist with smooth handovers, a mobile node SHOULD retain its previous primary care-of address as a (non-primary) care-of address, and SHOULD still accept packets at this address, even after registering its new primary care-of address with its home agent. This is reasonable, since the mobile node could only receive packets at its previous primary care-of address if it were indeed still connected to that link. If the previous primary care-of address was allocated using stateful Address Autoconfiguration [30], the mobile node may not wish to release the address immediately upon switching to a new primary care-of address.

11.5.4. Returning Home

A mobile node detects that it has returned to its home link through the movement detection algorithm in use (Section 11.5.1), when the mobile node detects that its home subnet prefix is again on-link. The mobile node SHOULD then send a Binding Update to its home agent, to instruct its home agent to no longer intercept or tunnel packets for it. In this home registration, the mobile node MUST set the Acknowledge (A) and Home Registration (H) bits, set the Lifetime field to zero, and set the care-of address for the binding to the mobile node's own home address. The mobile node MUST use its home address as the source address in the Binding Update.

When sending this Binding Update to its home agent, the mobile node must be careful in how it uses Neighbor Solicitation [12] (if needed) to learn the home agent's link-layer address, since the home agent will be currently configured to defend the mobile node's home address for Duplicate Address Detection (DAD). In particular, a Neighbor Solicitation from the mobile node using its home address as the Source Address would be detected by the home agent as a duplicate address. In many cases, Neighbor Solicitation by the mobile node for the home agent's address will not be necessary, since the mobile node may have already learned the home agent's link-layer address, for example from a Source Link-Layer Address option in the Router Advertisement from which it learned that its home address was on-link and that the mobile node had thus returned home.

If the mobile node does Neighbor Solicitation to learn the home agent's link-layer address, in this special case of the mobile node returning home, the mobile node MUST multicast the packet, and in addition set the Source Address of this Neighbor Solicitation to the unspecified address (0:0:0:0:0:0:0:0). The target of the Neighbor Solicitation MUST be set to the home agent's IPv6 address, which is known to the mobile node. The destination IP address MUST be set to the Solicited-Node multicast address [3]. The home agent will be unable to distinguish this solicitation from a similar packet that would only be used for DAD, and it will respond as if for DAD. The home agent will send a multicast Neighbor Advertisement back to the mobile node with the Solicited flag (S) set to zero. The mobile node SHOULD accept this advertisement, and set the state of the Neighbor Cache entry for the home agent to REACHABLE.

The mobile node then sends its Binding Update using the home agent's link-layer address, instructing its home agent to no longer serve as a home agent for it. By processing this Binding Update, the home agent will cease defending the mobile node's home address for Duplicate Address Detection and will no longer respond to Neighbor Solicitations for the mobile node's home address. The mobile node is then the only node on the link receiving packets at the mobile node's home address. In addition, when returning home prior to the expiration of a current binding for its home address, and configuring its home address on its network interface on its home link, the mobile node MUST NOT perform Duplicate Address Detection on its own home address, in order to avoid confusion or conflict with its home agent's use of the same address. If the mobile node returns home after the bindings for all of its care-of addresses have expired, then it SHOULD perform DAD. It SHOULD also perform DAD for addresses which may have been registered with 'D' and 'S' bits set to one.

After the Mobile Node sends the Binding Update, the Home Agent MUST remove the Proxy Neighbor Cache entry for the Mobile Node and MAY learn its link-layer address based on the link-layer packet or cached information, or if that is not available, it SHOULD send a Neighbor Solicitation with the target address equal to the Binding Update's source IP address. The Mobile Node MUST then reply with a unicast

Neighbor Advertisement to the Home Agent with its link-layer address. While the Mobile Node is waiting for a Binding Acknowledgement, it MUST NOT respond to any Neighbor Solicitations for its Home Address other than those originating from the IP address to which it sent the Binding Update.

After receiving the Binding Acknowledgement for its Binding Update to its home agent, the mobile node MUST multicast onto the home link (to the all-nodes multicast address) a Neighbor Advertisement [12], to advertise the mobile node's own link-layer address for its own home address. The Target Address in this Neighbor Advertisement MUST be set to the mobile node's home address, and the Advertisement MUST include a Target Link-layer Address option specifying the mobile node's link-layer address. The mobile node MUST multicast such a Neighbor Advertisement for each of its home addresses, as defined by the current on-link prefixes, including its link-local address and site-local address. The Solicited Flag (S) in these Advertisements MUST NOT be set, since they were not solicited by any Neighbor Solicitation. The Override Flag (O) in these Advertisements MUST be set, indicating that the Advertisements SHOULD override any existing Neighbor Cache entries at any node receiving them.

Since multicasting on the local link (such as Ethernet) is typically not guaranteed to be reliable, the mobile node MAY retransmit these Neighbor Advertisements up to MAX_ADVERT_REXMIT times to increase their reliability. It is still possible that some nodes on the home link will not receive any of these Neighbor Advertisements, but these nodes will eventually be able to recover through use of Neighbor Unreachability Detection [12].

11.6. Return Routability Procedure

This section defines the rules that the mobile node must follow when performing the return routability procedure. Section 11.7.2 describes the rules when the return routability procedure needs to be initiated.

11.6.1. Sending Home and Care-of Test Init Messages

A mobile node that initiates a return routability procedure MUST send (in parallel) a Home Test Init message and a Care-of Test Init messages. However, if the mobile node has recently received one or both home or care-of keygen tokens, and associated nonce indices for the desired addresses, it MAY reuse them. Therefore, the return routability procedure may in some cases be completed with only one message pair. It may even be completed without any messages at all, if the mobile node has a recent home keygen token and and has previously visited the same care-of address so that it also has a recent care-of keygen token. If the mobile node sets the Lifetime to zero or the care-of address in the Binding Update equal to its home address - such as when returning home - it MUST use the home keygen token and nonce index by itself (without a care-of keygen token and nonce index). In this case, generation of the binding management key depends exclusively on the home keygen token (Section 5.2.5).

A Home Test Init message MUST be created as described in Section 6.1.3. A Care-of Test Init message MUST be created as described in Section 6.1.4. When sending a Home Test Init or Care-of Test Init message the mobile node MUST record in its Binding Update List the following fields from the messages:

- The IP address of the node to which the message was sent.

- The home address of the mobile node. This value will appear in the Source Address field of the Home Test Init message. When sending the Care-of Test Init message, this address does not appear in the message, but represents the home address for which the binding is desired.

- The time at which each of these messages was sent.

- The cookies used in the messages.

Note that a single Care-of Test Init message may be sufficient even when there are multiple home addresses. In this case the mobile node MAY record the same information in multiple Binding List entries.

11.6.2. Receiving Return Routability Messages

Upon receiving a packet carrying a Home Test message, a mobile node MUST validate the packet according to the following tests:

- The Header Len field in the Mobility Header is greater than or equal to the length specified in Section 6.1.5.

- The Source Address of the packet belongs to a correspondent node for which the mobile node has a Binding Update List entry with a state indicating that return routability procedure is in progress. Note that there may be multiple such entries.

- The Binding Update List indicates that no home keygen token has been received yet.

- The Destination Address of the packet has the home address of the mobile node, and the packet has been received in a tunnel from the home agent.

- The home init cookie field in the message matches the value stored in the Binding Update List.

Any Home Test message not satisfying all of these tests MUST be silently ignored. Otherwise, the mobile node MUST record the Home

Nonce Index and home keygen token in the Binding Update List. If the Binding Update List entry does not have a care-of keygen token, the mobile node SHOULD continue waiting for additional messages.

Upon receiving a packet carrying a Care-of Test message, a mobile node MUST validate the packet according to the following tests:

- The Header Len field in the Mobility Header is greater than or equal to the length specified in Section 6.1.6.

- The Source Address of the packet belongs to a correspondent node for which the mobile node has a Binding Update List entry with a state indicating that return routability procedure is in progress. Note that there may be multiple such entries.

- The Binding Update List indicates that no care-of keygen token has been received yet.

- The Destination Address of the packet is the current care-of address of the mobile node.

- The care-of init cookie field in the message matches the value stored in the Binding Update List.

Any Care-of Test message not satisfying all of these tests MUST be silently ignored. Otherwise, the mobile node MUST record the Care-of Nonce Index and care-of keygen token in the Binding Update List. If the Binding Update List entry does not have a home keygen token, the mobile node SHOULD continue waiting for additional messages.

If after receiving either the Home Test or the Care-of Test message and performing the above actions, the Binding Update List entry has both the home and the care-of keygen tokens, the return routability procedure is complete. The mobile node SHOULD then proceed with sending a Binding Update as described in Section 11.7.2.

Correspondent nodes from the time before this specification was published may not support the Mobility Header protocol. These nodes will respond to Home Test Init and Care-of Test Init messages with an ICMP Parameter Problem code 1. The mobile node SHOULD take such messages as an indication that the correspondent node cannot provide route optimization, and revert back to the use of bidirectional tunneling.

11.6.3. Protecting Return Routability Packets

The mobile node MUST support the protection of Home Test and Home Test Init messages as described in Section 10.4.4.

11.7. Processing Bindings

11.7.1. Sending Binding Updates to the Home Agent

After deciding to change its primary care-of address as described in Sections 11.5.1 and 11.5.2, a mobile node MUST register this care-of address with its home agent in order to make this its primary care-of address. Also, if the mobile node wants the services of the home agent beyond the current registration period, the mobile node MUST send a new Binding Update to it well before the expiration of this period, even if it is not changing its primary care-of address.

In both of these situations, the mobile node sends a packet to its home agent containing a Binding Update, with the packet constructed as follows:

- The Home Registration (H) bit MUST be set in the Binding Update.

- The Acknowledge (A) bit MUST be set in the Binding Update.

- The packet MUST contain a Home Address destination option, giving the mobile node's home address for the binding.

- The care-of address for the binding MUST be used as the Source Address in the packet's IPv6 header, unless an Alternate Care-of Address mobility option is included in the Binding Update. This option MAY be included when the mobile node so desires, and MUST be included if the mobile node cannot be assured that the IPsec AH protocol is used to secure the Binding Update. The ESP protocol will not be able to protect care-of addresses in the IPv6 header. Mobile IPv6 implementations which are unaware of how IPsec secures their messaging will therefore need to use the Alternate Care-of Address option.

- The Single Address Only (S) bit is cleared to request a binding for all home addresses of the mobile node. These addresses are based on the interface identifier of the home address indicated in the Binding Update, and all on-link subnet prefixes on the home link. When this bit is cleared, the Link-Local Address Compatibility (L) bit MUST be set.

  If the mobile node desires that only a single home address should be affected by this Binding Update, the Single Address Only (S) bit is set to 1.

  The value of the Single Address Only (S) bit MUST be set equivalently for subsequent de-registrations and re-registrations with the same addresses.

- If the mobile node's link-local address has the same interface identifier as the home address for which it is supplying a new care-of address, then the mobile node SHOULD set the Link-Local Address Compatibility (L) bit.

- If the home address was generated using RFC 3041 [17], then the link local address is unlikely to have a compatible interface identifier. In this case, the mobile node MUST set the Single Address Only (S) bit and clear the Link-Local Address Compatibility (L) bit.

- The value specified in the Lifetime field SHOULD be less than or equal to the remaining lifetime of the home address and the care-of address specified for the binding.

The Acknowledge (A) bit in the Binding Update requests the home agent to return a Binding Acknowledgement in response to this Binding Update. As described in Section 6.1.8, the mobile node SHOULD retransmit this Binding Update to its home agent until it receives a matching Binding Acknowledgement. Once reaching a retransmission timeout period of MAX_BINDACK_TIMEOUT, the mobile node SHOULD restart the process of delivering the Binding Update, but trying instead the next home agent returned during dynamic home agent address discovery (see Section 11.4.1). If there was only one home agent, the mobile node instead SHOULD continue to periodically retransmit the Binding Update at this rate until acknowledged (or until it begins attempting to register a different primary care-of address). See Section 11.8 for information about retransmitting Binding Updates.

Depending on the value of the Single Address Only (S) bit in the Binding Update, the home agent is requested to serve either a single home address or all home addresses for the mobile node. Until the lifetime of this registration expires, the home agent considers itself the home agent for each such home address of the mobile node. As the set of on-link subnet prefixes on the home link changes over time, the home agent changes the set of home addresses for this mobile node for which it is serving as the home agent.

Each Binding Update MUST be authenticated as coming from the right mobile node, as defined in Section 5.1. The mobile node MUST use its home address - either in the Home Address destination option or in the Source Address field of the IPv6 header - in Binding Updates sent to the home agent. This is necessary in order to allow the IPsec policies to be matched with the right home address.

When sending a Binding Update to its home agent, the mobile node MUST also create or update the corresponding Binding Update List entry, as specified in Section 11.7.2.

The last Sequence Number value sent to the home agent in a Binding

Update is stored by the mobile node. If the sending mobile node has no knowledge of the right Sequence Number value, it may start at any value. If the home agent rejects the value, it sends back a Binding

Acknowledgement with status code 135, and the last accepted sequence number in the Sequence Number field of the Binding Acknowledgement. The mobile node MUST store this information and use the next Sequence Number value for the next Binding Update it sends.

If the mobile node has additional home addresses using a different interface identifier, then the mobile node SHOULD send an additional packet containing a Binding Update to its home agent to register the care-of address for each such other home address (or set of home addresses sharing an interface identifier).

While the mobile node is away from home, it relies on the home agent to participate in Duplicate Address Detection (DAD) to defend its home address against stateless autoconfiguration performed by another node. Therefore, the mobile node SHOULD set the Duplicate Address Detection (D) bit based on any requirements for DAD that would apply to the mobile node if it were at home [12, 13]. If the mobile node's recent Binding Update was accepted by the home agent, and the lifetime for that Binding Update has not yet expired, the mobile node SHOULD NOT set the Duplicate Address Detection (D) bit in the new Binding Update; the home agent will already be defending the home address(es) of the mobile node and does not need to perform DAD again.

The home agent will only perform DAD for the mobile node's home address when the mobile node has supplied a valid binding between its home address and a care-of address. If some time elapses during which the mobile node has no binding at the home agent, it might be possible for another node to autoconfigure the mobile node's home address. Therefore, the mobile node MUST treat creation of a new binding with the home agent using an existing home address the same as creation of a new home address. In the unlikely event that the mobile node's home address is autoconfigured as the IPv6 address of another network node on the home network, the home agent will reply to the mobile node's subsequent Binding Update with a Binding Acknowledgement containing a Status of 134 (Duplicate Address Detection failed). In this case, the mobile node MUST NOT attempt to re-use the same home address. It SHOULD continue to register care-of addresses for its other home addresses, if any. The mobile node MAY also attempt to acquire a new home address to replace the one for which Status 134 was received, for instance by using the techniques described in Appendix B.5.

11.7.2. Correspondent Binding Procedure

When the mobile node is assured that its home address is valid, it MAY at any time initiate a correspondent binding procedure with the purpose of allowing the correspondent node to cache the mobile node's current care-of address. The mobile node is responsible for the initiation and completion of this procedure, as well as any retransmissions that may be needed (subject to the rate limiting defined in Section 11.8).

This section defines the rules that the mobile node must follow when performing the correspondent binding procedure.

The mobile node can be assured that its home address is still valid, for example, by the home agent's use the Duplicate Address Detection (D) bit of Binding Updates (see Section 10.3.1). In any Binding Update sent by a mobile node, the care-of address (either the Source Address in the packet's IPv6 header or the Care-of Address in the Alternate Care-of Address mobility option of the Binding Update) MUST be set to one of the care-of addresses currently in use by the mobile node or to the mobile node's home address. A mobile node MAY set the care-of address differently for sending Binding Updates to different correspondent nodes.

A mobile node MAY choose to keep its location private from certain correspondent nodes, and thus need not initiate the return routability procedure, or send new Binding Updates to those correspondents. A mobile node MAY also send a Binding Update to such a correspondent node to instruct it to delete any existing binding for the mobile node from its Binding Cache, as described in Section 6.1.7. However, all Binding Updates to the correspondent node require the successful completion of the return routability procedure first, as no other IPv6 nodes are authorized to send Binding Updates on behalf of a mobile node.

If set to one of the mobile node's current care-of addresses (the care-of address given MAY differ from the mobile node's primary care-of address), the Binding Update requests the correspondent node to create or update an entry for the mobile node in the correspondent node's Binding Cache in order to record this care-of address for use in sending future packets to the mobile node. In this case, the value specified in the Lifetime field sent in the Binding Update SHOULD be less than or equal to the remaining lifetime of the home address and the care-of address specified for the binding.

If the care-of address is set to the mobile node's home address or the Lifetime field set to zero, the Binding Update requests the correspondent node to delete any existing Binding Cache entry that it has for the mobile node. In this case, generation of the binding management key depends exclusively on the home keygen token (Section 5.2.5). The care-of nonce index SHOULD be set to zero in this case. In keeping with the Binding Update creation rules below, the care-of address MUST be set to the home address if the mobile node is at home, or to the current care-of address if it is away from home.

After the mobile node has sent a Binding Update to its home agent to register a new primary care-of address (as described in

Section 11.7.1), the mobile node SHOULD send a Binding Update to each other node for which an entry exists in the mobile node's Binding Update List, as detailed below. Typically this requires starting a return routability procedure. Upon successful return routability procedure and after receiving a successful Binding Acknowledgement from the Home Agent, a Binding Update is sent to all other nodes. Thus, other relevant nodes are generally kept updated about the mobile node's binding and can send packets directly to the mobile node using the mobile node's current care-of address.

The mobile node, however, need not initiate these actions immediately after configuring a new care-of address. For example, the mobile node MAY delay initiating the return routability procedure to any correspondent node for a short period of time, if it isn't certain that there is any significant traffic to the correspondent node.

In addition, when a mobile node receives a packet for which the mobile node can deduce that the original sender of the packet either has no Binding Cache entry for the mobile node, or a stale entry for the mobile node in its Binding Cache, the mobile node SHOULD initiate a return routability procedure with the sender, in order to finally update the sender's Binding Cache with the current care-of address (subject to the rate limiting defined in Section 11.8). In particular, the mobile node SHOULD initiate a return routability procedure in response to receiving a packet that meets all of the following tests:

- The packet was tunneled using IPv6 encapsulation.

- The Destination Address in the tunnel (outer) IPv6 header is equal to any of the mobile node's care-of addresses.

- The Destination Address in the original (inner) IPv6 header is equal to one of the mobile node's home addresses.

- The Source Address in the tunnel (outer) IPv6 header differs from the Source Address in the original (inner) IPv6 header.

The destination address to which the procedure should be initiated to in response to receiving a packet meeting all of the above tests is the Source Address in the original (inner) IPv6 header of the packet. The home address for which this Binding Update is sent should be the Destination Address of the original (inner) packet.

If the mobile node wants to ensure that its new care-of address has been entered into a correspondent node's Binding Cache, the mobile node MAY request an acknowledgement by setting the Acknowledge (A) bit in the Binding Update. In this case, however, the mobile node SHOULD NOT continue to retransmit the Binding Update once the retransmission timeout period has reached MAX_BINDACK_TIMEOUT.

The mobile node SHOULD create a Binding Update as follows:

- The Source Address of the IPv6 header MUST contain the current care-of address of the mobile node.

- The Destination Address of the IPv6 header MUST contain the address of the correspondent node.

- The Mobility Header is constructed according to rules in Section 6.1.7 and 5.2.6, including the Binding Authorization Data (calculated as defined in Section 6.2.6) and possibly the Nonce Indices mobility options.

- The home address of the mobile node MUST be added to the packet in a Home Address destination option, unless the Source Address is the home address.

Each Binding Update MUST 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, as described in Section 9.5.1. There is no requirement, however, that the Sequence Number value strictly increase by 1 with each new Binding Update sent or received, as long as the value stays within the window. The last Sequence Number value sent to a destination in a Binding Update is stored by the mobile node in its Binding Update List entry for that destination. If the sending mobile node has no Binding Update List entry, the Sequence Number SHOULD start at a random value. The mobile node MUST NOT use the same Sequence Number in two different Binding Updates to the same correspondent node, even if the Binding Updates provide different care-of addresses.

11.7.3. Receiving Binding Acknowledgements

Upon receiving a packet carrying a Binding Acknowledgement, a mobile node MUST validate the packet according to the following tests:

- The packet meets the authentication requirements for Binding Acknowledgements, defined in Sections 6.1.8 and 5. That is, if the Binding Update was sent to the home agent, underlying IPsec protection is used. If the Binding Update was sent to the correspondent node, the Binding Authorization Data mobility option MUST be present and have a valid value.

- The Binding Authorization Data mobility option, if present, MUST be the last option and MUST not have trailing padding.

- The Header Len field in the Binding Acknowledgement is greater than or equal to the length specified in Section 6.1.8.

- The Sequence Number field matches the Sequence Number sent by the mobile node to this destination address in an outstanding Binding Update.

Any Binding Acknowledgement not satisfying all of these tests MUST be silently ignored.

When a mobile node receives a packet carrying a valid Binding Acknowledgement, the mobile node MUST examine the Status field as follows:

- If the Status field indicates that the Binding Update was accepted (the Status field is less than 128), then the mobile node MUST update the corresponding entry in its Binding Update List to indicate that the Binding Update has been acknowledged; the mobile node MUST then stop retransmitting the Binding Update. In addition, if the value specified in the Lifetime field in the Binding Acknowledgement is less than the Lifetime value sent in the Binding Update being acknowledged, then the mobile node MUST subtract the difference between these two Lifetime values from the remaining lifetime for the binding as maintained in the corresponding Binding Update List entry (with a minimum value for the Binding Update List entry lifetime of 0). That is, if the Lifetime value sent in the Binding Update was L_update, the Lifetime value received in the Binding Acknowledgement was L_ack, and the current remaining lifetime of the Binding Update List entry is L_remain, then the new value for the remaining lifetime of the Binding Update List entry should be

  ```
  max((L_remain - (L_update - L_ack)), 0)
  ```

  where max(X, Y) is the maximum of X and Y. The effect of this step is to correctly manage the mobile node's view of the binding's remaining lifetime (as maintained in the corresponding Binding Update List entry) so that it correctly counts down from the Lifetime value given in the Binding Acknowledgement, but with the timer countdown beginning at the time that the Binding Update was sent.

  Mobile nodes SHOULD send a new Binding Update well before the expiration of this period in order to extend the lifetime. This helps to avoid disruptions in communications, which might otherwise be caused by network delays or clock drift.

- If the Status field indicates that the Binding Update was rejected (the Status field is greater than or equal to 128), then the mobile node MUST delete the corresponding Binding Update List entry, and it MUST also stop retransmitting the Binding Update.

Optionally, the mobile node MAY then take steps to correct the cause of the error and retransmit the Binding Update (with a new

Sequence Number value), subject to the rate limiting restriction specified in Section 11.8.

The treatment of a Binding Refresh Advice mobility option within the Binding Acknowledgement depends on the where the acknowledgement came from. This option MUST be ignored if the acknowledgement came from a correspondent node. If it came from the home agent, the mobile node uses Refresh Interval field in the option as a suggestion that it SHOULD attempt to refresh its home registration at the indicated shorter interval.

11.7.4. Receiving Binding Refresh Requests

When a mobile node receives a packet containing a Binding Refresh Request message and there already exists a Binding Update List entry for the source of the Binding Refresh Request, it MAY start a return routability procedure. The mobile node MAY also choose to either ignore the Binding Refresh Request or to delete its binding from the sender of the Binding Refresh Request. Note that the mobile node SHOULD NOT respond Binding Refresh Requests from previously unknown correspondent nodes due to Denial-of-Service concerns.

If the return routability procedure completes successfully, a Binding Update message SHOULD be sent as described in Section 11.7.2. The Lifetime field in this Binding Update SHOULD be set to a new lifetime, extending any current lifetime remaining from a previous Binding Update sent to this node (as indicated in any existing Binding Update List entry for this node), and lifetime SHOULD again be less than or equal to the remaining lifetime of the home registration and the care-of address specified for the binding. When sending this Binding Update, the mobile node MUST update its Binding Update List in the same way as for any other Binding Update sent by the mobile node.

Instead, if the mobile node chooses to delete its binding from the sender of the Binding Refresh Request, the mobile node SHOULD return a Binding Update to the sender with the Lifetime specified as zero and specify a Care-of Address that matches the home address for the binding.

11.7.5. Receiving Binding Error Messages

When a mobile node receives a packet containing a Binding Error message, it should first check if the mobile node has a Binding Update List entry for the source of the Binding Error message. If the mobile node does not have such entry, it MUST ignore the message. This is necessary to prevent a waste of resources on e.g. return routability procedure due to spoofed Binding Error messages.

Otherwise, if the message Status field was 1 (unknown binding for Home Address destination option), the mobile node should perform one of the following two actions:

- If the mobile node does have a Binding Update List entry but has recent upper layer progress information that indicates communications with the correspondent node are progressing, it MAY ignore the message. This can be done in order to limit the damage that spoofed Binding Error messages can cause to ongoing communications.

- If the mobile node does have a Binding Update List entry but no upper layer progress information, it MUST remove the entry and route further communications through the home agent. It MAY also optionally start a return routability procedure (see Section 5.2).

If the message Status field was 2 (unrecognized MH Type value), the mobile node should perform one of the following two actions:

- If the mobile node is not expecting an acknowledgement or response from the correspondent node, the mobile node SHOULD ignore this message.

- Otherwise, the mobile node SHOULD cease the use of any extensions to this specification. If no extensions had been used, the mobile node should cease the attempt to use route optimization.

11.8. Retransmissions and Rate Limiting

The mobile node is responsible for retransmissions and rate limiting in the return routability and binding procedures.

When the mobile node sends a Home Test Init, Care-of Test Init or Binding Update for which it expects a response, the mobile node has to determine a value for the initial retransmission timer:

- If the mobile node is sending a Binding Update and it does not have an existing binding at the home agent, it SHOULD use a value for the initial retransmission timer that is at least 1.5 times longer than (RetransTimer * DupAddrDetectTransmits). This value is likely to be substantially longer than the otherwise specified value of INITIAL_BINDACK_TIMEOUT (see Section 12) that would be used by the mobile node. This longer retransmission interval will allow the home agent to complete the DAD procedure which is mandated in this case, as detailed in Section 11.7.1.

- Otherwise, the mobile node should use the specified value of

INITIAL_BINDACK_TIMEOUT for the initial retransmission timer.

If the mobile node fails to receive a valid, matching response within the selected initial retransmission interval, the mobile node SHOULD retransmit the message, until a response is received.

The retransmissions by the mobile node MUST use an exponential back-off process, in which the timeout period is doubled upon each retransmission until either the node receives a response or the timeout period reaches the value MAX_BINDACK_TIMEOUT. The mobile node MAY continue to send these messages at this slower rate indefinitely.

The mobile node SHOULD start a separate back-off process for different message types, different home addresses and different care-of addresses. However, in addition an overall rate limitation applies for messages sent to a particular correspondent node. This ensures that the correspondent node has sufficient amount of time to answer when bindings for multiple home addresses are registered, for instance. The mobile node MUST NOT send Mobility Header messages of a particular type to a particular correspondent node more often than once per MAX_UPDATE_RATE seconds.

Retransmitted Binding Updates MUST use a Sequence Number value greater than that used for the previous transmission of this Binding Update. Retransmitted Home Test Init and Care-of Test Init messages MUST use new cookie values.

12. Protocol Constants

HomeRtrAdvInterval	3,600 seconds
DHAAD_RETRIES	3 retransmissions
INITIAL_BINDACK_TIMEOUT	1 second
INITIAL_DHAAD_TIMEOUT	2 seconds
INITIAL_SOLICIT_TIMER	2 seconds
MAX_ADVERT_REXMIT	3 transmissions
MAX_BINDACK_TIMEOUT	256 seconds
MaxMobPfxAdvInterval	86,400 seconds
MAX_NONCE_LIFE	240 seconds
MAX_TOKEN_LIFE	210 seconds
MAX_RR_BINDING_LIFE	420 seconds
MAX_UPDATE_RATE	once per second
MinDelayBetweenRAs	0.05 seconds
MinMobPfxAdvInterval	600 seconds
PREFIX_ADV_RETRIES	3 retransmissions
PREFIX_ADV_TIMEOUT	5 seconds
SLOW_UPDATE_RATE	once per 10 second interval

The value MinDelayBetweenRAs overrides the value of the protocol constant MIN_DELAY_BETWEEN_RAS, as specified in RFC 2461 [12].

13. IANA Considerations

This document defines a new IPv6 protocol, the Mobility Header, described in Section 6.1. This protocol must be assigned a protocol number. The MH Type field in the Mobility Header is used to indicate a particular type of a message. The current message types are described in Sections 6.1.2 through 6.1.9, and include the following:

0	Binding Refresh Request
1	Home Test Init
2	Care-of Test Init
3	Home Test
4	Care-of Test
5	Binding Update
6	Binding Acknowledgement
7	Binding Error

Future values of the MH Type can be allocated using standards action [10].

Furthermore, each mobility message may contain mobility options as described in Section 6.2. The current mobility options are defined in Sections 6.2.2 through 6.2.7, and include the following:

0	Pad1
1	PadN
3	Alternate Care-of Address
4	Nonce Indices
5	Authorization Data
6	Binding Refresh Advice

Future values of the Option Type can be allocated using standards action [10].

This document also defines a new IPv6 destination option, the Home Address option, described in Section 6.3. This option must be assigned an Option Type value.

This document also defines a new IPv6 type 2 routing header, described in Section 6.4. The value 2 is to be allocated by IANA when this specification becomes an RFC.

In addition, this document defines four ICMP message types, two used as part of the dynamic home agent address discovery mechanism and two used in lieu of Router Solicitations and Advertisements when the mobile node is away from the home link:

- The Home Agent Address Discovery Request message, described in Section 6.5;

- The Home Agent Address Discovery Reply message, described in Section 6.6;

- The Mobile Prefix Solicitation, described in Section 6.7; and

- The Mobile Prefix Advertisement, described in Section 6.8.

This document also defines two new Neighbor Discovery [12] options, which must be assigned Option Type values within the option numbering space for Neighbor Discovery messages:

- The Advertisement Interval option, described in Section 7.3; and

- The Home Agent Information option, described in Section 7.4.

14. Security Considerations

14.1. Threats

Any mobility solution must protect itself against misuses of the mobility features and mechanisms. In Mobile IPv6, most of the potential threats are concerned with false Bindings, usually resulting in Denial-of-Service attacks. Some of the threats also pose potential for Man-in-the-Middle, Hijacking, Confidentiality, and Impersonation attacks. The main threats this protocol protects against are the following:

1. Threats involving Binding Updates sent to home agents and correspondent nodes. For instance, an attacker might claim that a certain mobile node is currently at a different location than it really is. If a home agent accepts such spoofed information sent to it, the mobile node might not get traffic destined to it. Similarly, a malicious (mobile) node might use the home address of a victim node in a forged Binding Update sent to a correspondent node.

These pose threats against confidentiality, integrity, and
availability. That is, an attacker might learn the contents

of packets destined to another node by redirecting the traffic to itself. Furthermore, an attacker might use the redirected packets in an attempt to set itself as a Man-in-the-Middle between a mobile and a correspondent node. This would allow the attacker to impersonate the mobile node, leading to integrity and availability problems.

A malicious (mobile) node might also send Binding Updates in which the care-of address is set to the address of a victim node. If such Binding Updates were accepted, the malicious node could lure the correspondent node into sending potentially large amounts of data to the victim; the correspondent node's replies to messages sent by the malicious mobile node will be sent to the victim host or network. This could be used to cause a Distributed Denial-of-Service attack. For example, the correspondent node might be a site that will send a high-bandwidth stream of video to anyone who asks for it. Note that the use of flow-control protocols such as TCP does not necessarily defend against this type of attack, because the attacker can fake the acknowledgements. Even keeping TCP initial sequence numbers secret doesn't help, because the attacker can receive the first few segments (including the ISN) at its own address, and only then redirect the stream to the victim's address. These types of attacks may also be directed towards networks instead of nodes. Further variations of this threat are described elsewhere [31, 32].

An attacker might also attempt to disrupt a mobile node's communications by replaying a Binding Update that the node had sent earlier. If the old Binding Update was accepted, packets destined for the mobile node would be sent to its old location and not its current location.

In conclusion, there are Denial-of-Service, Man-in-the-Middle, Confidentiality, and Impersonation threats against the parties involved in sending legitimate Binding Updates, and Denial-of-Service threats against any other party.

2. Threats associated with payload packets: Payload packets exchanged with mobile nodes are exposed to similar threats as regular IPv6 traffic is. However, Mobile IPv6 introduces the Home Address destination option, a new routing header type (type 2), and uses tunneling headers in the payload packets. The protocol must protect against potential new threats involving the use of these mechanisms.

   Third parties become exposed to a reflection threat via the Home Address destination option, unless appropriate security precautions are followed. The Home Address destination option could be used to direct response traffic toward a node whose IP address appears in the option. In this case, ingress filtering would not catch the forged "return address" [33] [34].

A similar threat exists with the tunnels between the mobile node and the home agent. An attacker might forge tunnel packets between the mobile node and the home agent, making it appear that the traffic is coming from the mobile node when it is not. Note that an attacker who is able to forge tunnel packets would typically be able forge also packets that appear to come directly from the mobile node. This is a not a new threat as such. However, it may make it easier for attackers to escape detection by avoiding ingress filtering and packet tracing mechanisms. Furthermore, spoofed tunnel packets might be used to gain access to the home network.

Finally, a routing header could also be used in reflection attacks, and in attacks designed to bypass firewalls. The generality of the regular routing header would allow circumvention of IP-address based rules in firewalls. It would also allow reflection of traffic to other nodes. These threats exist with routing headers in general, even if the usage that Mobile IPv6 requires is safe.

3. Threats associated with dynamic home agent and prefix discovery.

4. Threats against the Mobile IPv6 security mechanisms themselves: An attacker might, for instance, lure the participants into executing expensive cryptographic operations or allocating memory for the purpose of keeping state. The victim node would have no resources left to handle other tasks.

As a fundamental service in an IPv6 stack, Mobile IPv6 is expected to be deployed in most nodes of the IPv6 Internet. The above threats should therefore be considered in the light of being applicable to the whole Internet.

14.2. Features

This specification provides a number of security features designed to mitigate or alleviate the threats listed above. The main security features are the following:

- Reverse Tunneling as a mandatory feature.

- Protection of Binding Updates sent to home agents.

- Protection of Binding Updates sent to correspondent nodes.

- Protection against reflection attacks that use the Home Address destination option.

- Protection of tunnels between the mobile node and the home agent.

- Closing routing header vulnerabilities.

- Mitigating Denial-of-Service threats to the Mobile IPv6 security mechanisms themselves.

The support for encrypted reverse tunneling (see Section 11.3.1) allows mobile nodes to defeat certain kinds of traffic analysis.

Protecting those Binding Updates that are sent to home agents and those that are sent to arbitrary correspondent nodes requires very different security solutions due to the different situations. Mobile nodes and home agents are expected to be naturally subject to the network administration of the home domain.

Thus, they can and are supposed to have a strong security association that can be used to reliably authenticate the exchanged messages. See Section 5.1 for the description of the protocol mechanisms, and Section 14.3 below for a discussion of the resulting level of security.

It is expected that Mobile IPv6 route optimization will be used on a global basis between nodes belonging to different administrative domains. It would be a very demanding task to build an authentication infrastructure on this scale. Furthermore, a traditional authentication infrastructure cannot be easily used to authenticate IP addresses, because these change often. It is not sufficient to just authenticate the mobile nodes. Authorization to claim the right to use an address is needed as well. Thus, an "infrastructureless" approach is necessary. The chosen infrastructureless method is described in Section 5.2 and Section 14.4 discusses the resulting security level and the design rationale of this approach.

Specific rules guide the use of the Home Address destination option, the routing header, and the tunneling headers in the payload packets. These rules are necessary to remove the vulnerabilities associated with their unrestricted use. The effect of the rules is discussed in Sections 14.7, 14.8, and 14.9.

Denial-of-Service threats against Mobile IPv6 security mechanisms themselves concern mainly the Binding Update procedures with correspondent nodes. The protocol has been designed to limit the effects of such attacks, as will be described in Section 14.4.5.

14.3. Binding Updates to Home Agent

Signaling between the mobile node and the home agent requires message integrity, correct ordering and replay protection. This is necessary to assure the home agent that a Binding Update is from a legitimate mobile node.

IPsec AH or ESP protects the integrity of the Binding Updates and Binding Acknowledgements, by securing mobility messages between the mobile node and the home agent. For ESP, a non-null authentication algorithm MUST be applied.

However, IPsec can easily provide replay protection only if dynamic security association establishment is used. This may not always be possible, and manual keying would be preferred in some cases. IPsec also does not guarantee correct ordering of packets, only that they have not been replayed. Because of this, sequence numbers with the Mobile IPv6 messages ensure correct ordering (see Section 5.1). However, if a home agent reboots and loses its state regarding the sequence numbers, replay attacks become possible. he use of a key management mechanism together with IPsec can be used to prevent such replay attacks.

A sliding window scheme is used for the sequence numbers. The protection against replays and reordering attacks without a key management mechanism works when the attacker remembers up to a maximum of 2**15 Binding Updates.

The above mechanisms do not show that the care-of address given in the Binding Update is correct. This opens the possibility for Denial-of-Service attacks against third parties. However, since the mobile node and home agent have a security association, the home agent can always identify an ill-behaving mobile node. This allows the home agent operator to discontinue the mobile node's service, and possibly take further actions based on the business relationship with the mobile node's owner.

Note that where forwarding from a previous care-of address is used, a router in the visited network must act as a temporary home agent for the mobile node. Nevertheless, the same security requirements apply in this case. That is, a pre-arranged security association must exist even with the temporary home agent. This limits the use of the forwarding feature to those networks where such arrangements are practical.

Note that the use of a single pair of manually keyed security associations conflicts with the generation of a new home addresses [17] for the mobile node, or with the adoption of a new home prefix. This is because IPsec SAs are bound to the used addresses. While certificate-based automatic keying alleviates this problem to an extent, it is still necessary to ensure that a given mobile node cannot send Binding Updates for the address of another mobile node. In general, this leads to the inclusion of home addresses in certificates in the Subject AltName field. This again limits the introduction of new addresses without either manual or automatic procedures to establish new certificates. Therefore, this specification limits restricts the generation of new home addresses (for any reason) to those situations where there already exists a security association or certificate for the new address. (Section B.4 lists the improvement of security for new addresses as one of the future developments for Mobile IPv6.)

14.4. Binding Updates to Correspondent Nodes

14.4.1. Overview

The motivation for designing the return routability procedure was to have sufficient support for Mobile IPv6, without creating significant new security problems. The goal for this procedure was not to protect against attacks that were already possible before the introduction of Mobile IPv6.

The chosen infrastructureless method verifies that the mobile node is "live" (that is, it responds to probes) at its home and care-of addresses. Section 5.2 describes the return routability procedure in detail. The procedure uses the following principles:

- A message exchange verifies that the mobile node is reachable at its addresses i.e. is at least able to transmit and receive traffic at both the home and care-of addresses.

- The eventual Binding Update is cryptographically bound to the tokens supplied in the exchanged messages.

- Symmetric exchanges are employed to avoid the use of this protocol in reflection attacks. In a symmetric exchange, the responses are always sent to the same address as the request was sent from.

- The correspondent node operates in a stateless manner until it receives a fully authorized Binding Update.

- Some additional protection is provided by encrypting the tunnels between the mobile node and home agent with IPsec ESP. As the tunnel transports also the nonce exchanges, this limits the ability of attackers to see these nonces. For instance, this prevents attacks launched from the mobile node's current foreign link where no link-layer confidentiality is available.

For further information about the design rationale of the return routability procedure, see [31, 32, 35, 34]. The used mechanisms have been adopted from these documents.

14.4.2. Offered Protection

This procedure protects Binding Updates against all attackers who are unable to monitor the path between the home agent and the correspondent node. The procedure does not defend against attackers who can monitor this path. Note that such attackers are in any case able to mount an active attack against the mobile node when it is at its home location. The possibility of such attacks is not an impediment to the deployment of Mobile IPv6, because these attacks are possible regardless of whether Mobile IPv6 is in use.

This procedure also protects against Denial-of-Service attacks in which the attacker pretends to be a mobile, but uses the victim's address as the care of address. This would cause the correspondent node to send the victim some unexpected traffic. The procedure defends against these attacks by requiring at least passive presence of the attacker at the care-of address or on the path from the correspondent to the care of address. Normally, this will be the mobile node.

The Binding Acknowledgement is not authenticated in other ways than including the right sequence number in the reply.

14.4.3. Comparison to Regular IPv6 Communications

This section discusses the protection offered by the return routability method by comparing it to the security of regular IPv6 communications. We will divide vulnerabilities in three classes: (1) those related to attackers on the local network of the mobile node, home agent, or the correspondent node, (2) those related to attackers on the path between the home network and the correspondent node, and (3) off-path attackers, i.e. the rest of the Internet.

We will now discuss the vulnerabilities of regular IPv6 communications. The on-link vulnerabilities of IPv6 communications include Denial-of-Service, Masquerading, Man-in-the-Middle, Eavesdropping, and other attacks. These attacks can be launched through spoofing Router Discovery, Neighbor Discovery and other IPv6 mechanisms. Some of these attacks can be prevented with the use of cryptographic protection in the packets.

A similar situation exists with on-path attackers. That is, without cryptographic protection the traffic is completely vulnerable.

Assuming that attackers have not penetrated the security of the Internet routing protocols, attacks are much harder to launch from off-path locations. Attacks that can be launched from these locations are mainly Denial-of-Service attacks, such as flooding and/or reflection attacks. It is not possible for an off-path attacker to become a MitM. (Since IPv6 communications are relatively well protected against off-path attackers, it is important that Mobile IPv6 prevents off-path attacks as well.)

Next, we will consider the vulnerabilities that exist when IPv6 is used together with Mobile IPv6 and the return routability procedure. On the local link the vulnerabilities are same as those as in IPv6, but Masquerade and MitM attacks can now be launched also against future communications, and not just against current communications. If a Binding Update was sent while the attacker was present on the link, its effects stay during the lifetime of the binding. This happens even if the attacker moves away from the link. In regular IPv6, the attacker generally has to be stay on the link in order to continue the attack. Note that in order to launch these new attacks, the IP address of the victim must be known. This makes this attack feasible mainly in the context of well-known interface IDs, such as those already appearing in the traffic on the link or registered in the DNS.

On-path attackers can exploit similar vulnerabilities as in regular IPv6. There are some minor differences, however. Masquerade, MitM, and DoS attacks can be launched with just the interception of a few packets, whereas in regular IPv6 it is necessary to intercept every packet. The effect of the attacks is the same regardless of the method, however. In any case, the most difficult task attacker faces in these attacks is getting to the right path.

The vulnerabilities for off-path attackers are the same as in regular IPv6. Those nodes that are not on the path between the home agent and the correspondent node will not be able to receive the probe messages.

In conclusion, we can state the following main results from this comparison:

- Return routability procedure prevents any off-path attacks beyond those that are already possible in regular IPv6. This is the most important result, and prevents attackers from the Internet from exploiting any vulnerabilities.

- Vulnerabilities to attackers on the home agent link, the correspondent node link, and the path between them are roughly the same as in regular IPv6.

- However, one difference is that in basic IPv6 an on-path attacker must be constantly present on the link or the path, whereas with Mobile IPv6 an attacker can leave a binding behind after moving away.

  For this reason, this specification limits the creation of bindings to at most MAX_TOKEN_LIFE seconds after the last routability check has been performed, and limits the duration of a binding to at most MAX_RR_BINDING_LIFE seconds. With these limitation, attackers cannot take practical advantages of this vulnerability. This limited vulnerability can also be compared to similar vulnerabilities in IPv6 Neighbor Discovery, with Neighbor Cache entries having a limited lifetime.

- There are some other minor differences, such as an effect to the DoS vulnerabilities. These can be considered to be insignificant.

- The path between the home agent and a correspondent node is typically easiest to attack on the links at either end, in particular if these links are publicly accessible wireless LANs. Attacks against the routers or switches on the path are typically harder to accomplish. The security on layer 2 of the links plays then a major role in the resulting overall network security. Similarly, security of IPv6 Neighbor and Router Discovery on these links has a large impact. If these were secured using some new technology in the future, this could make the return routability procedure the easiest route for attackers. For this reason, this specification should have a protection mechanism for selecting between return routability and potential other future mechanisms.

For a more in-depth discussion of these issues, see [34].

14.4.4. Return Routability Replays

The return routability procedure also protects the participants against replayed Binding Updates. The attacker is unable replay the same message due to the sequence number which is a part of the Binding Update. It is also unable to modify the Binding Update since the MAC would not verify after such modification.

Care must be taken when removing bindings at the correspondent node, however. If a binding is removed while the nonce used in its creation is still valid, an attacker could replay the old Binding Update. Rules outlined in Section 5.2.8 ensure that this cannot happen.

14.4.5. Return Routability Denial-of-Service

The return routability procedure has protection against resource exhaustion Denial-of-Service attacks. The correspondent nodes do not retain any state about individual mobile nodes until an authentic Binding Update arrives. This is achieved through the construct of keygen tokens from the nonces and node keys that are not specific to individual mobile nodes. The keygen tokens can be reconstructed by the correspondent node, based on the home and care-of address information that arrives with the Binding Update. This means that the correspondent nodes are safe against memory exhaustion attacks except where on-path attackers are concerned. Due to the use of symmetric cryptography, the correspondent nodes are relatively safe against CPU resource exhaustion attacks as well.

Nevertheless, as [31] describes, there are situations in which it is impossible for the mobile and correspondent nodes to determine if they actually need a binding or whether they just have been fooled into believing so by an attacker. Therefore, it is necessary to consider situations where such attacks are being made.

Even if route optimization is a very important optimization, it is still only an optimization. A mobile node can communicate with a correspondent node even if the correspondent refuses to accept any Binding Updates. However, performance will suffer because packets from the correspondent node to the mobile node will be routed via the mobile's home agent rather than a more direct route. A correspondent node can protect itself against some of these resource exhaustion attacks as follows. If the correspondent node is flooded with a large number of Binding Updates that fail the cryptographic integrity checks, it can stop processing Binding Updates. If a correspondent node finds that it is spending more resources on checking bogus Binding Updates than it is likely to save by accepting genuine Binding Updates, then it may silently discard some or all Binding Updates without performing any cryptographic operations.

Layers above IP can usually provide additional information to decide if there is a need to establish a binding with a specific peer. For example, TCP knows if the node has a queue of data that it is trying to send to a peer. An implementation of this specification is not required to make use of information from higher protocol layers, but some implementations are likely to be able to manage resources more effectively by making use of such information.

We also require that all implementations MUST allow route optimization to be administratively enabled or disabled. The default SHOULD be enabled.

14.5. Dynamic Home Agent Address Discovery

The dynamic home agent address discovery function could be used to learn the addresses of home agents in the home network. Attackers will not be able to learn much from this information, however, and mobile nodes cannot be tricked into using wrong home agents as all other communication with the home agents is secure.

14.6. Prefix Discovery

The prefix discovery function may leak interesting information about network topology and prefix lifetimes to eavesdroppers, and for this reason requests for this information have to be authenticated. Responses and unsolicited prefix information needs to be authenticated to prevent the mobile nodes from being tricked into believing false information about the prefixes, and possibly preventing communications with the existing addresses. Optionally, encryption may be applied to prevent leakage of the prefix information.

14.7. Tunneling via the Home Agent

Tunnels between the mobile node and the home agent can be protected by ensuring proper use of source addresses, and optional cryptographic protection. These procedures are discussed in Section 5.5.

Binding Updates to the home agents are secure. When receiving tunneled traffic the home agent verifies the outer IP address corresponds to the current location of the mobile node. This prevents attacks where the attacker is controlled by ingress filtering. It also prevents attacks when the attacker does not know the current care-of address of the mobile node. Attackers who know the care-of address and are not controlled by ingress filtering could still send traffic through the home agent. This includes attackers on the same local link as the mobile node is currently on. But such attackers could also send spoofed packets without using a tunnel.

Home agents and mobile nodes may use IPsec AH or ESP to protect payload packets tunneled between themselves. This is useful to protect communications against attackers on the path of the tunnel.

When site local home address are used, reverse tunneling can be used to send site local traffic from another location. Administrators should be aware of this when allowing such home addresses. In particular, the outer IP address check described above is not sufficient against all attackers. The use of encrypted tunnels is particularly useful for this kind of home addresses.

14.8. Home Address Option

When the mobile node sends packets directly to the correspondent node, the Source Address field of the packet's IPv6 header is the care-of address. Ingress filtering [23] works therefore in the usual manner even for mobile nodes, as the Source Address is topologically correct. The Home Address option is used to inform the correspondent node of the mobile node's home address.

However, the care-of address in the Source Address field does not survive in replies sent by the correspondent node unless it has a binding for this mobile node. Also, not all attacker tracing mechanisms work when packets are being reflected through correspondent nodes using the Home Address option. For these reasons, this specification restricts the use of the Home Address option. It may only used when a binding has already been established with the participation of the node at the home address, as described in Sections 5.5 and 6.3. This prevents reflection attacks through the use of the Home Address option. It also ensures that the correspondent nodes reply to the same address as the mobile node sends traffic from.

No special authentication of the Home Address option is required beyond the above, except that if the IPv6 header of a packet is covered by authentication, then that authentication MUST also cover the Home Address option; this coverage is achieved automatically by the definition of the Option Type code for the Home Address option (Section 6.3), since it indicates that the option is included in the authentication computation. Thus, even when authentication is used in the IPv6 header, the security of the Source Address field in the IPv6 header is not compromised by the presence of a Home Address option. Without authentication of the packet, then any field in the IPv6 header, including the Source Address field, and any other parts of the packet, including the Home Address option, can be forged or modified in transit. In this case, the contents of the Home Address option is no more suspect than any other part of the packet.

14.9. Type 2 Routing Header

The definition of the type 2 routing header is described in Section 6.4. This definition and the associated processing rules have been chosen so that the header cannot be used for what is traditionally viewed as source routing. In particular, the Home Address in the routing header will always have to be assigned to the home address of the receiving node. Otherwise the packet will be dropped.

Generally, source routing has a number of security concerns. These include the automatic reversal of unauthenticated source routes (which is an issue for IPv4, but not for IPv6). Another concern is the ability to use source routing to "jump" between nodes inside, as well as outside a firewall. These security concerns are not issues in Mobile IPv6, due to the rules mentioned above.

In essence the semantics of the type 2 routing header is the same as a special form of IP-in-IP tunneling where the inner and outer source addresses are the same.

This implies that a device which implements filtering of packets should be able to distinguish between a type 2 routing header and other routing headers, as required in Section 8.3. This is necessary in order to allow Mobile IPv6 traffic while still having the option to filter out other uses of routing headers.

Contributors

Tuomas Aura, Mike Roe, Greg O'Shea (Microsoft), Pekka Nikander (Ericsson), Erik Nordmark (Sun Microsystems), and Michael Thomas (Cisco) worked on the return routability protocols which eventually led to the procedures used in this protocol. The procedures described in [32] were adopted in the protocol.

Significant contributions were made by members of the Mobile IPv6 Security Design Team, including (in alphabetical order) Gabriel Montenegro, Erik Nordmark (Sun Microsystems) and Pekka Nikander (Ericsson), who have contributed volumes of text to this specification.

Acknowledgements

We would like to thank the members of the Mobile IP and IPng Working Groups for their comments and suggestions on this work. We would particularly like to thank (in alphabetical order) Fred Baker (Cisco), Josh Broch (Carnegie Mellon University), Samita Chakrabarti (Sun Microsystems), Robert Chalmers (University of California, Santa Barbara), Noel Chiappa (MIT), Vijay Devarapalli (Nokia Research Center), Rich Draves (Microsoft Research), Francis Dupont (ENST Bretagne), Thomas Eklund (Xelerated), Jun-Ichiro Itojun Hagino (IIJ Research Laboratory), Brian Haley (Compaq), John Ioannidis (AT & T Labs Research), James Kempf (DoCoMo), Rajeev Koodli (Nokia), Krishna Kumar (IBM Research), T.J. Kniveton (Nokia Research), Joe Lau (HP), Jiwoong Lee (KTF), Aime Le Rouzic (Bull S.A.), Vesa-Matti Mantyla (Ericsson), Kevin Miles (Cisco), Glenn Morrow (Nortel Networks), Thomas Narten (IBM), Karen Nielsen (Ericsson Telebit), Simon Nybroe (Ericsson Telebit), David Oran (Cisco), Brett Pentland (Monash University), Lars Henrik Petander (HUT), Basavaraj Patil (Nokia), Mohan Parthasarathy (Tahoe Networks), Alexandru Petrescu (Motorola), Mattias Petterson (Ericsson), Ken Powell (HP), Phil Roberts (Megisto), Patrice Romand (Bull S.A.), Jeff Schiller (MIT), Pekka Savola (Netcore), Arvind Sevalkar (Intinfotech), Keiichi Shima (IIJ Research Laboratory), Tom Soderlund (Nokia Research), Hesham Soliman (Ericsson), Jim Solomon (RedBack Networks), Tapio Suihko (Technical Research Center of Finland), Dave Thaler (Microsoft), Benny Van Houdt (University of Antwerp), Jon-Olov Vatn (KTH), Vladislav Yasevich

(HP), Alper Yegin (DoCoMo), and Xinhua Zhao (Stanford University) for their detailed reviews of earlier versions of this document. Their suggestions have helped to improve both the design and presentation of the protocol.

We would also like to thank the participants in the Mobile IPv6 testing event held at Nancy, France, September 15-17, 1999, for their valuable feedback as a result of interoperability testing of four Mobile IPv6 implementations coming from four different organizations: Bull, Ericsson Research and Ericsson Telebit, NEC, and INRIA. Further, we would like to thank the feedback from the implementors who participated in the Mobile IPv6 interoperability testing at Connectathons 2000, 2001, and 2002 in San Jose, California. Similarly, we would like to thank the participants at the ETSI interoperability testing at ETSI, in Sophia Antipolis, France, during October 2-6, 2000, including teams from Compaq, Ericsson, INRIA, Nokia, and Technical University of Helsinki.

References

[1] D. Eastlake, 3rd, S. Crocker, and J. Schiller. Randomness Recommendations for Security. Request for Comments (Informational) 1750, Internet Engineering Task Force, December 1994.

[2] S. Bradner. Key words for use in RFCs to Indicate Requirement Levels. Request for Comments (Best Current Practice) 2119, Internet Engineering Task Force, March 1997.

[3] R. Hinden and S. Deering. IP Version 6 Addressing Architecture. Request for Comments (Proposed Standard) 2373, Internet Engineering Task Force, July 1998.

[4] S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. Request for Comments (Proposed Standard) 2401, Internet Engineering Task Force, November 1998.

[5] S. Kent and R. Atkinson. IP Authentication Header. Request for Comments (Proposed Standard) 2402, Internet Engineering Task Force, November 1998.

[6] S. Kent and R. Atkinson. IP Encapsulating Security Payload (ESP). Request for Comments (Proposed Standard) 2406, Internet Engineering Task Force, November 1998.

[7] D. Piper. The Internet IP Security Domain of Interpretation for ISAKMP. Request for Comments (Proposed Standard) 2407, Internet Engineering Task Force, November 1998.

[8] D. Maughan, M. Schertler, M. Schneider, and J. Turner. Internet Security Association and Key Management Protocol (ISAKMP). Request for Comments (Proposed Standard) 2408, Internet Engineering Task Force, November 1998.

[9] D. Harkins and D. Carrel. The Internet Key Exchange (IKE). Request for Comments (Proposed Standard) 2409, Internet Engineering Task Force, November 1998.

[10] T. Narten and H. Alvestrand. Guidelines for Writing an IANA Considerations Section in RFCs. Request for Comments (Best Current Practice) 2434, Internet Engineering Task Force, October 1998.

[11] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. Request for Comments (Draft Standard) 2460, Internet Engineering Task Force, December 1998.

[12] T. Narten, E. Nordmark, and W. Simpson. Neighbor Discovery for IP Version 6 (IPv6). Request for Comments (Draft Standard) 2461, Internet Engineering Task Force, December 1998.

[13] S. Thomson and T. Narten. IPv6 Stateless Address Autoconfiguration. Request for Comments (Draft Standard) 2462, Internet Engineering Task Force, December 1998.

[14] A. Conta and S. Deering. Internet Control Message Protocol (ICMPv6) for the Internet Protocol version 6 (IPv6) specification. Request for Comments (Draft Standard) 2463, Internet Engineering Task Force, December 1998.

[15] A. Conta and S. Deering. Generic Packet Tunneling in IPv6 Specification. Request for Comments (Proposed Standard) 2473, Internet Engineering Task Force, December 1998.

[16] D. Johnson and S. Deering. Reserved IPv6 Subnet Anycast Addresses. Request for Comments (Proposed Standard) 2526, Internet Engineering Task Force, March 1999.

[17] T. Narten and R. Draves. Privacy Extensions for Stateless Address Autoconfiguration in IPv6. Request for Comments (Proposed Standard) 3041, Internet Engineering Task Force, January 2001.

[18] Editor J. Reynolds. Assigned Numbers: RFC 1700 is Replaced by an On-line Database. Request for Comments (Informational) 3232, Internet Engineering Task Force, January 2002.

[19] National Institute of Standards and Technology. Secure hash standard. Technical Report NIST FIPS PUB 180-1, U.S. Department of Commerce, April 1995.

[20] C. Perkins. IP Mobility Support. Request for Comments (Proposed Standard) 2002, Internet Engineering Task Force, October 1996.

[21] C. Perkins. IP Encapsulation within IP. Request for Comments (Proposed Standard) 2003, Internet Engineering Task Force, October 1996.

[22] C. Perkins. Minimal Encapsulation within IP. Request for Comments (Proposed Standard) 2004, Internet Engineering Task Force, October 1996.

[23] P. Ferguson and D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP source address spoofing. Request for Comments (Informational) 2267, Internet

Engineering Task Force, January 1998.

[24] Jari Arkko, Vijay Devarapalli, and Francis Dupont. Using IPsec to Protect Mobile IPv6 signaling between Mobile Nodes and Home Agents (work in progress). Internet Draft, Internet Engineering Task Force, October 2002.

[25] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-Hashing for Message Authentication. Request for Comments (Informational) 2104, Internet Engineering Task Force, February 1997.

[26] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. Request for Comments (Proposed Standard) 1883, Internet Engineering Task Force, December 1995.

[27] P. V. Mockapetris. Domain names - concepts and facilities. Request for Comments (Standard) 1034, Internet Engineering Task Force, November 1987.

[28] P. V. Mockapetris. Domain names - implementation and specification. Request for Comments (Standard) 1035, Internet Engineering Task Force, November 1987.

[29] S. Deering, W. Fenner, and B. Haberman. Multicast Listener Discovery (MLD) for IPv6. Request for Comments (Proposed Standard) 2710, Internet Engineering Task Force, October 1999.

[30] J. Bound, C. Perkins, M. Carney, and R. Droms. Dynamic Host Configuration Protocol for IPv6 (DHCPv6) (work in progress). Internet Draft, Internet Engineering Task Force, January 2001.

[31] Tuomas Aura and Jari Arkko. MIPv6 BU Attacks and Defenses (work in progress). Internet Draft, Internet Engineering Task Force, February 2002.

[32] Michael Roe, Greg O'Shea, Tuomas Aura, and Jari Arkko. Authentication of Mobile IPv6 Binding Updates and Acknowledgments (work in progress). Internet Draft, Internet Engineering Task Force, February 2002.

[33] Pekka Savola. Security of IPv6 Routing Header and Home Address Options (work in progress). Internet Draft, Internet Engineering Task Force, November 2001.

[34] Erik Nordmark, Gabriel Montenegro, Pekka Nikander, and Jari Arkko. Mobile IPv6 Security Design Rationale (work in progress). Internet Draft, Internet Engineering Task Force, 2002.

[35] Erik Nordmark. Securing MIPv6 BUs using Return Routability

(BU3WAY) (work in progress). Internet Draft, Internet
Engineering Task Force, November 2001.

References [1] through [19] are normative and others are informative.

A. Changes from Previous Version of the Draft

This appendix briefly lists some of the major changes in this draft relative to the previous version of this same draft, draft-ietf-mobileip-ipv6-18.txt:

A.1. Changes from Draft Version 18

- The draft no longer requires Home Address option and Binding Error support from all nodes. Similarly, we no longer support Home Address options protected solely using IPsec (tracked issues 53 and 54).

- Dynamic home agent address advertisement optimizations for excluding the sender's own address have been aligned with the priority mechanism (tracked issue 56).

- Units for Binding Update and Acknowledgement lifetimes have been aligned, and Status code values are now consistent across the document (tracked issue 58, 91).

- The ability to use link-local and site-local care-of addresses, home agent addresses, and home addresses has been clarified (tracked issues 62 and 94).

- Clarified the kind of multicast support provided in the base Mobile IPv6 specification (tracked issue 63).

- Inconsistencies on using routing headers and Binding Acknowledgment have been removed (tracked issue 65).

- Semantics for de-registration with the Single Address Only (S) bit have been specified (tracked issue 66).

- More exact rules for how to use IPsec between the mobile node and home agent have been provided in this draft as well as in a separate informative draft (tracked issue 69).

- Rules for when the Alternate Care-of Address mobility option is needed have been clarified (tracked issue 70).

- Forwarding from previous care-of address has be deprecated (tracked issue 72).

- New values for MaxRtAdvInterval have been provided (tracked issue

73).

- The rules on how care-of address can be used for some communications have been clarified (tracked issue 74)

- State machine description has been removed and only the normative text remains (tracked issue 76).

- Rules for processing Mobility Header messages have been clarified (tracked issue 77).

- Rules on how to not use Home Address destination option in Neighbor Discovery packets have been introduced (tracked issue 78).

- Behavior after an address collision has been specified (tracked issue 79).

- There are no longer specific rules for re-starting return routability procedure after a Binding Refresh Request has been received (tracked issue 82).

- It is no longer required to clear the contents of the Binding Cache upon reboot (tracked issue 83).

- Rules for filling the Home Address field within the Binding Error message have been clarified (tracked issue 85).

- Binding Acknowledgement length and padding values have been corrected (tracked issue 87).

- MIN_DELAY_BETWEEN_RAS has been redefined (tracked issue 88).

- The MH Type field has been shortened to 8 bits and MH Length no longer includes the first 8 bytes (tracked issues 89 and 93).

- It has been clarified that the Home Address option may be used within the Mobility Header checksum calculation. Also Mobility Header is considered as an upper layer protocol for the purposes of checksum calculation (tracked issues 90 and 111).

- Reflection attacks using Binding Acknowledgements have been prevented (tracked issue 92).

- References to routing headers indicate the type (tracked issue 95).

- The rules for when new nonces are needed have been clarified, as has the rules for (re-)using keygen tokens (tracked issues 96, 103).

- Binding Refresh Advice type number has been corrected (tracked issue 97).

- Keygen tokens are now produced with a different formula for home and care-of tokens (tracked issue 98).

- Binding Acknowledgements with Status code 136-138 are no longer authenticated (tracked issue 99).

- New requirements have been placed to Section 8.

- The coverage of the Authenticator has been clarified (tracked issue 106).

- Rules for registering home bindings with the Link-Local Address Compatibility (L) bit have been improved (tracked issue 108).

- Type 0 routing headers has been specified as orthogonal to type 2 usage (tracked issue 109).

- The inclusion of nonce indices has been made mandatory when return routability is the authorization method for correspondent bindings (tracked issue 113).

- Invalid Home and Care-of Test Init messages have to be silently discarded (tracked issue 114).

- The Binding Authorization Data mobility option is required to be the last one (tracked issue 115).

- The use of zero lifetime and home addresses in de-registration and Binding in Refresh Request responses has been clarified (tracked issue 116).

- Home keygen tokens are now sufficient for de-registration (tracked issue 117).

- A new Status code has been added to signal the expiry of both nonces (tracked issue 118).

- Kbm length has been changed to 20 bytes (tracked issue 119).

- Unique Identifier mobility option has been removed (tracked issue 121).

- The security mechanisms and requirements for dynamic home agent address and prefix discovery have been included (tracked issues 123 and 124).

- Processing order for route headers has been corrected (tracked issue 125).

- Rate-limiting and retransmission procedures have been combined and simplified (tracked issues 126 and 136).

- The allowed start time for return routability procedure has been specified (tracked issue 127).

- Rules for regenerating nonces and Kcn have been changed to accommodate situations where these values have not been used at all (tracked issue 131).

- The correspondent node's address which is used in Binding Authorization Data calculation has been specified to take in account Home Address destination option (tracked issue 133).

- The matching rules for Home and Care-of Test messages against sent Init messages have been specified (tracked issue 138).

- Rules for when Home Address destination option may appear in Binding Updates have been changed and made consistent (tracked issue 139).

- Authenticator calculation shall precede checksum calculation (tracked issue 140).

- Rules for sending Binding Acknowledgement errors have been made consistent (tracked issue 142).

- Invalid authenticator and route optimization not desired Status values have been removed, and values higher than these have been renumbered (tracked issues 100).

- The acknowledgement for Mobile Prefix Advertisements is now Mobile Prefix Solicitation, and not a Binding Update (tracked issue 144).

- Multiple tries to different home agents are now timed in a manner that does not cause problems for Duplicate Address Detection (tracked issue 145).

- Correspondent node binding updates can be secured with also pre-configured binding management key in addition to return routability (tracked issue 146).

- Router Advertisement and prefix rules have been clarified (tracked issue 147).

- Requirements section has been completed to include all necessary requirements (tracked issue 148).

- Implementations have been given the freedom to implement the security association - home address check either in the security policy data base or in the mobile IPv6 code (tracked issue 149).

- A procedure has been provided to deal with failed de-registration, to ensure that the Binding Acknowledgement still reaches the mobile node (tracked issue 150).

- Binding Error messages are now sent only to unicast addresses (tracked issue 151).

- Mobile nodes are now expected to limit their requested bindings to valid, not preferred, lifetime (tracked issue 152).

- Acknowledgements are now recommended for correspondent bindings (tracked issue 153).

- A large number of editorial modifications have been performed, including some restructuring of the document. Some of these modifications have been tracked as issues 52, 55, 57, 59, 64, 67, 84, 86, 102, 104, 107, 112, 120, 122, 128, 130, 137.

B. Future Extensions

B.1. Piggybacking

This document does not specify how to piggyback payload packets on the binding related messages. However, it is envisioned that this can be specified in a separate document when currently discussed issues such as the interaction between piggybacking and IPsec are fully resolved (see also Section B.3). The return routability messages can indicate support for piggybacking with a new mobility option.

B.2. Triangular Routing and Unverified Home Addresses

Due to the concerns about opening reflection attacks with the Home Address destination option, this specification requires that this option must be verified against the Binding Cache, i.e., there must be a Binding Cache entry for the Home Address and Care-of Address.

Future extensions may be specified that allow the use of unverified Home Address destination options in ways that do not introduce security issues.

B.3. New Authorization Methods beyond Return Routability

While the return routability procedure provides a good level of security, there exists methods that have even higher levels of security. Secondly, as discussed in Section 14.4, future

enhancements of IPv6 security may cause a need to improve also the
security of the return routability procedure. Using IPsec as the

sole method for authorizing Binding Updates to correspondent nodes is also possible. The protection of the Mobility Header for this purpose is easy, though one must ensure that the IPsec SA was created with appropriate authorization to use the home address referenced in the Binding Update. For instance, a certificate used by IKE to create the security association might contain the home address. A future specification may specify how this is done.

B.4. Security and Dynamically Generated Home Addresses

A future version of this specification may include functionality that allows the generation of new home addresses without requiring pre-arranged security associations or certificates even for the new addresses.

B.5. Remote Home Address Configuration

The method for initializing a mobile node's home addresses on power-up or after an extended period of being disconnected from the network is beyond the scope of this specification. Whatever procedure is used should result in the mobile node having the same stateless or stateful (e.g., DHCPv6) home address autoconfiguration information it would have if it were attached to the home network. Due to the possibility that the home network could be renumbered while the mobile node is disconnected, a robust mobile node would not rely solely on storing these addresses locally.

Such a mobile node could initialize by using the following procedure:

1. Generate a care-of address.

2. Query DNS for the home network's mobile agent anycast address.

3. Send a Home Agent Address Discovery Request message to the home network.

4. Receive Home Agent Address Discovery Reply.

5. Select the most preferred home agent and establish a security association between the mobile node's current care-of address and the home agent for temporary use during initialization only.

6. Send a Home Prefix Solicitation with the Request All Prefixes flag set to the home agent from the mobile node's care-of address.

7. Receive a Home Prefix Advertisement from the home agent, follow

stateless address autoconfiguration rules to configure home
addresses for prefixes received.

8. Create a security association between the mobile node's home address and the home agent.

9. Send a Binding Update(s) to the home agent to register the mobile node's home addresses.

10. Receive Binding Acknowledgement(s) then begin normal communications.

Chairs' Addresses

The Working Group can be contacted via its current chairs:

Basavaraj Patil
Nokia Corporation
6000 Connection Drive
M/S M8-540
Irving, TX 75039
USA
Phone: +1 972-894-6709
Fax : +1 972-894-5349
EMail: Raj.Patil@nokia.com

Phil Roberts
Megisto Corp.
Suite 120
20251 Century Blvd
Germantown MD 20874
USA
Phone: +1 847-202-9314
Email: PRoberts@MEGISTO.com

Authors' Addresses

Questions about this document can also be directed to the authors:

David B. Johnson
Rice University
Dept. of Computer Science, MS 132
6100 Main Street
Houston, TX 77005-1892
USA

Phone: +1 713 348-3063
Fax: +1 713 348-5930
E-mail: dbj@cs.rice.edu

Charles E. Perkins
Nokia Research Center

313 Fairchild Drive
Mountain View, CA 94043
USA

Phone: +1 650 625-2986
Fax: +1 650 625-2502
E-mail: charliep@iprg.nokia.com

Jari Arkko
Ericsson
Jorvas 02420
Finland

Phone: +358 40 5079256
E-mail: jari.arkko@ericsson.com