IETF Mobile IP Working Group
INTERNET-DRAFT

David B. Johnson
Rice University
Charles Perkins
Nokia Research Center
Jari Arkko
Ericsson
1 May 2002

Mobility Support in IPv6
<draft-ietf-mobileip-ipv6-17.txt>

Status of This Memo

This document specifies the operation of mobile computers using IPv6. 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, MUST support communications with mobile nodes.

Contents

1. Introduction

This document specifies the operation of mobile computers using Internet Protocol Version 6 (IPv6) [6]. Without specific support for mobility in IPv6, packets destined to a mobile node (host or router) would not be able to reach it while the mobile node is away from its home link (the link on which its home IPv6 subnet prefix is in use), since routing is based on the subnet prefix in a packet's destination IP address. 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 IP address. A mobile node is always addressable by its "home address", an IP address assigned to the mobile node within its home subnet prefix on its home link. Packets may be routed to the mobile node using this address regardless of the mobile node's current point of attachment to the Internet, and the mobile node may 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, reestablishing link-layer connectivity to the node in each new location. Within the natural limitations imposed by link-management solutions, and as long as such handover occurs only within cells of the mobile node's home link, such link-layer mobility mechanisms MAY offer faster

convergence and lower overhead than Mobile IPv6. Extensions to the Mobile IPv6 protocol have been proposed to support a more local, hierarchical form of mobility management, but such extensions are beyond the scope of this document.

The protocol specified in this document solves the problem of transparently routing packets to and from mobile nodes while away from home. However, it 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 11.4.1).
- Access control on a link being visited by a mobile node.
- 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) represents a natural combination of the experiences gained from the development of Mobile IP support in IPv4 (Mobile IPv4) [25, 24, 26], together with the opportunities provided by the design and deployment of a new version of IP itself (IPv6) and the new protocol features offered by IPv6. Mobile IPv6 thus shares many features with Mobile IPv4, but the protocol is now fully integrated into IP and provides many improvements over Mobile IPv4. This section summarizes the major differences between Mobile IPv4 and Mobile IPv6:

- Support for what is known in Mobile IPv4 as "Route Optimization" [27] is now built in as a fundamental part of the protocol, rather than being added on as an optional

set of extensions that may not be supported by all nodes as in Mobile IPv4. This integration of Route Optimization functionality allows direct routing from any correspondent node to any mobile node, without needing to pass through the mobile node's home network and be forwarded by its home agent, and thus eliminates the problem of "triangle routing" present in the base Mobile IPv4 protocol [25]. The Mobile IPv4 "registration" functionality and the Mobile IPv4 Route Optimization functionality are performed by a single protocol rather than two separate (and different) protocols.

- Support is also integrated into Mobile IPv6 -- and into IPv6 itself -- for allowing Route Optimization to coexist efficiently with routers that perform "ingress filtering" [7]. A mobile

node uses its care-of address as the Source Address in the IP header of packets it sends, allowing the packets to pass normally through ingress filtering routers. The home address of the mobile node is carried in the packet in a Home Address destination option, allowing the use of the care-of address in the packet to be transparent above the IP layer. The ability to correctly process a Home Address option in a received packet is required in all IPv6 nodes, whether mobile or stationary, whether host or router.

- The use of the care-of address as the Source Address in each packet's IP header also simplifies routing of multicast packets sent by a mobile node. With Mobile IPv4, the mobile node had to tunnel multicast packets to its home agent in order to transparently use its home address as the source of the multicast packets. With Mobile IPv6, the use of the Home Address option allows the home address to be used but still be compatible with multicast routing that is based in part on the packet's Source Address.

- There is no longer any need to deploy special routers as "foreign agents" as are used in Mobile IPv4. In Mobile IPv6, mobile nodes make use of IPv6 features, such as Neighbor Discovery [20] and Address Autoconfiguration [33], to operate in any location away from home without any special support required from the local router.

- 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 (packets that the router sends are reaching the mobile node, and packets that the mobile node sends are reaching the router). This confirmation provides a detection of the "black hole" situation that may exist in some wireless environments where the link to the router does not work equally well in both directions, such as when the mobile node has moved out of good wireless transmission range from the router. The mobile node may then attempt to find a new router and begin using a new care-of address if its link to its current router is not working well. In contrast, in Mobile IPv4, only the forward direction (packets from the router are reaching the mobile node) is confirmed, allowing the black hole condition to persist.

- 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, whereas Mobile IPv4 must use encapsulation for all packets. The use of a Routing header requires less additional header bytes to be added to the packet, reducing the overhead of Mobile IP packet delivery. To avoid modifying the packet in flight, however, packets intercepted and tunneled by a mobile

node's home agent in Mobile IPv6 must still use encapsulation for delivery to the mobile node.

- While a mobile node is away from home, its home agent intercepts any packets for the mobile node that arrive at the home network, using IPv6 Neighbor Discovery [20] rather than ARP [29] as is used in Mobile IPv4. The use of Neighbor Discovery improves the robustness of the protocol (e.g., due to the Neighbor Advertisement "override" bit) and decouples Mobile IP from any particular link layer, unlike in ARP.

- The use of IPv6 encapsulation (and the Routing header) removes the need in Mobile IPv6 to manage "tunnel soft state", which was required in Mobile IPv4 due to limitations in ICMP for IPv4. Due to the definition of ICMP for IPv6, the use of tunnel soft state is no longer required in IPv6 for correctly relaying ICMP error messages from within the tunnel back to the original sender of

the packet.

- The dynamic home agent address discovery mechanism in Mobile IPv6 uses IPv6 anycast [11] and returns a single reply to the mobile node, rather than the corresponding Mobile IPv4 mechanism that uses IPv4 directed broadcast and returns a separate reply from each home agent on the mobile node's home link. The Mobile IPv6 mechanism is more efficient and more reliable, since only one packet has to be sent back to the mobile node.

- Mobile IPv6 defines an Advertisement Interval option for Router Advertisements (equivalent to Agent Advertisements in Mobile IPv4), allowing a mobile node to decide for itself how many Router Advertisements (Agent Advertisements) it is willing to miss before declaring its current router unreachable.

- The return routability procedure (see section 5.5) provides a way to verify the that a mobile node is reachable at its claimed home address and at its claimed care-of address. This allows correspondent nodes to verify the authority of the Binding Updates sent to it. Given that the return routability procedure is light-weight and does not require participation in a security infrastructure, it is expected that Route Optimization can be deployed on a global scale between all mobile nodes and correspondent nodes.

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 [3].

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.

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. Mobile IPv6 defines one new destination option, the Home Address destination option.

3.2. Mobile IPv6 Terms

home address

An IP 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

An IP 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.

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 cookie 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 cookies related to the return routability procedure. The nonces are not specific to a mobile node, and are kept secret within the correspondent node, only used as one input in the creation of the cookies.

cookie

Cookies are numbers that are used by mobile nodes in the return routability procedure.

care-of cookie

A cookie sent directly to the mobile node's claimed care-of address from the correspondent node.

home cookie

A cookie sent to the mobile node's claimed home address from the correspondent node.

mobile cookie

A cookie sent to the correspondent node from the mobile node, and later returned to the mobile node. Mobile cookies are produced randomly.

nonce index

The mobile node uses a particular set of cookies in the return routability procedure. The cookies have been produced using a particular set of nonces. A nonce index is used to indicate which nonces have been used, without revealing the nonces themselves.

binding key

a key used for authenticating binding cache management messages.

binding security association

a security association established specifically for the purpose of producing and verifying authentication data passed with a Binding Authorization Data option.

4. Overview of Mobile IPv6

4.1. Basic Operation

A mobile node is always addressable at its home address, whether it

is currently attached to its home link or is away from home. While a mobile node is at home, packets addressed to its home address are routed to it using conventional Internet routing mechanisms in the same way as if the node were stationary. Since the subnet prefix of a mobile node's home address is one of the subnet prefixes of the mobile node's home link, packets addressed to the mobile node will be routed to its home link.

While a mobile node is attached to some foreign link away from home, it is also addressable at one or more care-of addresses, in addition to its home address. A care-of address is an IP address associated with a mobile node while visiting a particular foreign link. The subnet prefix of a mobile node's care-of address is one of the subnet prefixes on the foreign link being visited by the mobile node; if the mobile node is connected to this foreign link while using that care-of address, packets addressed to this care-of address will be routed to the mobile node in its location away from home.

The association between a mobile node's home address and care-of address is known as a "binding" for the mobile node. A mobile node typically acquires its care-of address through stateless [33] or stateful (e.g., DHCPv6 [2]) Address Autoconfiguration, according to the methods of IPv6 Neighbor Discovery [20]. Other methods of acquiring a care-of address are also possible, such as static pre-assignment by the owner or manager of a particular foreign link, but details of such other methods are beyond the scope of this document. The operation of the mobile node is specified in Section 11.

While away from home, a mobile node registers one of its care-of addresses 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 then replies to the mobile

node by returning a "Binding Acknowledgement" message. The care-of address associated with this binding registration is known as the mobile node's "primary care-of address". The mobile node's home agent thereafter uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the mobile node's home address (or home addresses) on the home link, and tunnels each intercepted packet to the mobile node's primary care-of address. To tunnel each

intercepted packet, the home agent encapsulates the packet using IPv6 encapsulation [4], with the outer IPv6 header addressed to the mobile node's primary care-of address. The operation of the home agent is specified in Section 10.

The Binding Update and Binding Acknowledgement messages, together with a "Binding Refresh Request" message, are also used to allow IPv6 nodes communicating with a mobile node are capable of dynamically learning and caching the mobile node's binding. This happens through the correspondent binding procedure which involves a return routability test in order to authorize the establishment of the binding, as specified in Sections 5.5.5 and 5.5.6. When sending a packet to any IPv6 destination, a 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 [6] (see section 6.4) to route the packet to the mobile node by way of the care-of address indicated in this binding. If, instead, the sending node has no cached binding for this destination address, the node sends the packet normally (with no Routing header), and the packet is subsequently intercepted and tunneled by the mobile node's home agent as described above. 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. The operation of the correspondent node is specified in Section 9.

Mobile IPv6 also defines one additional IPv6 destination option. When a mobile node sends a packet while away from home, it could generally use a tunnel via the home agent to send this packet. However, if the correspondent node in question has a binding for this mobile node it can use deliver packets more directly. In this case the mobile node can the Source Address in the packet's IPv6 header to one of its current care-of addresses, and include a "Home Address" destination option in the packet, giving the mobile node's home address. Many routers implement security policies such as "ingress filtering" [7] that do not allow forwarding of packets having a Source Address that appears topologically incorrect. By using the care-of address as the IPv6 header Source Address, the packet will be able to pass normally through such routers, and ingress filtering rules will still be able to locate the true topological source of the packet in the same way as packets from non-mobile nodes. By also including the Home Address destination option in each packet, the sending mobile node can communicate its home address to the correspondent node receiving this packet, allowing the use of the

care-of address to be transparent above the Mobile IPv6 support level (e.g., at the transport layer). The inclusion of a Home Address destination option in a packet affects only the correspondent node's receipt of this single packet; no state is created or modified in the correspondent node as a result of receiving a Home Address destination option in a packet.

It is possible that while a mobile node is away from home, some nodes on its home link may be reconfigured, such that the router that was operating as the mobile node's home agent is replaced by a different router serving this role. In this case, the mobile node may not know the IP address of its own home agent. Mobile IPv6 provides a mechanism, known as "dynamic home agent address discovery", that allows a mobile node to dynamically discover the IP address of a home agent on its home link with which it may register its (primary) care-of address while away from home. The mobile node sends an ICMP "Home Agent Address Discovery Request" message to the "Mobile IPv6 Home-Agents" anycast address for its own home subnet prefix [11] and thus reaches one of the routers on its home link currently operating as a home agent. This home agent then returns an ICMP "Home Agent Address Discovery Reply" message to the mobile node, including a list of home agents on the home link. This procedure is specified in Sections 10.9 and 11.3.2.

When a mobile node moves from one care-of address to a new care-of address on a new link, it is desirable for packets arriving at the previous care-of address to be tunneled to the mobile node's new care-of address. Since the purpose of a Binding Update is to establish exactly this kind of tunneling, it can be used (at least temporarily) for tunnels originating at the mobile node's previous care-of address, in exactly the same way that it is used for establishing tunnels from the mobile node's home address to the mobile node's current care-of address. Section 11.6.6 describes the use of the Binding Update for this purpose.

Section 11.4.3 discusses the reasons why it may be desirable for a mobile node to use more than one care-of address at the same time. However, a mobile node's primary care-of address is distinct among these in that the home agent maintains only a single care-of address registered for each home address belonging to a mobile node, and always tunnels packets sent to a mobile node's home address and intercepted from its home link to this mobile node's registered primary care-of address. The home agent thus need not implement any policy to determine the particular care-of address to which it will tunnel each intercepted packet. The mobile node alone controls the policy by which it selects the care-of addresses to register with its home agent.

4.2. New IPv6 Protocols

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

The Home Test Init message is used to initiate the return routability procedure from the mobile node to a correspondent node. This procedure ensures that subsequent Binding Updates are properly authorized to redirect the traffic of a particular home address. The Home Test Init message is described in detail in Section 6.1.3.

Care-of Test Init

The Care-of Test Init message is used to initiate the correspondent routability procedure, for a particular care-of address. The Care-of Test Init message is described in detail in Section 6.1.4.

Home Test

The Home Test message carries a cookie which the mobile node needs before it can properly authorize itself for sending a Binding Update. This message is sent in reply to the Home Test Init message, and is described in detail in Section 6.1.5.

Care-of Test

The Care-of Test message carries another cookie which the mobile node needs before it can properly authorize itself for sending a Binding Update. This message is sent in reply to the Care-of Test Init message, and is described in detail in Section 6.1.6.

Binding Update

A Binding Update message 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 and its specific authentication requirements are described in detail in Section 6.1.7.

Binding Acknowledgement

A Binding Acknowledgement message is used to acknowledge receipt of a Binding Update, if an acknowledgement was

requested in the Binding Update. The Binding Acknowledgement message and its specific authentication requirements are described in detail in Section 6.1.8.

Binding Refresh Request

A Binding Refresh Request message is used to request that a mobile node send to the requesting node a Binding Update containing the mobile node's current binding. This message is typically used by a correspondent node to refresh a cached binding for a mobile node, when the cached binding is in active use but the binding's lifetime is close to expiration. The Binding Refresh Request message is described in detail in Section 6.1.2.

No authentication is required for the Binding Refresh Request message.

Binding Error

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

4.3. New IPv6 Destination Options

Mobile IPv6 defines a new IPv6 destination option, the Home Address destination option. This option is used in a packet sent by a mobile node to inform the recipient of that packet of the mobile node's home address. For packets sent by a mobile node while away from home, the mobile node generally uses one of its care-of addresses as the Source Address in the packet's IPv6 header. By including a Home Address option in the packet, the correspondent node receiving the packet is able to substitute the mobile node's home address for this care-of address when processing the packet, thus making the use of the care-of address transparent to the correspondent node above the Mobile IPv6 support level. If the IP header of a packet carrying a Home Address option is covered by authentication, then the Home Address option MUST also be covered by this authentication, but no other authentication is required for the Home Address option. See Sections 6.3 and 11.2.2 for additional details about requirements for the calculation and verification of the authentication data. The Home Address destination 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 discussed in general in Section 4.1, the following two new ICMP message types are used for home agent address discovery:

Home Agent Address Discovery Request

The ICMP Home Agent Address Discovery Request message is used by a mobile node to initiate the dynamic home agent address discovery mechanism. When attempting a home registration, the mobile node may use this mechanism to discover the address of one or more routers currently operating as home agents on its home link, with which it may register while away from home. The Home Agent Address Discovery Request message is described

in detail in Section 6.5.

Home Agent Address Discovery Reply

The ICMP Home Agent Address Discovery Reply message is used by a home agent to respond to a mobile node using the dynamic home agent address discovery mechanism. When a home agent receives a Home Agent Address Discovery Request message, it replies with a Home Agent Address Discovery Reply message, giving a list of the routers on the mobile node's home link serving as home agents. The Home Agent Address Discovery Reply message is described in detail 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 10.9.1:

Mobile Prefix Solicitation

The ICMP Mobile Prefix Solicitation message is used by a mobile node to request prefix information about the home subnet, in order to retrieve prefixes that are served by home agents and can be used to configure one or more home addresses, or to refresh home addresses before the expiration of their validity. This message is specified in Section 6.7.

Mobile Prefix Advertisement

The ICMP Mobile Prefix Advertisement is used by a home agent to distribute information to a mobile node about prefixes on the home link which are available for use by the mobile node while away from home. This message may be sent as a response to a Mobile Prefix Solicitation, or due to network renumbering

or other prefix changes. This message is specified in Section Section 10.9.3.

4.5. Conceptual Data Structures

This document describes the Mobile IPv6 protocol in terms of the

following three conceptual data structures:

Binding Cache

A cache, maintained by each IPv6 node, of bindings for other nodes. A separate Binding Cache is maintained by each IPv6 node for each of its IPv6 addresses. When sending a packet, the Binding Cache is searched before the Neighbor Discovery conceptual Destination Cache [20].

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 all of a node's Binding Cache entries are cleared when it reboots.

Binding Cache entries are marked either as "home registration" entries or "correspondent registration" entries. Home registration entries are deleted when its binding lifetime expires, while other entries may be replaced at any time through a local cache replacement policy.

Binding Update List

A list, maintained by each mobile node, recording 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: those to correspondent nodes, those to the mobile node's home agent, and those to a home agent on the link on which the mobile node's previous care-of address is located.

Home Agents List

A list, maintained by each home agent and each mobile node, recording information about each home agent from which this node has received recent a Router Advertisement in which the Home Agent (H) bit is set. The home agents list is thus similar to the Default Router List conceptual data structure maintained by each host for Neighbor Discovery [20].

Each home agent maintains a separate Home Agents List for each link on which it is serving as a home agent; this list is used by a home agent in the dynamic home agent address discovery mechanism. Each mobile node, while away from home, also

maintains a Home Agents List, to enable it to notify a home agent on its previous link when it moves to a new link.

4.6. Binding Management

When a mobile node configures a new care-of address and decides to use this new address as its primary care-of address, the mobile node registers this new binding with its home agent by sending the home agent a Binding Update. The mobile node indicates that an acknowledgement is needed for this Binding Update and continues to periodically retransmit it until acknowledged. The home agent acknowledges the Binding Update by returning a Binding Acknowledgement to the mobile node.

When a mobile node receives a packet tunneled to it from its home agent, the mobile node uses that as an indication that the original sending correspondent node has no Binding Cache entry for the mobile node, since the correspondent node would otherwise have sent the packet directly to the mobile node using a Routing header. The mobile node SHOULD then start a correspondent binding procedure in order to establish a binding. This would allow the correspondent node to cache the mobile node's binding for routing future packets to it.

A correspondent node with a Binding Cache entry for a mobile node may refresh this binding, for example if the binding's lifetime is near expiration, by sending a Binding Refresh Request to the mobile node. Normally, a correspondent node will only refresh a Binding Cache entry in this way if it is actively communicating with the mobile node and has indications, such as an open TCP connection to the mobile node, that it will continue this communication in the future. When a mobile node receives a Binding Refresh Request, it MAY reply by initiating a correspondent binding procedure.

A mobile node may use more than one care-of address at the same time. Use of more than one care-of address by a mobile node may be useful, for example, to improve smooth handover when the mobile node moves from one wireless link to another. If each of these wireless links is connected to the Internet through a separate base station, such that the wireless transmission range from the two base stations overlap, the mobile node may be able to remain connected to both links while in the area of overlap. In this case, the mobile node could acquire a new care-of address on the new link before moving out of transmission range and disconnecting from the old link. The mobile node may thus still accept packets at its old care-of address while it works to update its home agent and correspondent nodes,

notifying them of its new care-of address on the new link.

Since correspondent nodes cache bindings, it is expected that correspondent nodes usually will route packets directly to the mobile

node's care-of address, so that the home agent is rarely involved with packet transmission to the mobile node. This is important for scalability and reliability, and for minimizing overall network load. By caching the care-of address of a mobile node, direct delivery of packets can be achieved from the correspondent node to the mobile node. Routing packets directly to the mobile node's care-of address 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, the home link, or intervening networks leading to or from the home link is reduced, since these nodes and links are not involved in the delivery of most packets to the mobile node.

5. Overview of Mobile IPv6 Security

5.1. Threats

Any mobility solution must protect itself against misuses of the mobility features. In Mobile IPv6, most of the potential threats are concerned with denial of service. Some of the threats also include potential for man-in-the-middle, hijacking, and impersonation attacks. The main threats this protocol protects against are as follows:

1. Threats against 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 the home agent accepts the information sent to it as is, the mobile node might not get traffic destined to it, and other nodes might get traffic they did not want.

   Similarly, a malicious mobile node might use the home address of a victim node in a forged Binding Update to a correspondent node. If such Binding Updates were accepted, the communications between the correspondent node and the victim would be then be disrupted, because packets that the correspondent node intended to send to the victim would be sent to the wrong care-of address. This is

a threat to confidentiality as well as availability, because an attacker might redirect packets meant for another node to itself in order to learn the content of those packets.

A malicious mobile node might also send Binding Updates in which the care-of address is set to the address of a victim node or an address within a victim network. If such Binding Updates were accepted, the malicious mobile node could force the correspondent node into sending data to the victim node or the victim network; 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. Variations of this threat are described elsewhere [1][31].

A malicious node might also send a large number of invalid Binding Updates to a victim node. If each Binding Update takes a significant amount of resources (such as CPU) to process before it can be recognized either as valid or as invalid, then a denial of service attack can be caused by sending the correspondent node so many invalid Binding Updates that it has no resources left for other tasks.

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.

2. Reflection attack threats against third partied with the help of Mobile IPv6 correspondent nodes that do not use appropriate security precautions. The Home Address destination option can be used to direct response traffic toward a node whose IP address appears in the option, without allowing ingress filtering to catch the forged "return address" [32] [23].

3. Threats where an attacker forges tunneled 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.

4. Threats against IPv6 functionality used by Mobile IPv6, such as the Routing header. The generality of the regular Routing Header

would allow circumvention of IP-address based rules in firewalls or reflection of traffic to other nodes, even if the usage that Mobile IPv6 requires is safe.

5. The security mechanisms of Mobile IPv6 may also be attacked themselves, e.g. in order to force the participants to execute expensive cryptographic operations or allocate memory for the purpose of keeping state.

5.2. Features

This specification provides a number of security features. The main features are:

- Protection of Binding Updates to home agents.
- Protection of Binding Updates to correspondent nodes.
- Protection against reflection attacks through the Home Address destination option.
- Protection of tunnels between the mobile node and the home agent.

- Preventing Routing Header vulnerabilities.
- Preventing Denial-of-Service attacks to the Mobile IPv6 security mechanisms themselves.

Protecting the Binding Updates to home agents and to arbitrary correspondent nodes require 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, and thus to have a strong security association to reliably authenticate the exchanged messages. With such a security arrangement, IPsec Encapsulating Security Payload (ESP) can be used to implement the necessary security features. See Section 5.4.

It is expected that Mobile IPv6 will be used on a global basis between nodes belonging to different administrative domains. Building an authentication infrastructure to authenticate mobile

nodes and correspondent nodes would be a very demanding task in this scale. Furthermore, traditional authentication infrastructure keep track of correct IP addresses for all hosts is either impossible or at least very hard. That is, it isn't sufficient to authenticate mobile nodes, authorization to claim right to use an address is needed. Thus, an "infrastructureless" approach is necessary.

The chosen infrastructureless method verifies that the mobile node is "live" (that is, it responds to probes) at its home and care-of addresses by performing a cookie exchange with the nodes in question, and by requiring that the eventual Binding Update is cryptographically bound to the exchanged cookies. Some additional protection is provided by requiring the cookies be protected by ESP when exchanged between the mobile node and the correspondent node via the home agent. This method limits the vulnerabilities to those attackers who are on the path between the home agent and the correspondent node. As adversaries on this path would be able to cause also other types of attacks, this is seen as sufficient base security between mobile and correspondent nodes.

Vulnerabilities relating to the use of correspondent nodes as reflectors via the Home Address destination option can be solved as follows: We ensure that the mobile node is authorized to use a given home address before this option can be used. Such authorization is already performed in the context of Route Optimization, and therefore this specification limits the use of the Home Address option to the situation where the correspondent node already has a binding cache entry for the given home address.

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 5.3.

Potential abuses of the Routing Header can be prevented by using a Mobile IPv6 specific type of a Routing Header. This type provides the necessary functionality but does not open vulnerabilities.

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 5.5.9.

5.3. Tunnels to and from the Home Agents

Mobile IPv6 tunneling -- as tunneling in general -- needs protection so that it isn't possible, e.g., for anyone to pose as the home agent and send traffic to the mobile node. To protect the tunnels to the mobile node, the mobile node verifies that the outer IP address corresponds to its home agent, to prevent attacks against the tunnel from other IP addresses.

Tunnels from the mobile node to the home agent need protection so that it isn't possible for anyone to send traffic through the home agent, pose as the mobile node, and escape detection through traditional tracing mechanisms.

Binding Updates sent to the home agents are secure. The home agent verifies that the outer IP address corresponds to the current location of the mobile node, to prevent attacks against the tunnel from other IP addresses.

For tunneled traffic to and from the mobile node, encapsulating the traffic inside IPsec ESP offers an optional mechanism to protect the confidentiality and integrity of the traffic against on-path attackers.

5.4. Binding Updates to Home Agents

Signaling between the mobile node and the home agent requires message integrity, correct ordering and replay protection.

In order to have this protection, the mobile node and the home agent must have a security association. IPsec Encapsulating Security Payload (ESP) can be used for integrity protection when a non-null authentication algorithm is 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, Mobile IPv6 provides its own mechanism inside the Binding Update and Acknowledgement messages.

A sequence number field is used to ensure correct ordering. If the mobile node reboots and forgets its current sequence number, the home agent uses the status value 141 (Sequence number out of window, see Section 6.1.8) to inform the mobile node of the use of an improper sequence number.

Note that the the sequence number mechanism provides also a weak form of replay protection. However, if a home agent reboots and loses its state regarding the sequence numbers, replay attacks become possible. If the home agent is vulnerable to this, the use of a key management mechanism together with IPsec can be used to prevent 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.

In order to protect messages exchanged between the mobile node and the home agent with IPsec, appropriate security policy database entries must be created. We need to avoid the possibility that a mobile node could use its security association to send a Binding Update on behalf of another mobile node using the same home agent. In order to do this, the security policy database entries MUST unequivocally identify a single SA for any given home address and home agent. In order for the home address of the mobile node to be visible when the policy check is made, the mobile node MUST use the Home Address destination option in Binding Updates sent to the home agent. The home address in the Home Address destination option and the Binding Update message MUST be equal and MUST be checked by the home agent.

5.5. Binding Updates to Correspondent Nodes

Binding Updates to correspondent nodes are protected using the return routability procedure. The motivation for designing the return routability procedure was to have sufficient support for Mobile IP, without creating major new security problems. It was not our goal to protect against attacks that were already possible before the introduction of Mobile IP. This protocol does not defend against an attacker who can monitor the home agent to correspondent node path, as such attackers would in any case be 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 IP, because these attacks are possible regardless of whether Mobile IP is in use.

This protocol 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, and so causes the correspondent node to send the victim traffic that it does not expect. For example,

suppose that the correspondent node is a news 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 then redirect the stream to the victim's address. This protocol defends against these attacks by only completing if packets sent by the correspondent node to the care of address are received and processed by an entity that is willing to participate in the protocol. Normally, this will be the mobile node.

For further information about the design rationale of the return routability procedure, see [1] [31] [22] [23].

The return routability procedure method uses the following principles:

- A cookie exchange verifies that the mobile node is reachable at its addresses i.e. is at least able to transmit and receive traffic at its addresses.

- The eventual Binding Update is protected cryptographically using the cookies.

- Requiring that the cookies be protected by ESP when forwarded by the home agent to the mobile node.

- The use of symmetric exchanges where responses are sent to the same address as the request was sent from, to avoid the use of this protocol in reflection attacks.

- Correspondent nodes operate in a stateless manner until they receive a Binding Update that can be authorized.

The return routability procedure can be broken by an attacker on the

route between the home agent and the correspondent node, but not by attackers on the network the mobile node is currently at and not from elsewhere on the Internet.

5.5.1. Node Keys

Each correspondent node has a secret key, Kcn. This key is used by the correspondent node to accept only the use of cookies which it has created itself. This key does not need to be shared with any other entity, so no key distribution mechanism is needed for it.

A correspondent node can generate a fresh Kcn each time that it boots to avoid the need for secure persistent storage for Kcn. Kcn can be

either a fixed value or regularly updated. Procedures for updating Kcn are discussed later in Section 5.5.7.

Kcn consists of 20 octets.

5.5.2. Nonces

Each correspondent node also generates a nonce at regular intervals, for example every few minutes. A correspondent node uses the same Kcn and nonce with all the mobiles it is in communication with, so that it does not need to generate and store a new nonce when a new mobile contacts it. Each nonce is identified by a nonce index. Nonce indices are 16-bit values that are e.g. incremented each time a new nonce is created. 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. Correspondent nodes keep both the current nonce and a small set of old nonces. Older values can be discarded, and messages using them will be rejected as replays.

The specific nonce index values can not 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 5.5.7.

Nonce is an octet string of any length. The recommended length is 16 octets.

5.5.3. Cookies

Three different types of cookies are used in the protocol:

- Mobile cookie is sent to the correspondent node from the mobile node, and later returned to the mobile node. Mobile cookies are produced randomly, and used to verify that the response matches the request, and to ensure that parties who have not seen the request can not spoof responses.

- A home cookie sent to the mobile node from the correspondent node via the home agent. Home cookies are produced cryptographically from nonces.

- A care-of cookie sent directly to the mobile node from the correspondent node. Home cookies are produced cryptographically from nonces.

Mobile cookies are typically newly generated random values for each new request that needs them. They could also be changed periodically

only. The policy to use new or old mobile cookies is purely a local matter for the mobile node.

Home and care-of cookies are produced by the correspondent node, and they are based on the currently active secret keys and nonces of the correspondent node as well as the home or care-of address. Such a cookie is valid as long as both the secret key and the nonce used to create it are valid.

5.5.4. Cryptographic Functions

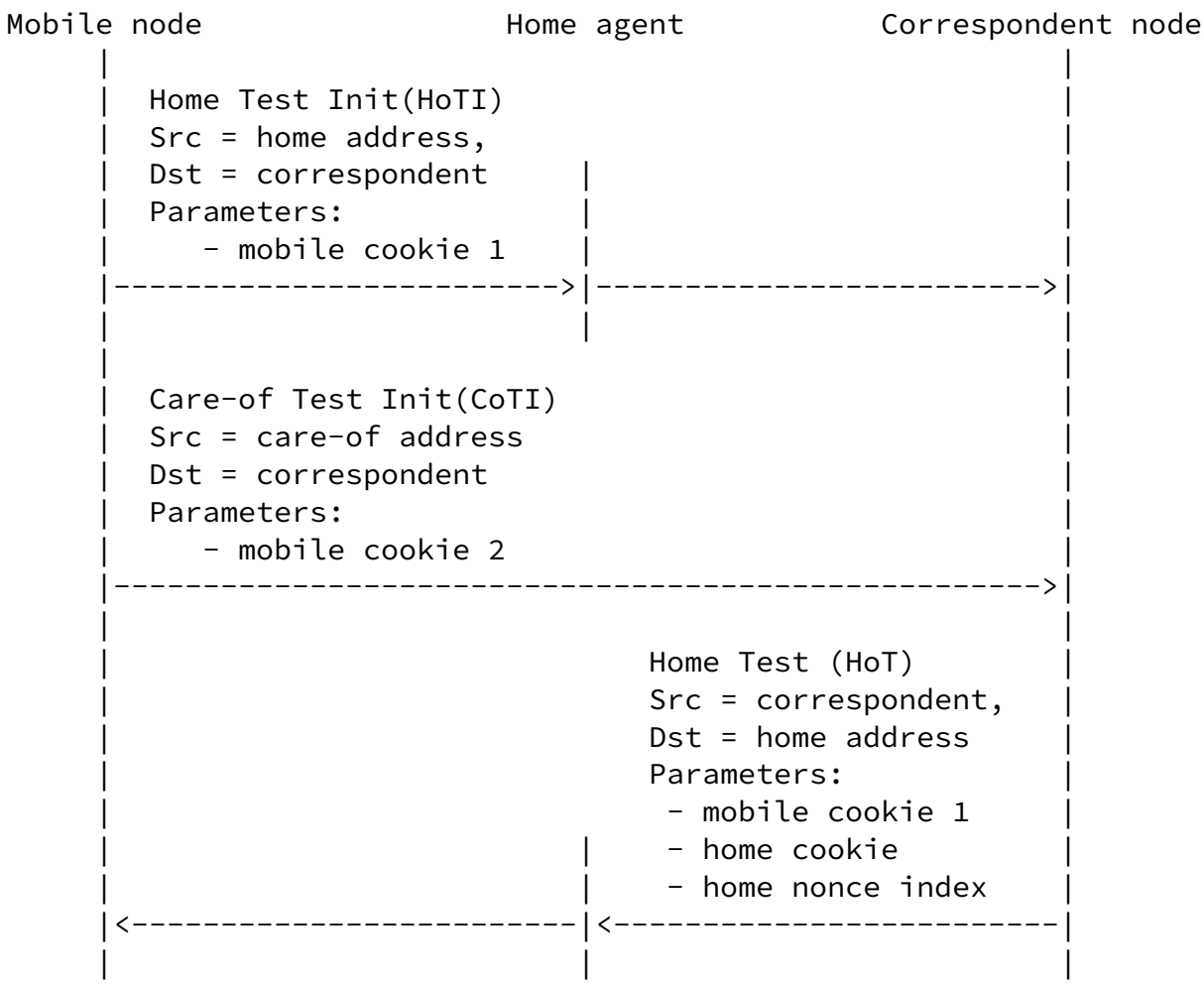
MAC_K(m) denotes a Message Authentication Code computed on message m with key K. In this specification, HMAC SHA1 function [15][21] is used to compute these codes.

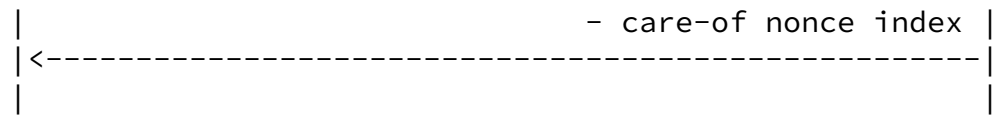
H(m) denotes a hash of message m. In this specification, SHA1

function [21] is used to compute the hash.

5.5.5. Return Routability Procedure

The return routability signaling happens as follows:





The HoTI and CoTI messages are sent at the same time. The correspondent node returns the HoT and CoT messages as quickly as possible, and perhaps nearly simultaneously, requiring very little processing. The four messages form the return routability procedure. (After the return routability procedure, a binding will be created with a single request with an optional response.) Due to the simultaneous sending of messages, the return routability procedure completes in 1 roundtrip (and the whole process completes in 1.5 roundtrips excluding the acknowledgement message).

The four messages (HoTI, CoTI, HoT, and CoT) belonging to the return routability procedure are described in more detail below. The use of the results of the return routability procedure for authenticating a correspondent binding procedure is described in Section 5.5.6.

HoTI

Home Test Init Message:

When a mobile nodes wants to perform route optimization it sends a HoTI message to the correspondent node in order to initiate the return routability verification for the Home Address.

```
Src = home address
Dst = correspondent
Parameters:
 - mobile cookie 1
```

This message conveys the mobile node's home address to the correspondent node. The mobile node also sends along mobile cookie C0 that the correspondent node must return later, along with its own cookie that it generates based on the home address. The HoTI message is reverse tunneled through the home agent.

CoTI

Care-of Test Init Message:

When a mobile nodes wants to perform route optimization it sends a CoTI message to the correspondent node in order to initiate the return routability verification for the care-of Address.

```
Src = care-of address
Dst = correspondent
Parameters:
 - mobile cookie 2
```

The second message is sent in parallel with the first one. It conveys the mobile node's care-of address to the correspondent node. The mobile node also sends along mobile cookie C1 that the correspondent node must return later, along with its own cookie that it generates based on the care-of address. The CoTI message is sent directly to the correspondent node.

HoT

Home Test Message:

This message is sent in response to a HoTI message.

```
Src = correspondent
Dst = home address
Parameters:
- mobile cookie 1
- home cookie
- home nonce index
```

When the correspondent node receives the HoTI message, it generates a 16 octet home cookie as follows:

```
home cookie = MAC_Kcn(home address | nonce)
```

The cookie is sent in the message to the mobile node via the Home Agent; it is an assumption of the protocol that the home agent - mobile node route is secure. Home cookie also acts as a challenge to test that the mobile can receive messages sent to its home address. Kcn is used in the production of home cookie in order to allow the correspondent node to verify that the cookies used later really came from itself, without forcing the correspondent node to remember a list of all cookies it has handed out.

Mobile cookie 1 from the mobile node is returned as well in the HoT message, to ensure that the message comes from someone on

the path to the correspondent node.

The home nonce index is carried along in the protocol to allow the correspondent node to later efficiently find the nonce value Ni that it used in creating this cookie.

CoT

Care-of Test Message:

This message is sent in response to a CoTI message.

```
Src = correspondent
Dst = care-of address
Parameters:
- mobile cookie 2
- care-of cookie
- care-of nonce index
```

The correspondent node also sends a challenge to the mobile's care-of address. When the correspondent node receives the CoTI message, it generates a 16 octet care-of cookie as follows:

```
care-of cookie = MAC_Kcn(care-of address | nonce)
```

The cookie is sent directly to the mobile node at its care-of address. Mobile cookie 2 from the mobile node is returned as well, to ensure that the message comes from someone on the path to the correspondent node.

Again, an index is sent along the cookie in order to identify the used nonce. Note that home and care-of nonce indices are likely to be the same in HoT and CoT messages, except when the correspondent node changed its nonce value between the reception of HoTI and the CoTI messages.

When the mobile node has received both the HoT and CoT messages, the return routability procedure is complete. As a result, the mobile node has the means to prove its authority to send a Binding Update

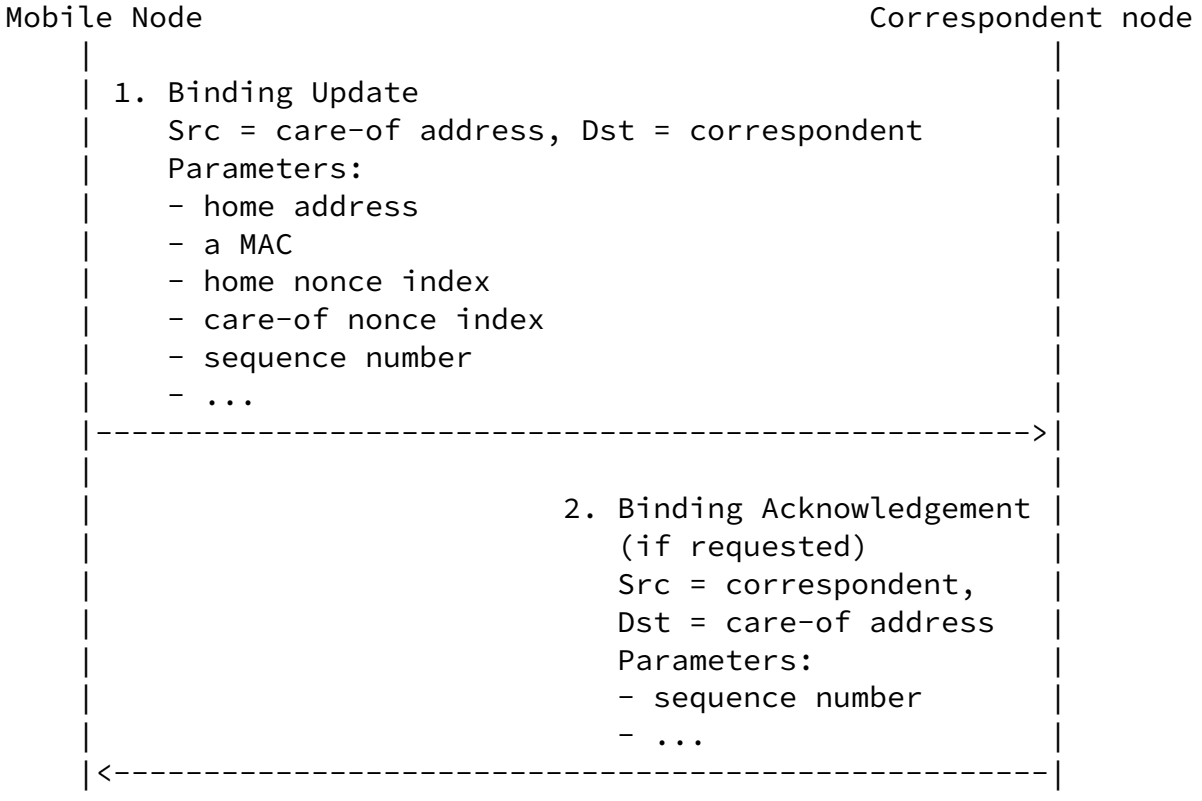
to the correspondent node. The mobile node hashes together the challenges to form a 20 octet session key (Kbu):

```
Kbu = H(home cookie | care-of cookie)
```

Note that the correspondent node has not created any state at this point. It is unaware of the session key Kbu, though it can recreate Kbu if it is presented the right addresses and nonce indices.

5.5.6. Applying Return Routability for Correspondent Bindings

After the return routability procedure, the mobile node can proceed to perform a binding procedure with the correspondent node. An overview of the binding procedure is shown below.



| |

Message 1 actually creates a binding, and message 2 is optional. The correspondent binding procedure consists of the return routability procedure followed by the messages 1 and 2.

1.

Binding Update (BU) Message:

The mobile node uses the created session key Kbu to authorize the Binding Update.

```
Src = care-of address
Dst = correspondent
Parameters:
- home address
- MAC_Kbu(care-of address | correspondent node address | BU)
- home nonce index
- care-of nonce index
- sequence number
- ...
```


The message contains home and care-of nonce indices, so that the correspondent node knows which nonces to use to recompute the session key. "BU" is the content of the Binding Update message, excluding (1) the IP header, (2) any extension headers between the IP header the Mobility Header, and (3) the Authenticator field inside the Binding Update. The result of the MAC_Kbu function is used as the Authenticator field in the Binding Update. A sequence number will be used to match an eventual acknowledgement with this message. The sequence numbers start from a random value, which offers a weak form of authentication also to the acknowledgement messages. The three dots represent all the remaining (not security related) information in the message.

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

2.

Binding Acknowledgement (BA) Message:

The Binding Update is optionally acknowledged by the correspondent node.

```
Src = correspondent
Dst = care-of address
Parameters:
- sequence number
- ...
```

The Binding Acknowledgement is not authenticated in other ways than including the right sequence number in the reply. The three dots represent all the remaining (not security related) information in the message.

5.5.7. Updating Node Keys and Nonces

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

Before sending a Binding Update in Step 3, the mobile node has to wait for both the Home and Care-of Cookies to arrive. Due to resource limitations, rapid deletion of bindings, or reboots it can not be guaranteed that the cookies are still fresh and acceptable when the correspondent node uses them in the processing of the Binding Update. If the cookies have become too old, the correspondent node replies with an an error code in the Binding Acknowledgement. The mobile node can then retry the return routability procedure. However, it is recommended that correspondent

nodes try to keep these cookies acceptable as long as possible and SHOULD NOT accept them beyond MAX_COOKIE_LIFE seconds.

Given that the cookies are normally expected to be usable for some time, the mobile node MAY use them beyond a single run of the return routability procedure. A fast moving mobile node may reuse a recent Home Cookie from a correspondent node when moving to a new

location, and just acquire a new Care-of Cookie to show routability in the new location. While this does not save roundtrips due to the parallel nature of the home and care-of return routability tests, the roundtrip through the home agent may be longer, and consequently this optimization is often useful. A mobile node that has multiple home addresses, may also use the same Care-of Cookie for Binding Updates concerning all of these addresses.

5.5.8. Preventing Replay Attacks

The return routability procedure also protects the participants against replayed Binding Updates. The attacker can't replay the same message due to the sequence number which is a part of the Binding Update, and the attacker can't modify the Binding Update since the MAC would not verify after that. Care must be taken when removing bindings at the correspondent node, however. If a binding is removed either due to garbage collection, request, or expiration and the nonce used in its creation is still valid, an attacker can replay the old Binding Update. This can be prevented by having the correspondent node 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.

5.5.9. Preventing Denial-of-Service Attacks

The return routability procedure has been designed with protection against resource exhaustion Denial-of-Service attacks. In these attacks the victim has only a limited amount of some resource (such as network bandwidth or CPU cycles), and the attack consumes some of this resource. This leaves the victim without enough resources to carry out other work.

The correspondent nodes do not have to retain any state about individual mobile nodes until an authentic Binding Update arrives. This is achieved through the use of the nonces and Kcn that are not specific to individual mobile nodes. The cookies are specific, but they can be reconstructed 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 [1] 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.

The binding updates that are used in Mobile IPv6 are only an optimization, albeit a very important optimization. A mobile node can communicate with a correspondent node even if the correspondent refuses to accept any of its 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 the resource exhaustion attacks by not processing binding updates when it is flooded with a large number of binding updates that fail the cryptographic integrity checks. 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 reject some or all Binding Updates without performing any cryptographic operations.

Additional information needed to make this decision about responding to requests will usually originate in layers above IP. For example, TCP knows if the node has a queue of data that it is trying to send to a peer. A conformant implementation of the protocols in this specification is not required to make use of information from higher protocol layers, but implementations are likely to be able to manage resources more effectively by making use of such information.

5.5.10. Correspondent Binding Procedure Extensibility

As discussed in Appendix D.3, in the future there may be other mechanisms beyond the return routability procedure for authorizing mobile nodes to correspondent nodes. The nodes can use other methods based on future definition of flag values in the Reserved fields of HoTI, HoT, CoTI, CoT, and BU messages. Nodes need assurance against bidding down attacks in this selection by following the procedure described in Section 14.3.

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

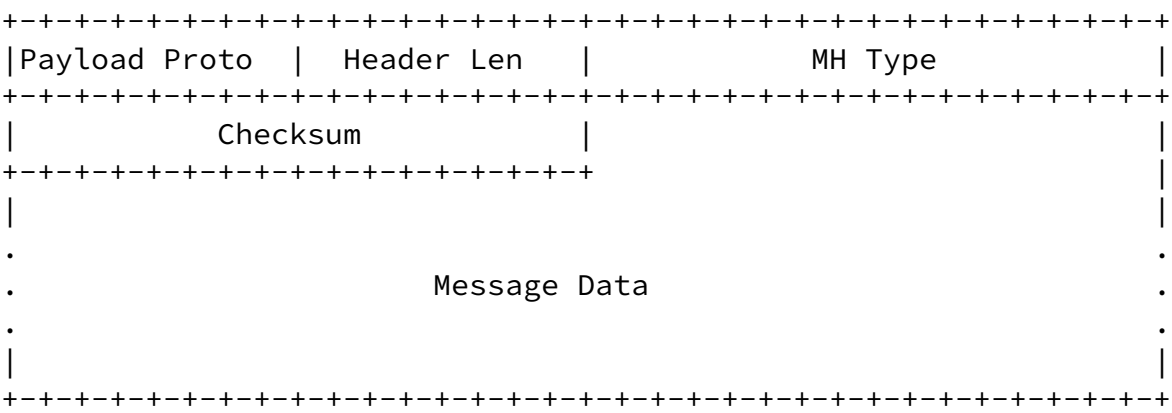
6.1. Mobility Header

The Mobility Header is used by mobile nodes, correspondent nodes, and home agents in all messaging related to the creation and management of bindings. The Mobility Header is an IPv6 protocol. Rules

regarding how it is sent and what addresses are used in the IPv6 header are given separately in Sections 6.1.2 through 6.1.9, which describe the message types used in this protocol.

6.1.1. Format

The Mobility Header is identified by a Next Header value of 62 (XXX) in the immediately preceding header, and has the following format:



Payload Proto

8-bit selector. Identifies the type of header immediately following the Mobility Header. Uses the same values as the IPv4 Protocol field [10].

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

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

Header Len

8-bit unsigned integer. Length of the Mobility Header in units of 8 octets, including the the Payload Proto, MH Type, Header Len, Checksum, and Message Data fields.

MH Type

16-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 to be sent to the source.

Checksum

16-bit unsigned integer. This field contains the checksum of the Mobility Header. The checksum is the 16-bit one's complement of the one's complement sum of an octet string consisting of a "pseudo-header" followed by the entire Mobility Header starting with the Payload Proto field. The pseudo-header contains IPv6 header fields, as specified in Section 8.1 of [6]. The Next Header value used in the pseudo-header is 62 (XXX). 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 is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options options. The encoding and format of defined options are described in Section 6.2.

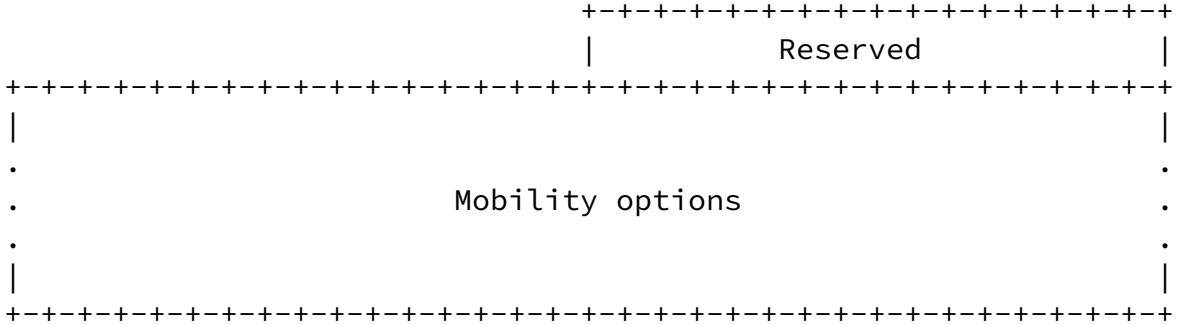
Alignment requirements for the Mobility Header are same as for any

IPv6 protocol Header. That is, they MUST be aligned on an 8-octet boundary. We also require that the Mobility Header length is a multiple of 8 octets.

6.1.2. Binding Refresh Request (BRR) Message

The Binding Refresh Request (BRR) message is used to request a mobile node's binding from the mobile node. A packet containing a Binding Refresh Request message is sent in the same way as any packet to a mobile node (Section 9.6). 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 (see Section 5.5) if it believes the amount of traffic with the correspondent justifies the use of Route Optimization. Note that the mobile node SHOULD NOT respond to Binding Refresh Requests from previously unknown correspondent nodes due to Denial-of-Service concerns.

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

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 Requests sent. This use of mobility options also allows for future extensions to the format of the Binding Refresh Request message to be defined. The following options are valid in a Binding Refresh Request message:

- Unique Identifier Option

- Binding Authorization option

The Header Length field in the Mobility Header for this message MUST be set to 1 (since unit is 8 octets) plus the total length of all mobility options present (also in 8 octet units). If no actual options are present in this message, no padding is necessary.

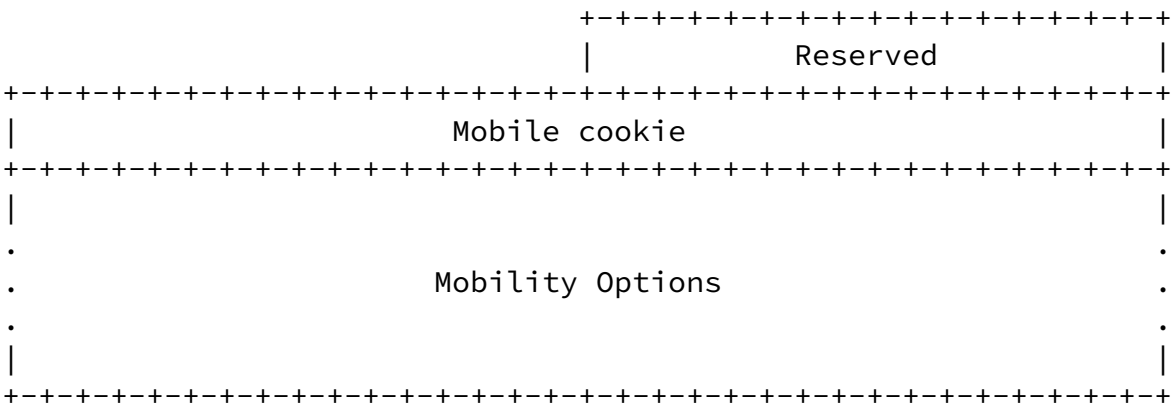
6.1.3. Home Test Init (HoTI) Message

The Home Test Init (HoTI) message is used to initiate the return routability procedure from the mobile node to a correspondent node (see Section 11.6.2). The purpose of this message is to test the reachability of the home address. This message is always sent with

the Source Address set to the home address of the mobile node, Destination Address set to the correspondent node's address, and 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 guided by the IPsec Policy Data Base. (Note the protection of HoTI messages is different from the requirement to protect regular payload traffic,

which MAY use such tunnels as well.)

The HoTI 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

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

Mobile cookie

32-bit field which contains a random value, mobile cookie 1, selected by the mobile node.

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 message that need not be present in all HoTI messages. This use of mobility options also allows for future extensions to the format of the HoTI message to be defined. The encoding and format of defined options are described in Section 6.2. The following options are valid in a HoTI message:

- Unique Identifier Option

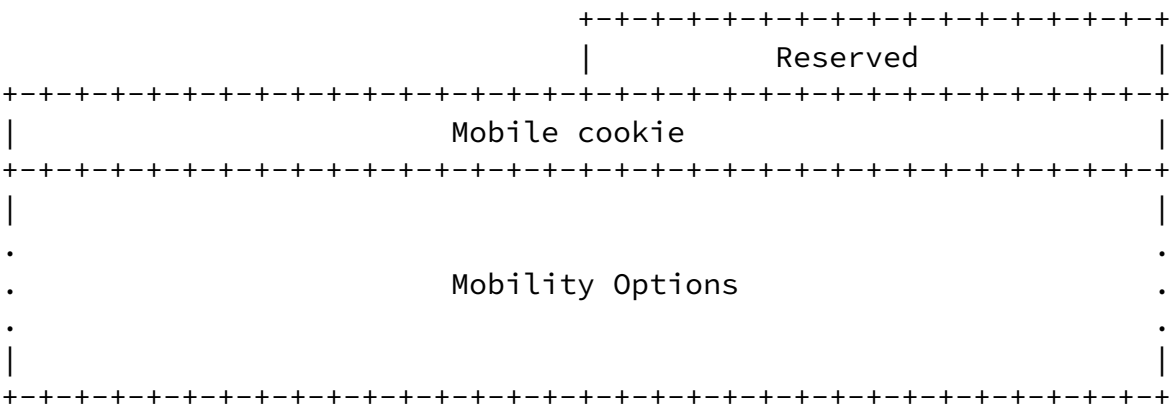
The Header Length field in the Mobility Header for this message MUST be set to 2 (since unit is 8 octets) plus the total length of all mobility options present (also in 8 octet units). If no actual options are present in this message, 4 bytes of padding is necessary.

A packet that includes a HoTI message MUST NOT include a Home Address destination option.

6.1.4. Care-of Test Init (CoTI) Message

The Care-of Test Init (CoTI) message is used to initiate the return routability procedure from the mobile node to a correspondent node (see Section 11.6.2). The purpose of this message is to test the reachability of the care-of address. This message is always sent with the Source Address set to the care-of address of the mobile node, and is sent directly to the correspondent node.

The CoTI 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

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

Mobile cookie

32-bit field which contains a random value, mobile cookie 2, selected by the mobile node.

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 message that need not be present in all CoTI messages. This use of mobility options also allows for future extensions to the format of the CoTI message to be defined. The encoding and format of defined options are described in Section 6.2. The following options are valid in a CoTI message:

- Unique Identifier Option

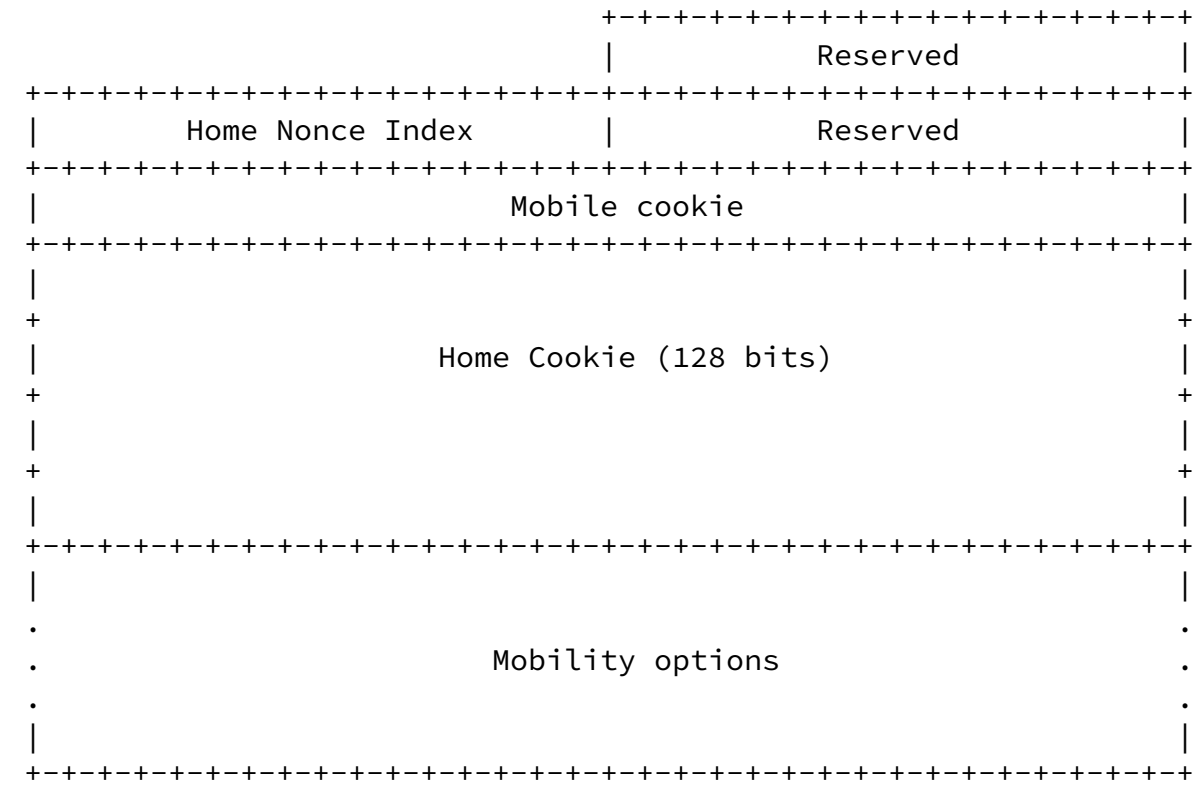
The Header Length field in the Mobility Header for this message MUST be set to 2 (since unit is 8 octets) plus the total length of all mobility options present (also in 8 octet units). If no actual options are present in this message, 4 bytes of padding is necessary.

A packet that includes a CoTI message MUST NOT include a Home Address destination option.

6.1.5. Home Test (HoT) Message

The Home Test (HoT) message is a response to the HoTI message, and is sent from the correspondent node to the mobile node (see Section 8.2). This message is always sent with the Destination Address set to the home address of the mobile node, Source Address set to the address of the correspondent node, and 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 guided by the IPsec Policy Data Base.

The HoT 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:



Reserved

The two 16-bit fields are reserved for future use. These values MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Home Nonce Index

This field will be echoed back by the mobile node to the correspondent node in a subsequent binding update. Strictly speaking, this value is not necessary in the authentication, but allows the correspondent node to efficiently find the nonce value Ni that it used in creating the Home Cookie. Without this field, the correspondent node would have to search through all currently acceptable nonce values when testing for the correctness of the authenticator sent in a Binding Update.

Mobile cookie

32-bit field which contains mobile cookie 1, returned by the correspondent node.

Home Cookie

This field contains the home cookie in the return routability procedure; it is the first of two cookies which are to be processed to form a key which is then used to authenticate a binding update.

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 message that need not be present in all HoT messages. Mobility options are used to carry that information. The encoding and

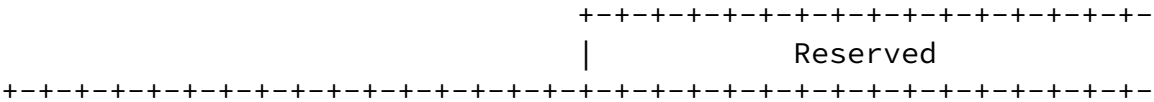
format of defined options are described in Section 6.2. This use of mobility options also allows for future extensions to the format of the HoT message to be defined. This specification does not define any options valid for the HoT message.

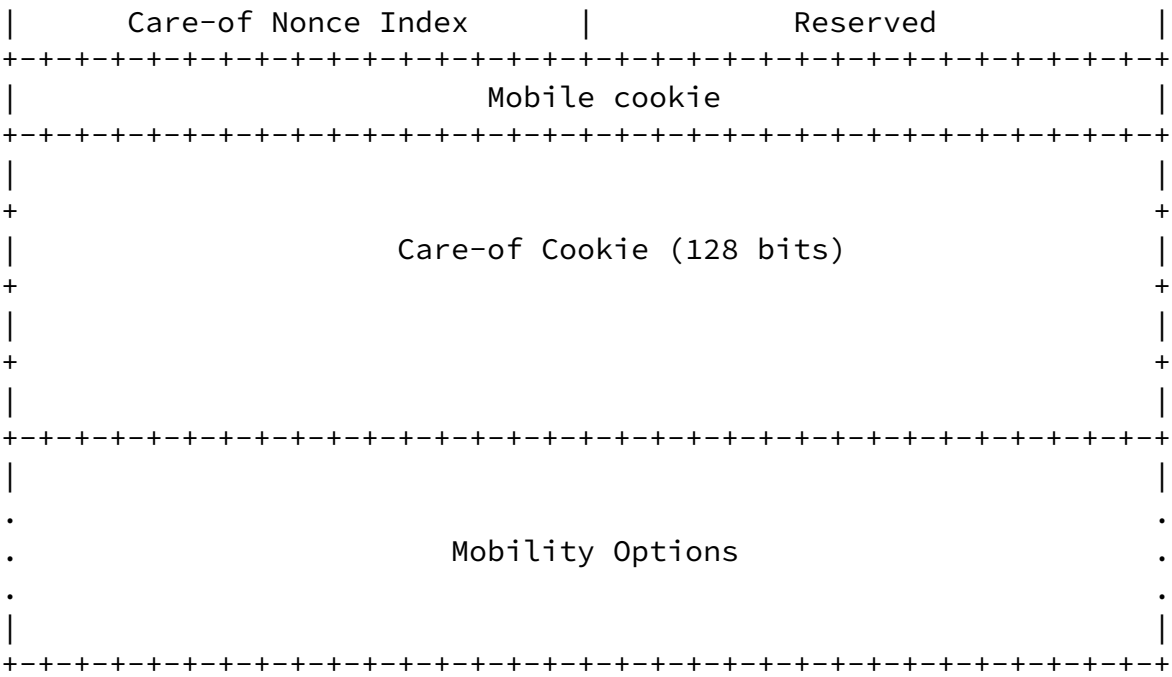
The Header Length field in the Mobility Header for this message MUST be set to 4 (since unit is 8 octets) plus the total length of all mobility options present (also in 8 octet units). If no actual options are present in this message, no padding is necessary.

6.1.6. Care-of Test (CoT) Message

The Care-of Test (CoT) message is a response to the CoTI message, and is sent from the correspondent node to the mobile node (see Section 8.2). This message is always sent with the Source Address set to the address of the correspondent node, the Destination Address set to the care-of address of the mobile node, and is sent directly to the mobile node.

The CoT 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:





Reserved

The two 16-bit fields and the one 32-bit field are reserved for future use. These values MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Care-of Nonce Index

This field will be echoed back by the mobile node to the correspondent node in a subsequent binding update. It will allow the correspondent node to select the appropriate challenge values to authenticate the binding update.

Mobile cookie

32-bit field which contains the mobile cookie 2, returned by the correspondent node.

Care-of Cookie

This field contains the care-of cookie in the return routability procedure; it is the second of two cookies which are to be processed to form a key which is then used to authenticate a binding update.

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.

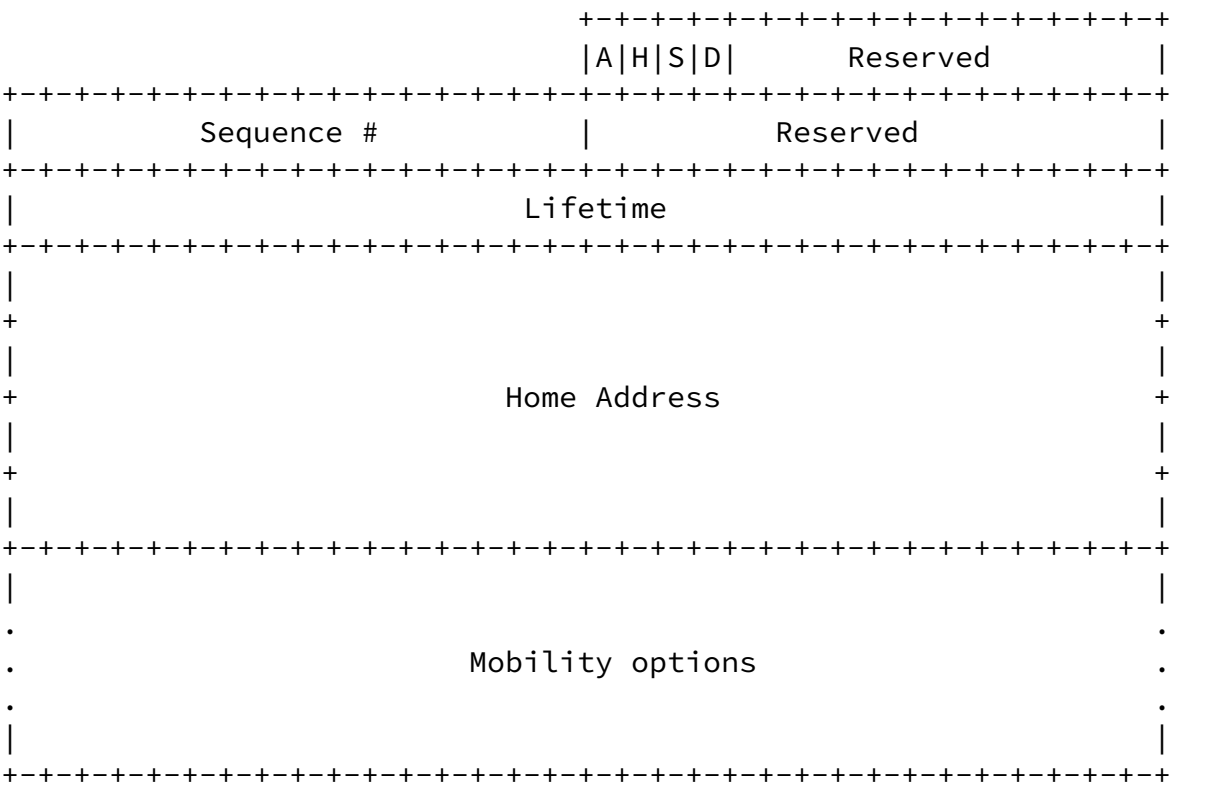
There MAY be additional information, associated with this message that need not be present in all CoT messages. Mobility options are used to carry that information. The encoding and format of defined options are described in Section 6.2. This use of mobility options also allows for future extensions to the format of the CoT message to be defined. This specification does not define any options valid for the CoT message.

The Header Length field in the Mobility Header for this message MUST be set to 4 (since unit is 8 octets) plus the total length of all mobility options present (also in 8 octet units). If no actual options are present in this message, no padding is necessary.

6.1.7. Binding Update (BU) Message

The Binding Update (BU) message is used by a mobile node to notify other nodes of a new care-of address for itself. A packet containing a Binding Update message is sent with the Source Address set to the care-of address of the mobile node and the Destination Address set to the correspondent node's address.

The Binding Update message 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:



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 the `S' 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 10.2.

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 [33] 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. If the Duplicate Address Detection performed by the home agent fails, the Status field in the returned Binding Acknowledgement will be set to 138 (Duplicate Address Detection failed).

Reserved

This field is unused. It 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. Each Binding Update sent by a mobile node MUST use a Sequence Number greater than the Sequence Number value sent in the previous Binding Update (if any) to the same destination address (modulo 2**16, as defined in Section 4.5). 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. A Binding Acknowledgement with Status field set to 141 (Sequence number out of window) will be returned if the value is outside the window. Both home agents and correspondent nodes use the sequence number also to prevent replay attacks.

Lifetime

32-bit unsigned integer. The number of seconds remaining before the binding MUST be considered expired. A value of all one bits (0xffffffff) indicates infinity. A value of zero indicates that the Binding Cache entry for the mobile node MUST be deleted.

Bindings established with correspondent nodes using the return routability procedure MUST NOT exceed MAX_RR_BINDING_LIFE seconds.

Home Address

The home address of the mobile node associated with this Binding Update.

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. A Binding Update sent to a correspondent node MUST include the following options when the return routability procedure is used as the authorization method:

- Nonce Indices option. This option contains information the correspondent node needs in order to find the challenge values Ni and Nj.

- Binding Authorization Data option. This option contains a cryptographic hash value which is used to ensure that

it has been sent by the same party who received the HoT and CoT messages. The authenticator covering a Binding Update MUST be 96 bits and computed over a string of octets containing the following fields of the IPv6 header and the Mobility Header, in order:

* Care-of Address, in the Source Address field of the IPv6 header

* The address of the correspondent node, in the Destination Address field of the IPv6 header.

* The contents of the Mobility Header, excluding the Authenticator field (within the Binding Authorization Data mobility option) which is not included for the purposes of calculating the Authenticator. Options of the Mobility Header are included in the calculation.

The actual authenticator calculation over a sequence of bits is described in Section 5.5.

There MAY be additional information, associated with this Binding Update message, that need not be present in all Binding Updates sent. This use of mobility options also allows for future extensions to the format of the Binding Update message to be defined. The following options are valid in a Binding Update message:

- Unique Identifier option

- Binding Authorization Data option

- Alternate Care-of Address option

The Header Length field in the Mobility Header for this message MUST be set to 4 (since unit is 8 octets) plus the total length of all mobility options present (also in 8 octet units). If no actual options are present in this message, no padding is necessary.

A Binding Update to the home agent MUST include the Home Address destination option in order to allow for the use of manually keyed

IPsec in the protection of these messages. Note also that as described in Section 6.3, the Home Address destination option is not accepted by correspondent nodes that do not have an existing binding with the sender.

When a packet contains both a Home Address destination option and a Binding Update message, the sender MUST use the same address in both. The receiver MUST check for equal values and MUST silently discard a packet that does not pass this test.

The care-of address for the binding given in the Binding Update message is normally that which was received as the value in the Source Address field in the IPv6 header of the packet carrying the Binding Update message. However, a care-of address different from the Source Address MAY be specified by including an Alternate Care-of Address mobility option in the Binding Update message. When such 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 contents of the Nonce Indices and the Authenticator mobility options MUST be based on information gained in this test.

In any case, the care-of address MUST NOT be any IPv6 address which is prohibited for use within a Routing Header; thus multicast addresses, the unspecified address, loop-back address, and link-local addresses are excluded. Binding Updates indicating any such excluded care-of address MUST be silently discarded.

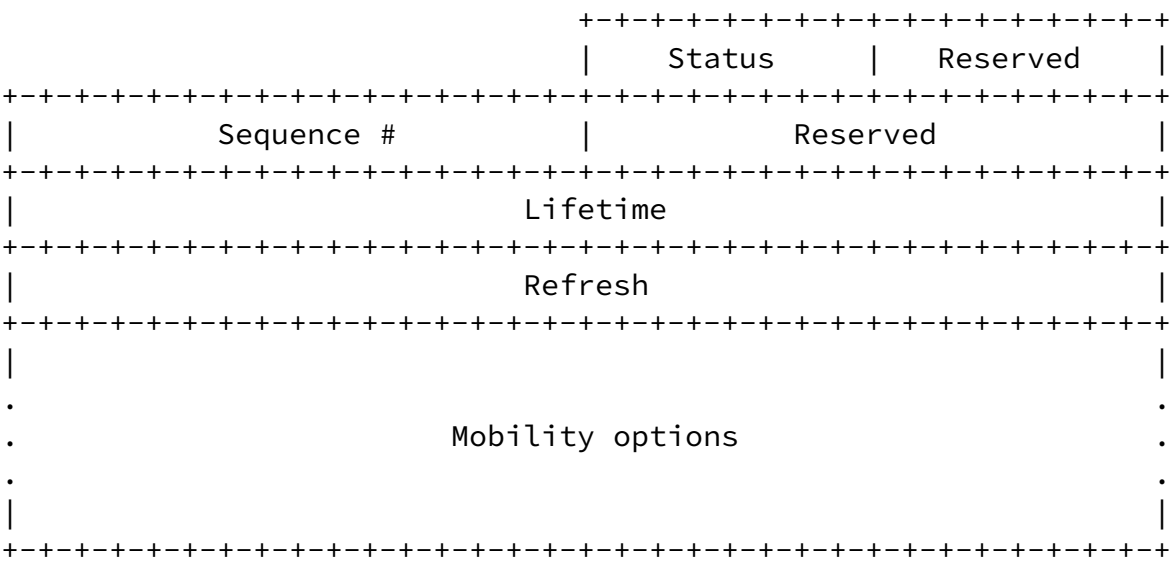
The deletion of a binding can be indicated by setting the Lifetime field to 0 or by setting the care-of address as equal to the home address (the care-of address can be specified either in an Alternate Care-of Address mobility option in the Binding Update message, if present, or in the Source Address field in the packet's IPv6 header).

6.1.8. Binding Acknowledgement (BA) Message

The Binding Acknowledgement message is used to acknowledge receipt of a Binding Update message (Section 6.1.7). When a node receives a packet containing a Binding Update message, with this node being the destination of the packet, this node MUST return a Binding Acknowledgement to the mobile node, if the Acknowledge (A) bit is set in the the Binding Update. The Binding Acknowledgement

message is sent to the Source Address of the Binding Update message which is being acknowledged. The Source Address of the Binding Acknowledgement is the Destination Address from the Binding Update.

The Binding Acknowledgement message 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:



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. The following such Status values are currently defined:

0

Binding Update accepted

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

128

Reason unspecified

130

Administratively prohibited

131

Insufficient resources

132

Home registration not supported

133

Not home subnet

137

Not home agent for this mobile node

138

Duplicate Address Detection failed

141

Sequence number out of window

142

Route optimization unnecessary due to low traffic

143

Invalid authenticator

144

Expired Home Nonce Index

145

Expired Care-of Nonce Index

Up-to-date values of the Status field are to be specified in the most recent "Assigned Numbers" [30].

Sequence #

The Sequence Number in the Binding Acknowledgement is copied from the Sequence Number field in the Binding Update being acknowledged, for use by the mobile node in matching this Acknowledgement with an outstanding Binding Update.

Lifetime

The granted lifetime, in seconds, for which this node SHOULD retain the entry for this mobile node in its Binding Cache. Correspondent nodes should make an effort to honor the lifetimes, since an entry that was garbage collected too early might cause subsequent packets from the mobile node to be dropped, if they contained the Home Address destination option. While this situation is recoverable since an error message is sent to the mobile node, it causes an unnecessary break in the communications.

Mobile nodes SHOULD send a new Binding Update well before the expiration of this period in order to extend the lifetime and not cause a disruption in communications. This is particularly necessary in order to prevent packets from being dropped due to the use of the Home Address destination option without an existing Binding Cache Entry, and the possibility of clock drift.

If the node sending the Binding Acknowledgement is serving as the mobile node's home agent, the Lifetime period also indicates the period for which this node will continue this service; if the mobile node requires home agent service from this node beyond this period, the mobile node MUST send a new Binding Update to it before the expiration of this period (even if it is not changing its primary care-of address), in order

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

Refresh

The recommended interval, in seconds, at which the mobile node SHOULD send a new Binding Update to this node in order to "refresh" the mobile node's binding in this node's Binding Cache. This refreshing of the binding is useful in case the node fails and loses its cache state. The Refresh period is determined by the node sending the Binding Acknowledgement (the node caching the binding). If this node is serving as the mobile node's home agent, the Refresh value may be set, for example, based on whether the node stores its Binding Cache in volatile storage or in nonvolatile storage.

If the node sending the Binding Acknowledgement is not serving as the mobile node's home agent, the Refresh period SHOULD be set equal to the Lifetime period in the Binding Acknowledgement; even if this node loses this cache entry due to a failure of the node, packets from it can still reach the mobile node through the mobile node's home agent, causing a new Binding Update to this node to allow it to recreate this cache

entry. 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 message, that need not be present in all Binding Acknowledgements sent. This use of mobility options also allows for future extensions to the format of the Binding Acknowledgement message to be defined. The following options are valid for the Binding Acknowledgement message:

- Binding Authorization Data option

The Header Length field in the Mobility Header for this message MUST be set to 3 (since unit is 8 octets) plus the total length of all mobility options present (also in 8 octet units). If no actual options are present in this message, 4 bytes of Pad1 or PadN mobility options are needed to make the length of the message a multiple of 8. The Header Length field does include this padding.

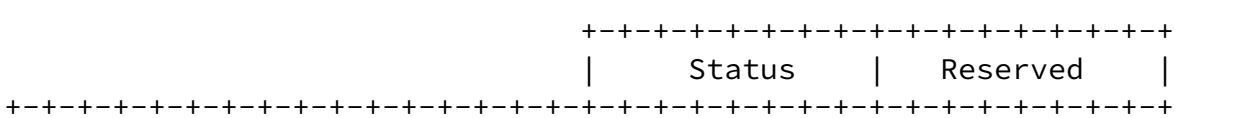
The Binding Acknowledgement is sent to the source address of the Binding Update message, regardless of whether the Binding Update succeeded or failed. No Routing Headers are added to the message.

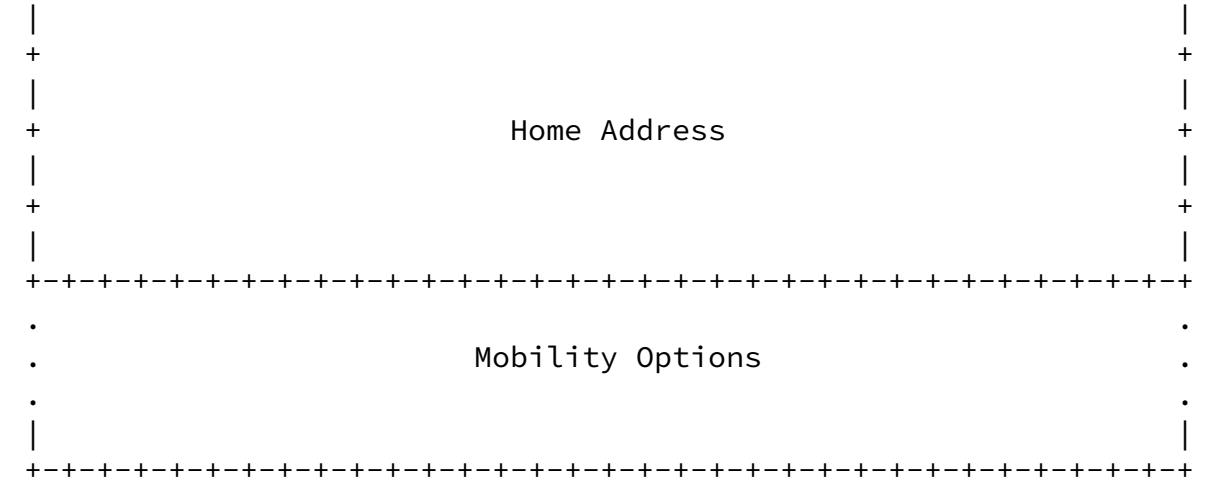
If the mobile node sends a sequence number which is not within the window of acceptable sequence numbers, then the home agent MUST send back a Binding Acknowledgement with status code 141, and the last accepted sequence number in the Sequence Number field of the Binding Acknowledgement message.

6.1.9. Binding Error (BE) 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. A packet containing a Binding Error message is sent to the source address of the offending packet. For instance, in the case of the Home Address destination option error, the packet is the one that contained the Home Address destination option and therefore the Binding Error message is sent to the care-of address of the mobile node. The source address of the Binding Error message is the correspondent node's address.

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

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

1

Home Address destination option used without a binding

2

Received message had an unknown value for the MH Type field

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. This use of mobility options also allows for future extensions to 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.

The Header Length field in the Mobility Header for this message MUST be set to 3 (since unit is 8 octets) plus the total length of all mobility options present (also in 8 octet units). If no actual options are present in this message, no padding is necessary.

6.2. Mobility Options

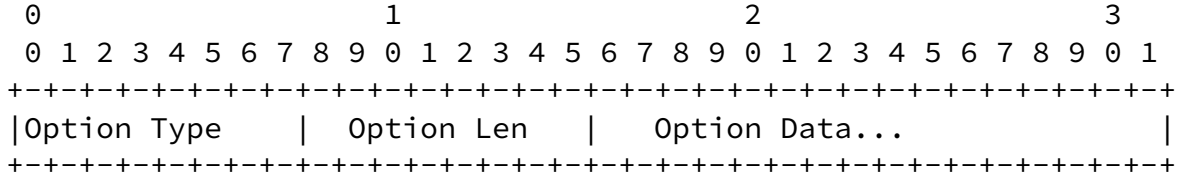
6.2.1. Format

In order to allow optional fields that may not be needed in every use of any given Mobility Header, and to allow future extensions to the format of these messages to be defined, any of the Mobility Header messages defined in this document MAY include one or more mobility options.

Such options are included in the data portion of the message itself, after the fixed portion of the message data specified in section 6.1.

The presence of such options will be indicated by the Header Len of the Mobility Header.

These options are encoded within the remaining space of the message data for that message, using a type-length-value (TLV) format as follows:



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. Length of this mobility option, in octets. The Option Len does not include the length of the Option Type and Option Len fields.

Option Data

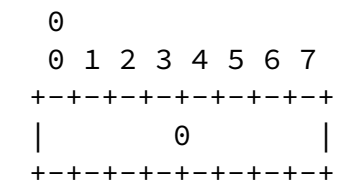
A variable length field that contains data specific to the option.

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:

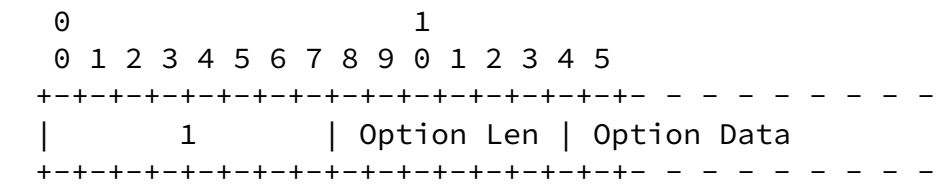


NOTE! the format of the Pad1 option is a special case -- it has neither Option Len nor Option Data fields.

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:

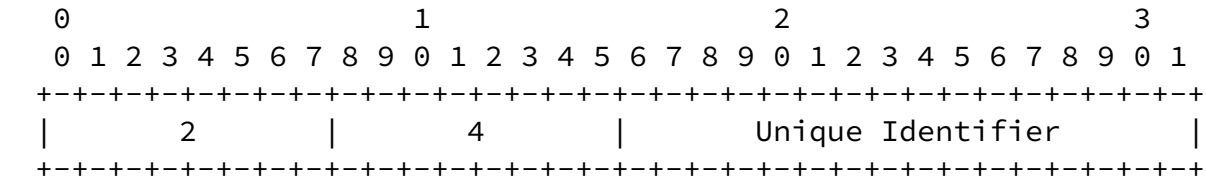


The PadN option is used to insert two or more octets of padding in the Mobility Options area of a Mobility Header message. For N octets

of padding, the Option Len field contains the value N, and the Option Data consists of N-2 zero-valued octets. Option data MUST be ignored by the receiver.

6.2.4. Unique Identifier

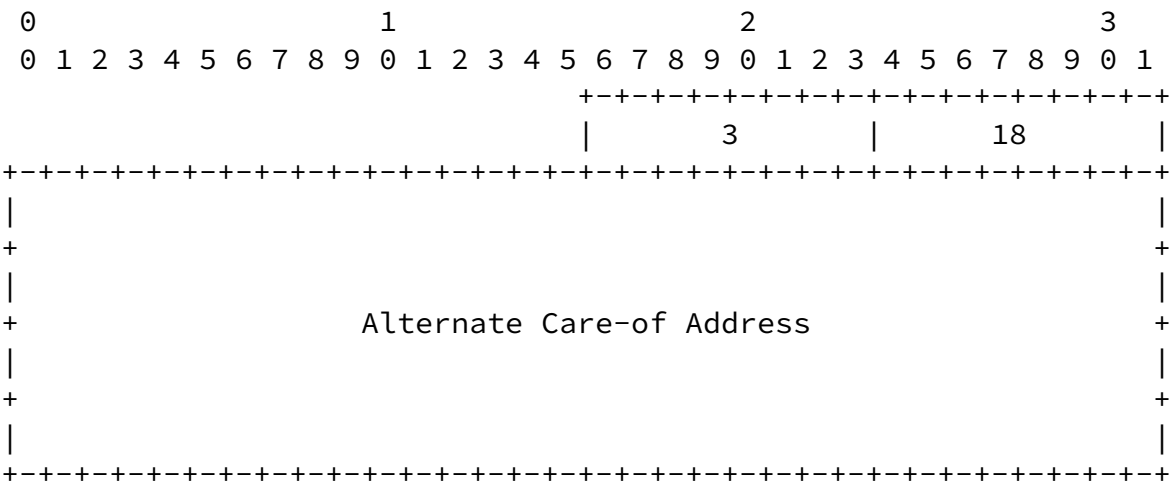
The Unique Identifier option has the alignment requirement of 2n. Its format is as follows:



The Unique Identifier option is valid only in Binding Refresh Request, HoTI, CoTI, and Binding Update messages. The Unique Identifier field contains a 16-bit value that serves to uniquely identify a Binding Request among those sent by this Source Address, and to allow the HoTI, CoTI, and Binding Update to identify the specific Binding Refresh Request to which it responds. This matching of Binding Updates to Binding Refresh Requests is required in the procedure for renumbering the home subnet while a mobile node is away from home (Section 10.9.1).

6.2.5. Alternate Care-of Address

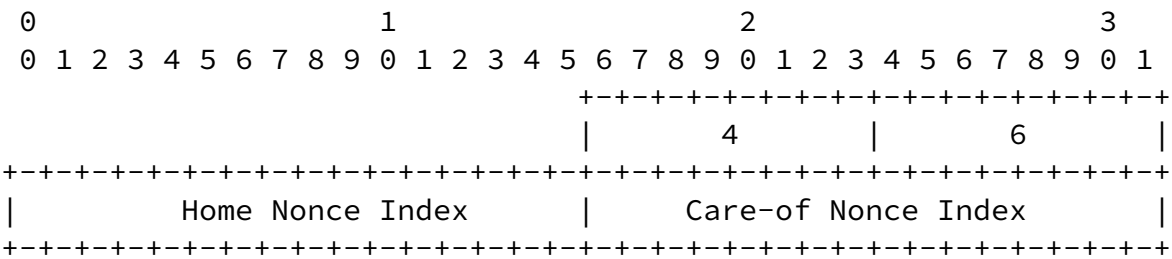
The Alternate Care-of Address option has an alignment requirement of 8n+6. Its format is as follows:



The Alternate Care-of Address option is valid only in Binding Update message. 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.

6.2.6. Nonce Indices

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



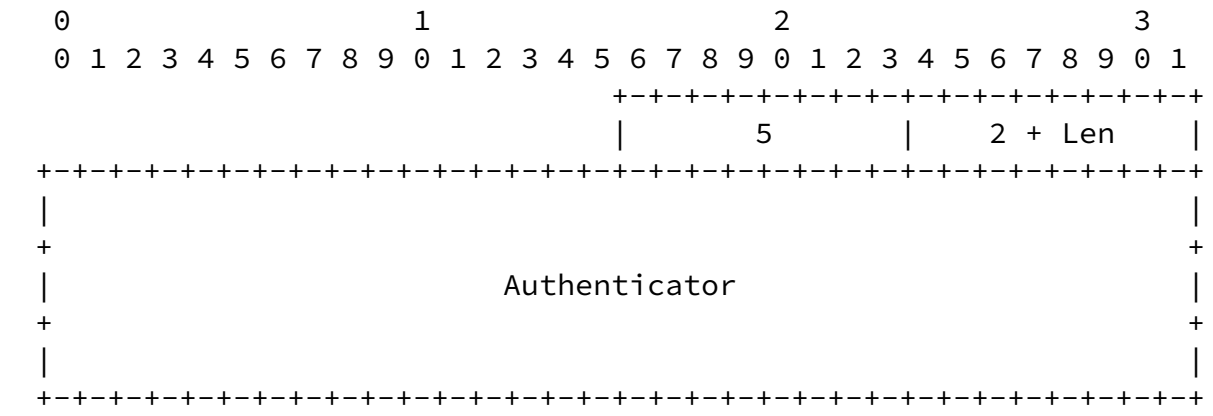
The Nonce Indices option is valid only in the Binding Update message, and only when present together with an Binding Authorization Data option.

The Home Nonce Index field tells the correspondent node that receives the message which of the challenge values (Ni) are to be used to authenticate the Binding Update.

The Care-of Nonce Index field tells the correspondent node that receives the message which of the challenge values (Nj) are to be used to authenticate the Binding Update.

6.2.7. Binding Authorization Data

The Binding Authorization Data option has an alignment requirement of 4n+2. Its format is as follows:



The Binding Authorization Data option is valid only in the Binding Refresh Request, Binding Update, and Binding Acknowledgment messages.

The Option Len field contains the value 2 + Len, where Len is the length of the authenticator in octets.

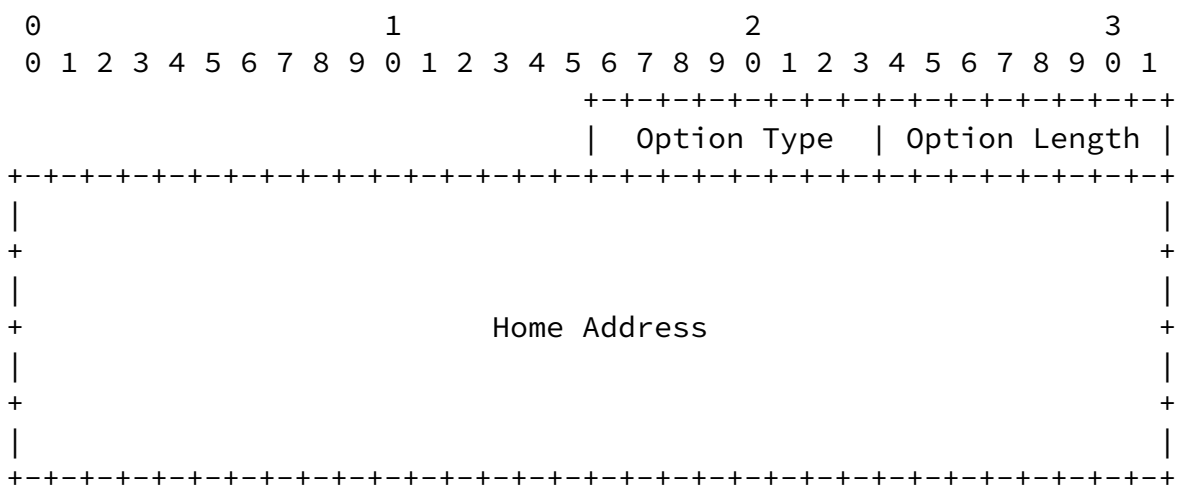
The Authenticator field contains a cryptographic value which can be used to determine that the message in question comes from the right

authority. Rules for calculating this value depend on the used authorization procedure. This specification gives the rules only for the return routability procedure. For this procedure, this option can only appear in a Binding Update message and rules for calculating the Authenticator value are described in Section 6.1.7.

6.3. Home Address Destination Option

The Home Address destination option is used in a packet sent by a mobile node while away from home, to inform the recipient of that packet of the mobile node's home address. For packets sent by a mobile node while away from home, the mobile node generally uses one of its care-of addresses as the Source Address in the packet's IPv6 header. By including a Home Address option in the IPv6 Destination Options header of the packet, the correspondent node receiving the packet is able to substitute the mobile node's home address for this care-of address when processing the packet. This makes the use of the care-of address transparent to the correspondent node above the Mobile IPv6 support level. Note that multicast addresses, link-local addresses, loopback addresses, IPv4 mapped addresses, and the unspecified address, MUST NOT be used within a Home Address option. The Home Address Option MUST not appear more than once in any given packet, except inside the payload part of the packet if tunneling is involved.

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



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.

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) [6]. The alignment requirement [6] for the Home Address option is 8n+6.

The three highest-order bits of the Option Type are encoded to indicate specific processing of the option [6]. For the Home Address option, these three bits are set to 110, indicating that any IPv6 node processing this option that does not recognize the Option Type must discard the packet and, only 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; and that the data within the option cannot change en-route to the packet's final destination.

A packet MUST NOT contain more than one Home Address option, except that an encapsulated packet [4] MAY contain a separate Home Address option associated with each encapsulating IP header.

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

Due to the threat of reflection attacks through the use of this option, this specification requires that packets containing Home Address option MUST be dropped if there is no corresponding Binding Cache Entry for that home address with the currently registered care-of address matching the source address of the packet. If the packet is dropped, the correspondent nodes SHOULD send the Binding

Error message to the source address of the packet that contained the Home Address option (see Section 6.1.9). The Status field in this message should be set to 1. These messages SHOULD be rate-limited.

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. Security issues related to the Home Address option are discussed further in Section 5. 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 11.2.2.

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.

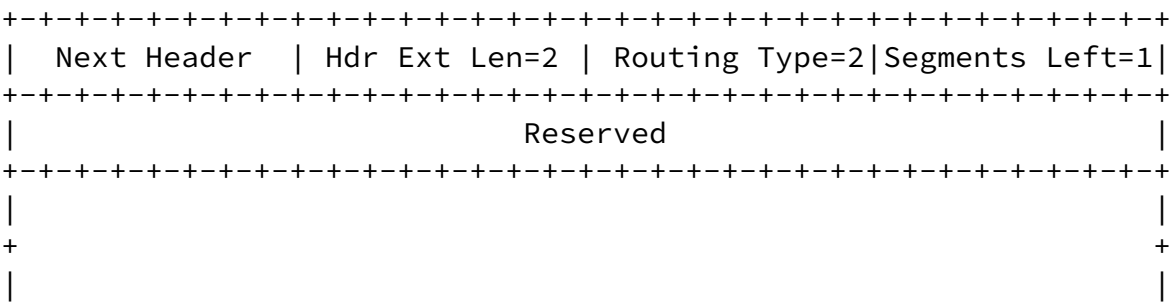
6.4. Routing Header type 2

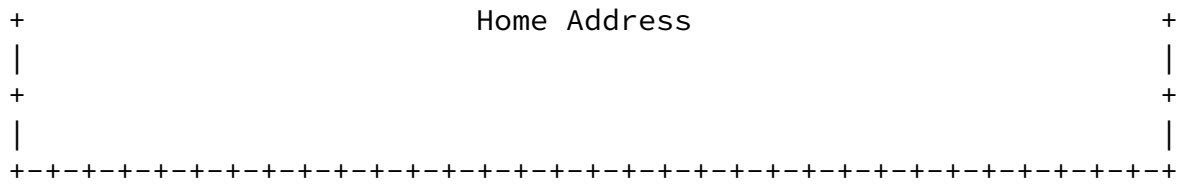
Mobile IPv6 uses a Routing header to carry the Home Address for packets sent from a correspondent node to a mobile node. The Care of Address of the mobile node is carried in the IPv6 destination field.

This uses a different Routing header type than defined for "regular" IPv6 source routing, enabling firewalls to apply different rules to source routed packets than to MIPv6. This Routing header type (Type 2) is restricted to carry only one IPv6 address. All IPv6 nodes 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.

6.4.1. Routing Header Packet format

The Type 2 Routing header has the following format:





Next Header

8-bit selector. Identifies the type of header immediately following the Routing header. Uses the same values as the IPv4 Protocol field [10].

Hdr Ext Len

8-bit unsigned integer. Length of the Routing header in 8-octet units, not including the first 8 octets. For the Type 2 Routing header, Hdr Ext Len is always 2.

Routing Type

8-bit unsigned integer that contains the value 2.

Segments Left

8-bit unsigned integer. Number of route segments remaining; i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination. Packets transmitted through an interface have Segments left is always 1 in this type of Routing header.

Reserved

32-bit reserved field. Initialized to zero for transmission, and ignored on reception.

Home Address

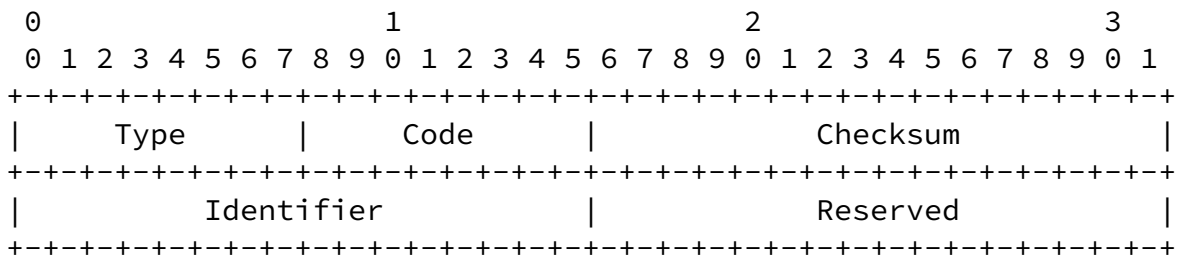
The Home Address of the destination Mobile Node.

The ordering rules for extension headers in an IPv6 packet are described in Section 4.1 of [6]. The new Routing header (Type 2) defined for Mobile IPv6 follows the same ordering as other routing headers. If more than one Routing header (e.g., both a Type 0 and a Type 2 Routing header are present), the Type 2 Routing header should follow all other Routing headers. Otherwise the order of routing headers is independent of their type and follows [6].

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 Sections 10.9 and 11.3.2. The mobile node sends a Home Agent Address Discovery Request message to the "Mobile IPv6 Home-Agents" anycast address for its own home subnet prefix [11], and one of the home agents responds to the mobile node with a Home Agent Address Discovery Reply message, providing a list of the routers on the mobile node's home link serving as home agents.



Type

150 <To Be Assigned by IANA>

Code

0

Checksum

The ICMP checksum [5].

Identifier

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

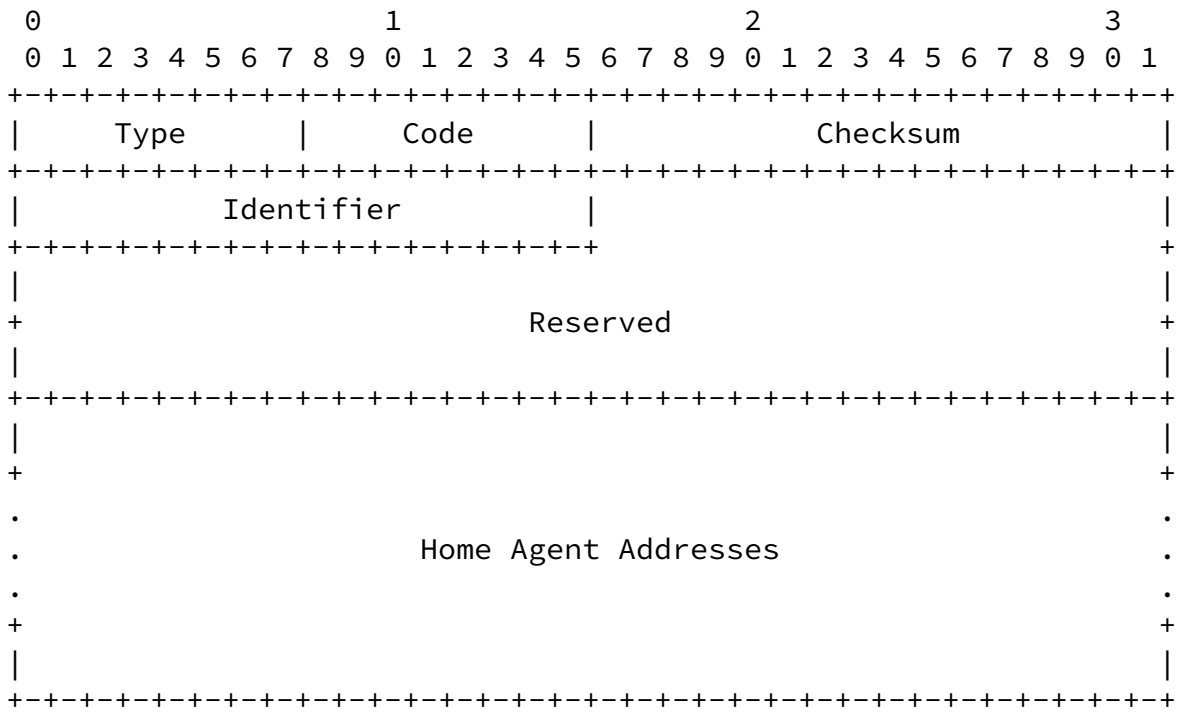
Reserved

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, 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 using the dynamic home agent address discovery mechanism, as described in Sections 10.9 and 11.3.2. The mobile node sends a Home Agent Address Discovery Request message to the "Mobile IPv6 Home-Agents" anycast address for its own home subnet prefix [11], and one of the home agents responds to the mobile node with a Home Agent Address Discovery Reply message, providing a list of the routers on the mobile node's home link serving as home agents.



Type

151 <To Be Assigned by IANA>

Code

0

Checksum

The ICMP checksum [5].

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.

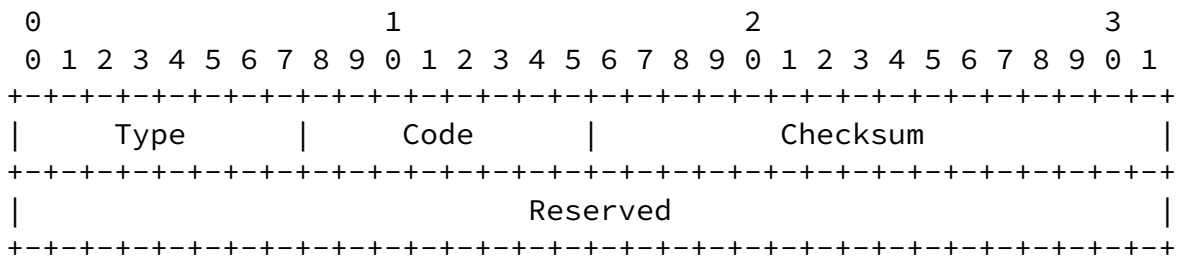
Home Agent Addresses

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 home address(es) by stateless address autoconfiguration [33], or update address(es) according to changes in prefix information supplied by the home agent.

The Mobile Prefix Solicitation is similar to the Router Solicitation used in Neighbor Discovery [20], 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.



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, and this message is routed according to the rules of a typical unicast packet. A hop limit of 64 is currently suggested [30].

Authentication Header

If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include this header. [subject to change]

ICMP Fields:

Type

152 <To Be Assigned by IANA>

Code

0

Checksum

The ICMP checksum [5].

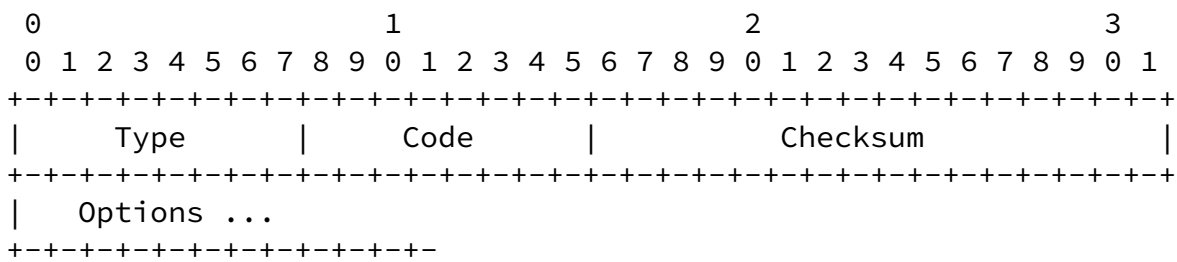
Reserved

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 message 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 10.9.1.



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, the Source Address field from that packet. For unsolicited messages, the mobile node's care-of address SHOULD be used, if it is currently registered with the home agent. Otherwise, the mobile node's home address SHOULD be used.

Authentication Header

An AH header MUST be included unless the mobile node has yet to configure a home address.

ICMP Fields:

Type

153 <To Be Assigned by IANA>

Code

0

Checksum

The ICMP checksum [5].

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 10.9.1 describes which prefixes should be advertised to the mobile node.

The Prefix Information option is defined in Section 4.6.2 of [20], 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 10.9.1.

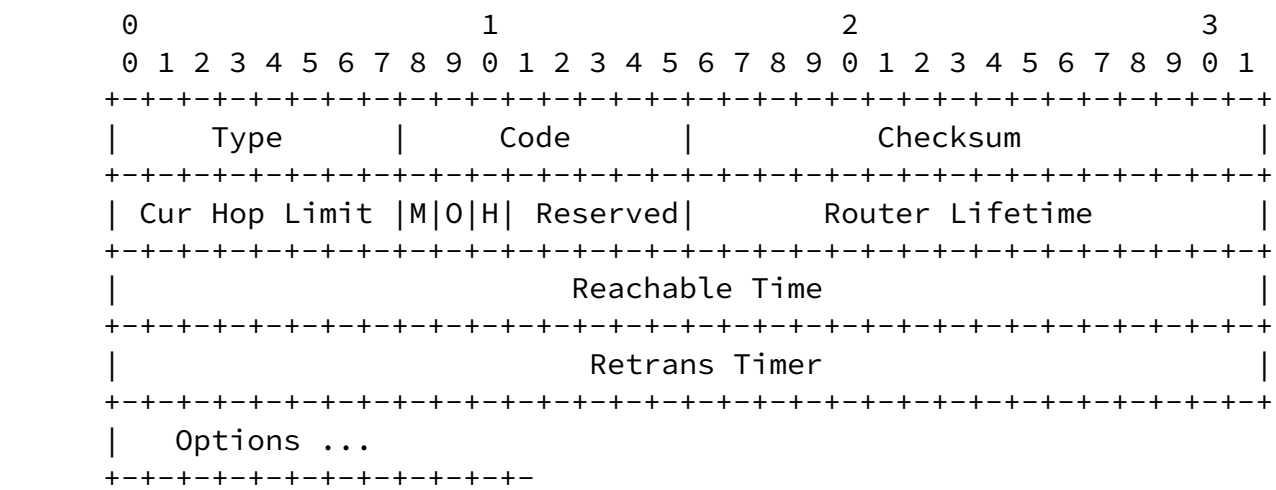
The Mobile Prefix Advertisement sent by the home agent MAY include the Source Link-layer Address option defined in RFC 2461 [20], or the Advertisement Interval option specified in Section 7.3.

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.

7. Modifications to IPv6 Neighbor Discovery

7.1. Modified Router Advertisement Message Format

Mobile IPv6 modifies the format of the Router Advertisement message [20] 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:



This format represents the following changes over that originally specified for Neighbor Discovery [20]:

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 IP home agent on this link.

Reserved

Reduced from a 6-bit field to a 5-bit field to account for the addition of the Home Agent (H) bit.

7.2. Modified Prefix Information Option Format

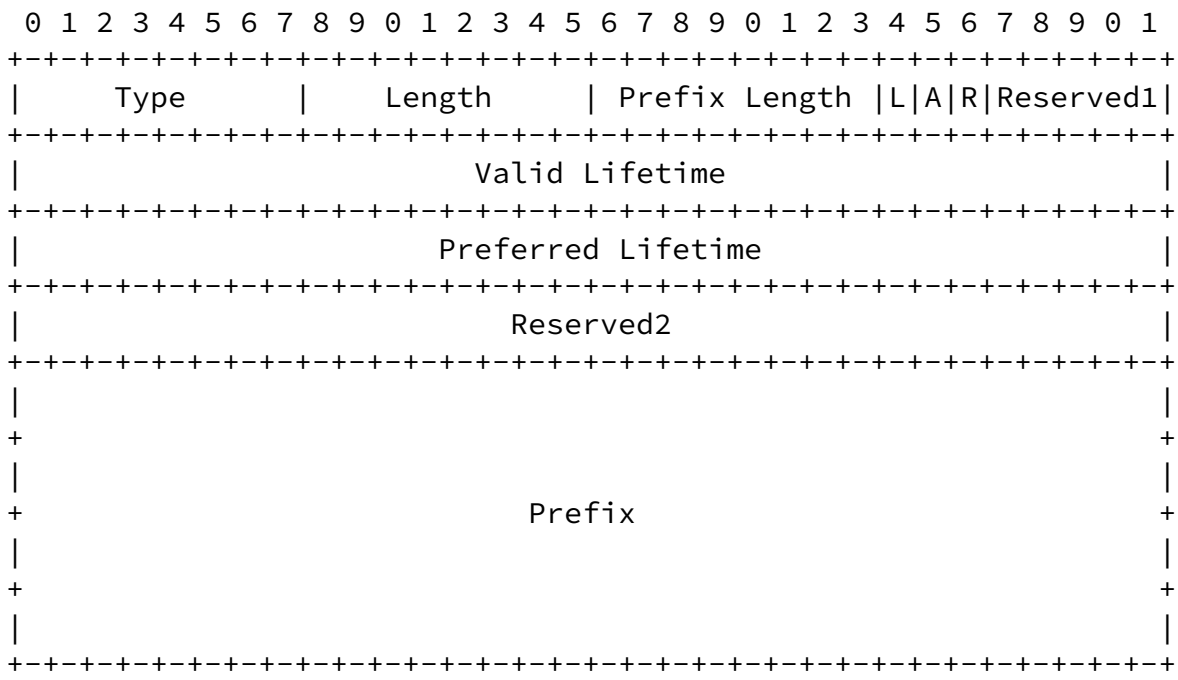
Mobile IPv6 requires knowledge of a router's global address for two reasons:

- To allow a home agent (a router) to learn the address of all other home agents on the link for which it is providing home agent service, for use in building its Home Agents List as part of the dynamic home agent address discovery mechanism (Sections 10.9 and 11.3.2).

- To allow a mobile node to send a Binding Update to a router on the link on which its previous care-of address is located, for purposes of establishing forwarding from this previous care-of address to its new care-of address (Section 11.6.6).

However, Neighbor Discovery [20] 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 easily and efficiently 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:



This format represents the following changes over that originally specified for Neighbor Discovery [20]:

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

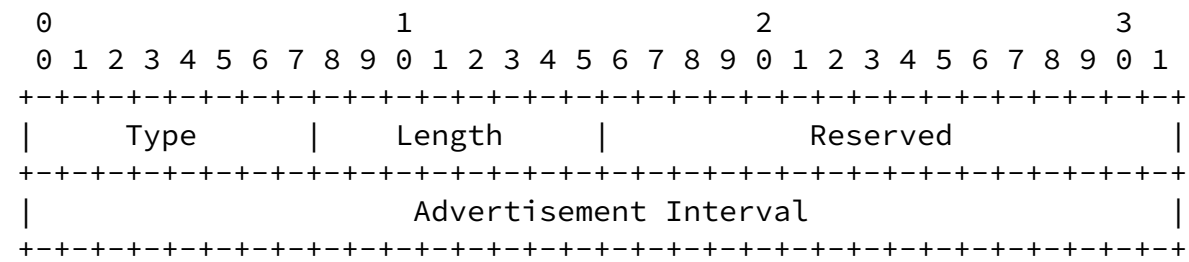
addition of the Router Address (R) bit.

In a solicited Router Advertisement, a home agent MUST, and all other routers SHOULD, 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 [20]. In this case, at least one of these multiple Advertisements being sent instead of a single larger solicited Advertisement, MUST include a Prefix Information option with the Router Address (R) bit set.

All routers SHOULD include at least one Prefix Information option with the Router Address (R) bit set, in each unsolicited multicast Router Advertisement that they send. If multiple Advertisements are being sent instead of a single larger unsolicited multicast Advertisement, at least one of these multiple Advertisements SHOULD include a Prefix Information option with the Router Address (R) bit set.

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:



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

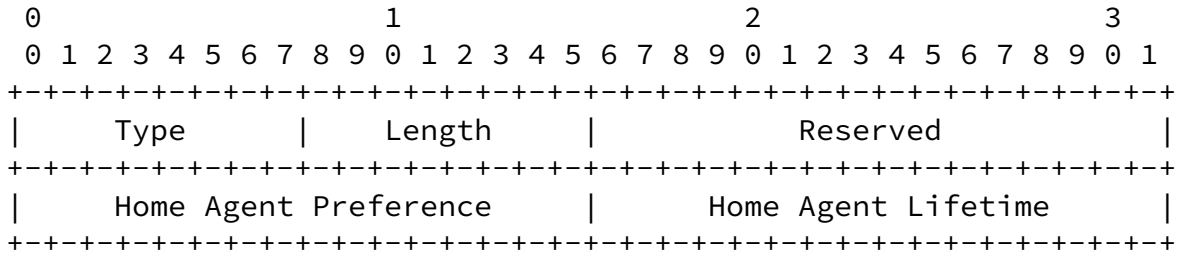
32-bit unsigned integer. The maximum time, in milliseconds, between successive unsolicited router Router Advertisement messages sent by this router on this network interface. Using the conceptual router configuration variables defined by Neighbor Discovery [20], this field MUST be equal to the value 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 11.4.1.

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 Advertisement messages 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:



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, twos-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 8.3. 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 message. 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 [20] 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.

Thus, to provide good support for mobile nodes, Mobile IPv6 relaxes this limit such that routers MAY send unsolicited multicast Router

Advertisements more frequently. In particular, 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), the router 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.

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 backoff 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 it current link, until its movement detection algorithm (Section 11.4.1) determines that it has moved and that its current care-of address might no longer be valid.

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. Further details on this functionality is provided in the following sections.

8.1. Requirements for All IPv6 Hosts and Routers

Since 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, the following requirements apply to ALL IPv6 nodes (whether host or router, whether mobile or stationary):

- Every IPv6 node MUST be able to process a Home Address option received in any IPv6 packet.

- Every IPv6 node SHOULD be able to participate in a return routability procedure, process Binding Update messages, and to return a Binding Acknowledgement option if the Acknowledge (A) bit is set in the received Binding Update.

- Every IPv6 node SHOULD be able to maintain a Binding Cache of the bindings received in accepted Binding Updates.

8.2. Requirements for All IPv6 Routers

The following requirements apply to all IPv6 routers, even those not serving as a home agent for Mobile IPv6:

- Every IPv6 router SHOULD be able to send an Advertisement Interval option in each of its Router Advertisements, to aid movement detection by mobile nodes. 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 'R' bit set and with its full IP address in its router advertisements.

- Filtering routers SHOULD support different rules for Type 0 and Type 2 Routing headers so that filtering of source routed packets (Type 0) will not necessarily limit MIPv6 traffic via Type 2 Routing headers.

8.3. Requirements for 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 capable of serving 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. Each such Binding Cache entry records the mobile node's binding with its primary care-of address and is marked as a "home registration".

- Every home agent MUST be able to intercept packets (using proxy Neighbor Discovery) 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.

- Every home agent MUST be able to encapsulate 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.

- Every home agent MUST support decapsulating 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.

- Every home agent MUST be able to return a Binding Acknowledgement message in response to a Binding Update option received with the Acknowledge (A) bit set.

- 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 Section 4.5.

- 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 [11], and MUST be

able to participate in dynamic home agent address discovery (Section 10.9).

- 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.

- Every home agent SHOULD support sending ICMP Mobile Prefix Advertisements, and SHOULD respond to Mobile Prefix Solicitations.

8.4. Requirements for IPv6 Mobile Nodes

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

- Every IPv6 mobile node MUST be able to perform IPv6 encapsulation and decapsulation [4].

- Every IPv6 mobile node MUST support the return routability procedure and sending Binding Update messages, as specified in Sections 11.6.1, 11.6.2, and 11.6.6; and MUST be able to receive and process Binding Acknowledgement messages, as specified in Section 11.6.3.

- Every IPv6 mobile node MUST support use of the dynamic home agent address discovery mechanism, as described in Section 11.3.2.

- Every IPv6 mobile node MUST maintain a Binding Update List in which it records the IP address of each other node to which it has sent a Binding Update, for which the Lifetime sent in that binding has not yet expired.

- Every IPv6 mobile node MUST support receiving a Binding Refresh Request, by responding with a Binding Update message.

- Every IPv6 mobile node MUST support sending packets containing a Home Address option. This option MUST be included in all packets

sent to a correspondent node when the following three conditions apply: The correspondent node has a binding with this mobile node. The mobile node is away from home. The packet would otherwise have been sent with the mobile node's home address as the IP Source Address.

- Every IPv6 mobile node MUST maintain a Home Agents List, as described in Section 4.5.

- Every mobile node MUST support receiving Mobile Prefix Advertisements and reconfiguring its home address based on the prefix information contained therein.

9. Correspondent Node Operation

This section explains the special processing required for the return routability and binding procedures, as well as to manage the binding cache, handle ICMP messages and send packets to a mobile node.

9.1. Conceptual Data Structures

Each IPv6 node maintains 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 [20]. When sending a packet, the Binding Cache is searched before the Neighbor Discovery conceptual Destination Cache [20] (i.e., 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, as described in Section 9.6, for packets originated by this node, or in Section 10.5, if this node is the mobile node's home agent and the packet was intercepted by it on the home link.

- 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.

- A flag indicating whether or not this Binding Cache entry represents a mobile node that should be advertised as a router in proxy Neighbor Advertisements sent by this node on its behalf.

This flag is only valid if the Binding Cache entry indicates that this is a "home registration" entry.

- The length of the routing prefix for the home address. This field is only valid if the "home registration" flag is set on this Binding Cache 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, and all comparisons between Sequence Number values MUST be performed modulo 2**16. For example, using an implementation in the C programming language, a Sequence Number value A is greater than another Sequence Number value B if ((short)((a) - (b)) > 0), if the "short" data type is a 16-bit signed integer.

- Recent usage information for this Binding Cache entry, as needed

to implement the cache replacement policy in use in the Binding Cache and to assist in determining whether 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. The contents of all of a node's Binding Cache entries, for each of its IPv6 addresses, MUST be cleared when the node reboots.

9.2. Receiving Packets from a Mobile Node

Packets sent by a mobile node with either a Home Address destination option or a Mobility Header (or both) require special processing at the correspondent node as explained below.

9.2.1. Processing Mobility Header (MH) Messages

All IPv6 correspondent nodes MUST observe the following rules when processing Mobility Header messages:

1. If an MH message of unknown type is received (Section 6.1, the correspondent node SHOULD issue a Binding Error message to the packet's Source Address with Status field set to 2. Finally, the correspondent node MUST discard the packet.

2. If the "Next Header" field is not NO_NXTHDR (59 decimal), the packet MUST be silently discarded.

3. The checksum must be verified as per Section 6.1.

Subsequent checks depend on the particular Mobility Header message. There are two types of Mobility Header messages. The return

routability procedure (Section 9.3) is used to verify liveness of the mobile node at both its home address as well as its care-of address. These liveness probes are used to secure binding updates.

The other type of Mobility Header messages are directly concerned with managing bindings (Section 9.4).

9.2.2. Receiving Packets with Home Address Destination Option

Packets sent by a mobile node while away from home MAY include a Home Address destination option, if the correspondent node has a Binding Cache Entry for that home address. It MUST process the option in a manner consistent with exchanging the Home Address field from the Home Address option into the IPv6 header, replacing the original value of the Source Address field there. However, any actual modifications to the Source Address field in the packet's IPv6 header MUST be carried out in such a fashion that further processing of such a packet after all IPv6 options processing (e.g., at the transport layer) does not depend on that information to know that the original Source Address was a care-of address, or that the Home Address option was used in the packet.

Since the sending mobile node uses its home address at the transport layer when sending such a packet, the use of the care-of address and Home Address option is transparent to both the mobile node and the correspondent node above the level of the Home Address option generation and processing.

Packets containing Home Address Option MUST be dropped if there is no corresponding Binding Cache Entry for that home address. In this case, the correspondent nodes SHOULD send the Binding Error message to the source address of the packet that contained the Home Address Option (see Section 6.1.9).

9.3. Return Routability Procedure

A correspondent node engages in the return routability procedure in order to secure a subsequent Binding Update. This is a requirement in order to authorize the creation of new bindings as well as to refresh existing ones. In particular, these messages are used to establish the mobile node's liveness (responsiveness to packets) at both its care-of address as well as its home address.

9.3.1. Receiving HoTI Messages

The HoTI message initiates the return routability procedure from the mobile node's home address to the correspondent node.

The correspondent node verifies the following:

- MH Type field for this message is 1.
- The Header Extension Length field MUST be greater than or equal to the length specified in Section 6.1.3.
- The packet MUST NOT include a Home Address destination option.

In preparation for sending the corresponding HoT Message, the correspondent node checks that it has the necessary material to engage in a return routability procedure, as specified in Section 5.5. For that procedure, the correspondent node MUST have a secret Kcn and a nonce Nj. If it does not have this material yet, it MUST produce it before continuing with the return routability procedure.

Section 9.3.3 specifies further processing.

9.3.2. Receiving CoTI Messages

The CoTI message initiates the return routability procedure from the mobile node's care-of address location to the correspondent node.

The correspondent node verifies the following:

- MH Type field for this message is 2.
- The Header Extension Length field MUST be greater than or equal to the length specified in Section 6.1.4.
- The packet MUST NOT include a Home Address destination option.

In preparation for sending the corresponding CoT Message, the correspondent node checks that it has the necessary material to engage in a return routability procedure, as specified in Section 5.5. For that procedure, the correspondent node MUST have a secret Kcn and a nonce Nl. If it does not have this material yet, it MUST produce it before continuing with the return routability procedure.

Section 9.3.4 specifies further processing.

9.3.3. Sending HoT Messages

Unless already created, the correspondent node creates a "Home Cookie" and an associated "Home Nonce Index". It then creates a HoT message (Section 6.1.5) and sends it to the mobile node at the latter's home address.

9.3.4. Sending CoT Messages

Unless already created, the correspondent node creates a "Care-of Cookie" and an associated "Care-of Nonce Index". It then creates a CoT message (Section 6.1.6) and sends it to the mobile node at the latter's care-of address.

9.4. Processing Bindings

This section explains how the correspondent node processes the binding cache messages. These messages are:

- Binding Update
- Binding Refresh Request
- Binding Acknowledgement
- Binding Error

9.4.1. Receiving Binding Updates

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

- The packet MUST NOT contain a Home Address option.

- The Header Len field in the Binding Update option is greater than or equal to the length specified in Section 6.1.7.

- The Sequence Number field in the Binding Update message is greater than the Sequence Number received in the previous Binding Update for this home address, if any. As noted in Section 5.5, this Sequence Number comparison MUST be performed modulo 2**16.

- The packet meets the specific authentication requirements for Binding Updates, defined in Section 5.5.

When the return routability procedure is used as an authorization method, the following are also required:

- The correspondent node MUST re-generate the Home Cookie and the Care-of Cookie from the information contained in the packet. It then generates the session key Kbu and uses it to verify the authenticator field in the Binding Update as specified in Section 6.1.7. 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 message. 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 Home and Care-of Nonce Index values in the Nonce Indices mobility option are recognized by the correspondent node. As described in Section 5.5, the correspondent node discards Nonce values that are too old.

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 141, and the last accepted sequence number in the Sequence Number field of the Binding Acknowledgement.

If the mobile node sends a Home or Care-of Nonce Index value which is no longer recognized by the correspondent node, then the receiving node MUST send back a Binding Acknowledgement with status code 144 or 145, respectively.

Any Binding Update which fails to satisfy all of these tests for any reason other than insufficiency of the Sequence Number or Nonce Indices MUST be silently ignored, and the packet carrying the Binding Update MUST be discarded.

In this section, the care-of address refers to the IPv6 address, which was originally located in the IPv6 header when the packet was transmitted by the mobile node.

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 10.2; otherwise, it is processed according to the procedure specified in Section 9.4.2.

- 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. 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; otherwise, it is processed according to the procedure specified in Section 9.4.3.

9.4.2. Requests to Cache a Binding

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 9.4.1. 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 Binding Cache entry records the association between this home address and the care-of address for the binding. 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 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.

9.4.3. Requests to Delete a Binding

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 9.4.1. 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.

In order to prevent replayed binding updates after a binding cache entry has been deleted the correspondent node needs to make sure that the nonce indices used to create the binding are no longer valid.

This applies whether the binding is deleted due to it timing out (lifetime expiry) or being deleted explicitly by the mobile node.

If a binding cache entry is logically deleted and either the home nonce index or the care-of nonce index used to create (or last update) the binding are still valid, the correspondent node must behave as if it retains the state about the binding (including the

sequence number) until at least one of the cookies has become too old.

A possible way to implement this is to mark the binding cache entry so that it does not effect sending and receiving of packets, but so that it is found when a binding update is received. Another way is to mark the used nonces immediately too old. However, this method may cause some unnecessary failures and retries with ongoing return routability procedures with other mobile nodes. Furthermore, unless the mobile node has requested a Binding Acknowledgement, it is possible that this method may even cause an error in the return routability procedure procedure to go unnoticed, and data packets to be dropped through the use of the Home Address destination option without an existing binding. The effect is similar to packet loss during the return routability procedure, but may in certain circumstances significantly increase the problems.

9.4.4. Sending Binding Acknowledgements

When any node receives a packet containing a Binding Update message in which the Acknowledge (A) bit is set, it MUST return a Binding Acknowledgement message acknowledging receipt of the Binding Update. If the node accepts the Binding Update and creates or updates an entry in its Binding Cache for this binding, the Status field in the Binding Acknowledgement MUST be set to a value less than 128; if, on the other hand the Binding Update is accepted and the `A' bit is not set, the node SHOULD NOT send a Binding Acknowledgement. If the node rejects the Binding Update and does not create or update an entry for this binding, a Binding Acknowledgement MUST be sent even if the `A' bit was not set, and the Status field in the Binding Acknowledgement MUST be set to a value greater than or equal to 128. Specific values for the Status field are described in Section 6.1.8 and in the most recent "Assigned Numbers" [10].

The packet in which the Binding Acknowledgement is returned MUST meet the specific authentication requirements for Binding Acknowledgements, defined in Section 5.5. Furthermore, if the packet is to be sent to the mobile node at any address other than the mobile node's home address, it MUST be sent using a Routing header (even if the binding was rejected). The intermediate IP address, to which the packet will be delivered immediately before the home address, is determined as follows:

- Whenever the Binding Update is accepted with a nonzero lifetime, the routing header will be constructed using the care-of address as described in Section 9.6.

- Otherwise, if the Source IP Address of the packet containing the Binding Update, is legal for inclusion in a Routing Header, the routing header will be constructed using that IP address. Note that multicast addresses, link-local addresses, loopback addresses, IPv4 mapped addresses, and the unspecified address, MUST NOT be used within a Routing Header for the Binding Acknowledgement.

Otherwise, if the Binding Update has a zero lifetime but the Source IP address is not allowable for use within the Routing Header, the Binding Acknowledgment MUST be sent to the mobile node's home address.

9.4.5. Sending Binding Refresh Requests

Entries in a node's Binding Cache MUST be deleted when their lifetime expires. If such an entry 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, where it will be intercepted and tunneled to the mobile node. The mobile node will then return a Binding Update to the sender, allowing it to create a new Binding Cache entry for sending future packets to the mobile node. Communication with the mobile node continues uninterrupted, but the forwarding of this packet through the mobile node's home agent creates additional overhead and latency in delivering packets to the mobile node. Such routing paths could, for instance, temporarily or permanently disrupt any negotiated Quality of Service reservations which had been made by the mobile node on its home network.

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. When the mobile node receives a packet from some sender containing a Binding Refresh Request option, it MAY start a return routability procedure, if necessary, before sending its current binding and a new lifetime in a new Binding Update.

The correspondent node MAY retransmit Binding Refresh Request messages provided that rate limitation is applied. The correspondent node SHOULD stop retransmitting when it receive a Home Test Init

message, as the mobile node is responsible for retransmissions during the return routability procedure.

9.4.6. Sending Binding Error Messages

If the correspondent node receives a packet with a Home Address destination option it MUST verify that it has a binding for that mobile node. Specifically, it MUST have a binding entry for the mobile node's home address (as obtained from the Home Address option) at the mobile node's care-of address (from the IP source address of the packet). If the correspondent node does not find such a binding entry, it MUST discard the packet and return a Binding Error message (Section 6.1.9).

9.5. 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 10.2) 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), just as if the mobile node had de-registered its primary care-of address (see Section 10.3).

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 node MUST reject the Binding Update and MUST return a Binding Acknowledgement to the sending mobile node, in which the Status field is set to 131 (insufficient

resources). When otherwise attempting to add a new entry to its Binding Cache, a node MAY, if needed, choose to drop any entry already in its Binding Cache, other than "home registration" entries, in order to make space for the 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.

Any binding dropped from a node's Binding Cache due to lack of cache space will be rediscovered and a new cache entry created, if the binding is still in active use by the node for sending packets. 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 normally,

leading to the mobile node's home link. There, the packet will be intercepted by the mobile node's home agent and tunneled to the mobile node's current primary care-of address. This indirect routing to the mobile node through its home agent will result in the mobile node sending a Binding Update to this sending node when it receives the tunneled packet, allowing it to again add an entry for this destination mobile node to its Binding Cache.

9.6. 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 Routing header to route the packet to this mobile node (the destination node) by way of the care-of address in the binding recorded in that Binding Cache entry. For example, assuming use of a Type 2 Routing header (see Section 6.4), if no other use of a Routing header is involved in the routing of this packet, 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 care-of address copied from the Binding Cache entry.

- The Routing header is initialized to contain a single route

segment, with an Address of the mobile node's home address (the original destination address to which the packet was being sent).

Following the definition of a Type 2 Routing header 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 (using IPv6 encapsulation [4]) to the mobile node's current primary care-of address, as described in Section 10.5. The mobile node MAY then send

a Binding Update to the sending node, as described in Section 11.6.2, allowing the sending node to create a Binding Cache entry for its use in sending subsequent packets to this mobile node.

9.7. Receiving ICMP Error Messages

When a correspondent node sends a packet to a mobile node, if the correspondent node has a Binding Cache entry for the destination address of the packet, then the correspondent node uses a Routing header to deliver the packet to the mobile node through the care-of address in the binding recorded in the Binding Cache entry. Any ICMP error message caused by the packet on its way to the mobile node will be returned normally 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 to the mobile

node's home link. There, it will be intercepted by the mobile node's home agent, encapsulated, and tunneled to the mobile node's primary care-of address. 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 (the source of the tunnel). By the definition of IPv6 encapsulation [4], the home agent (as the encapsulating node) MUST relay certain ICMP error messages back to the original sender of the packet, which in this case is the correspondent node.

Likewise, if a packet for a mobile node arrives at the mobile node's previous link and is intercepted there by a home agent for the mobile node's previous care-of address as described in Section 11.6.6 (e.g., the mobile node moved after the packet was sent), that home agent will encapsulate and tunnel the packet to the mobile node's new care-of address. As above, any ICMP error message caused by the packet while in this tunnel will be returned to that home agent (the source of the tunnel), which MUST relay certain ICMP error messages back to the correspondent node [4]. The relayed packet MUST NOT contain a routing header entry with the care-of address of the mobile 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. If the correspondent node subsequently transmits another packet to the mobile node, the packet will be routed to the mobile node's home link, intercepted by the mobile node's home agent, and tunneled to the mobile node's primary care-of address using IPv6 encapsulation. The mobile node will then return a Binding Update to

the correspondent node, allowing it to recreate a (correct) Binding Cache entry for the mobile node.

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. In addition, if an entry in a node's Binding Cache for which the node is serving as a home agent is marked as a "home registration" entry, it SHOULD NOT be deleted by the home agent until the expiration of its binding lifetime.

The Home Agents List is maintained by each home agent (as well as each mobile node), recording information about each home agent from which this node has received a Router Advertisement in which the Home Agent (H) bit is set, for which the remaining lifetime for this list entry (defined below) has not yet expired. The home agents list is thus similar to the Default Router List conceptual data structure maintained by each host for Neighbor Discovery [20], although 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; this list is used by a home agent in the dynamic home agent address discovery mechanism. Each mobile node, while away from home, also maintains a Home Agents List, to enable it to notify a home agent on its previous link when it moves to a new link; a mobile node MAY maintain a separate Home Agents List for each link to which it is (or has recently) connected, or it MAY maintain a single list for all links. Each Home Agents List entry conceptually contains the following fields:

- The link-local IP address of a router on the link, that this node currently believes is operating as a home agent for that link. A new entry is created or an existing entry is updated in the Home Agents List in response to receipt of a valid Router Advertisement in which the Home Agent (H) bit is set. The link-local address of the home agent is learned through the Source Address of the Router Advertisements received from it [20].

- One or more global IP addresses for this home agent, 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 [20].

Are there interactions with the new Router Advertisement stuff?

- 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. The Home Agents List entry lifetime is decremented until it reaches zero, at which time this 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 (a signed, twos-complement integer) 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 returned in an ICMP Home Agent Address Discovery message in response to a mobile node's initiation of dynamic home agent address discovery. A mobile node uses this preference in determining which of the home agents on its previous link to notify when it moves to a new link.

Can we delete the preference stuff? Is anyone using it?

10.2. 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 9.4.1. This section describes the processing of a valid Binding Update that requests the receiving node to serve as its home agent, registering its 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 132 (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 133 (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, and the value of the Home Address field in this option MUST correspond to the Home Address field in the Binding Update.

- Finally, if the Duplicate Address Detection (D) bit is set in the Binding Update, this home agent MUST perform Duplicate Address Detection [33] 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 can possibly use the mobile node's home address. The address used for Duplicate Address Detection SHOULD be the mobile node's link-local address. 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 [20, 33]; however, in this case, 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 138 (Duplicate Address Detection failed). When the home agent sends a successful Binding Acknowledgement to the mobile node, in response to a Binding Update with the `D' bit set, 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 mobile node transmits Binding Updates with new care-of

addresses for that home address.

If the home agent does not reject the Binding Update, then it becomes or remains the home agent for the mobile node. The home agent 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 of the mobile node is taken to be the value which, when the packet was originally received, was located in the Home Address field in the packet's Home Address option. The care-of address for this Binding Cache entry is taken to be the value which, when the packet was originally received, was located either in the Alternate Care-of Address option in the Binding Update option, if present, or from the Source Address field in the packet's IPv6 header, otherwise.

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 9.5) and MUST NOT be removed from the Binding Cache until the expiration of the Lifetime period.

If the `S' bit field in the Binding Update is zero, The home agent creates or updates 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 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 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 remaining valid lifetime for the subnet prefix in the mobile node's home address specified with the Binding Update, and MUST NOT be greater than the Lifetime value specified in 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 [20].

- , However, if the `S' bit field in the Binding Update is zero, the lifetime for the each 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 '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.

- The Refresh field MUST be set to a value less than or equal to the Lifetime value being returned in the Binding Update. If the home agent stores the Binding Cache entry in nonvolatile storage (that survives the crash or other failure of the home agent), then the Refresh field SHOULD be set to the same value as the Lifetime field; otherwise, the home agent MAY set the Refresh field to a value less than the Lifetime field, to indicate that the mobile node SHOULD attempt to refresh its home registration at the indicated shorter interval (although the home agent will still retain the registration for the Lifetime period, even if

the mobile node does not refresh its registration within the Refresh period).

In addition, the home agent MUST follow the procedure defined in Section 10.4 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 10.6. Finally, the home agent MUST also propagate new home network prefixes, as described in Section 10.9.1.

10.3. Primary Care-of Address De-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 9.4.1. 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 137 (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, and proceed as follows.

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 Refresh field MUST be set to zero.

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).

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 9.4.4.

10.4. Intercepting Packets for a Mobile Node

While a node is serving as the home agent for mobile node (while the node has an entry in its Binding Cache for this mobile node that is marked as a "home registration"), this node 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 [4].

In order to intercept such packets on the home link, when a node begins serving as the home agent for some mobile node (it did not already have a Binding Cache entry for this mobile node marked as a "home registration"), then the home agent MUST multicast onto the home link a "gratuitous" Neighbor Advertisement message [20] on behalf of the mobile node. Specifically, the home agent performs the following steps:

- The home agent examines the value of the `S' bit in the new "home registration" Binding Cache entry. If this bit is nonzero, the following step is carried out only for the individual home address specified for this binding. If, instead, this bit is zero, then the following step is carried out for each address for the mobile node formed from the interface identifier in the mobile node's home address in this binding (the remaining low-order bits in the address after the configured subnet prefix), together with each one of the subnet prefixes currently considered by the home agent to be on-link (including both the link-local and site-local prefix).

- For each specific IP address for the mobile node determined in the first step above, the home agent sends a Neighbor Advertisement message [20] 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 [20], with the following exceptions:

  * The Target Address in the Neighbor Advertisement message 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 message.

  * 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 for the mobile node normally destined to this address instead 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 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 [20].

While a node is serving as a home agent for some mobile node (it still has a "home registration" entry for this mobile node in its Binding Cache), the home agent uses IPv6 Neighbor Discovery [20] 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 Solicitation messages for it. When a home agent receives a Neighbor Solicitation message, 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 messages with the `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 message with a Neighbor Advertisement message, 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 copied from the corresponding bit in the home agent's Binding Cache entry for the mobile node. 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 [20].

10.5. 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 9.6 apply. The home agent (as a correspondent node) uses a Routing header to route the packet to the mobile node by way of the care-of address in the home agent's Binding Cache (the mobile node's primary care-of address, in this case).

While the mobile node is away from home and this node is acting as the mobile node's home agent, 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 Prefix Length field was nonzero in the Binding Update), as described in Section 10.4. The home agent cannot use a Routing header to forward these intercepted packets to the mobile node, since it cannot modify the packet in flight without invalidating any existing IPv6 AH [12] or ESP [13] header present in the packet.

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 [4]; the tunnel entry point node is the home agent, and the tunnel exit point node is the primary care-of address as registered with the home agent. 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 (using its primary care-of address), normal processing of the tunnel header [4] 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 [9], 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) [9], to which the mobile node is subscribed, SHOULD be tunneled to the mobile node by default, but this behavior MUST be configurable to disable it; this default behavior might change at some point in the future as the definition of these scopes become more completely defined in IPv6.

10.6. 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. This tunnel extends between the mobile node and the home agent. Home agents MUST support reverse tunneling as follows:

- The tunneled traffic arrives to the home agent using IPv6 encapsulation [4].

- 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 verifies that the Source Address in the tunnel IP header is the mobile node's primary care-of address.

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. In any case, the home agent MUST check that the source address in the tunneled packets corresponds to the currently registered location of the mobile node, as otherwise any node in the

Internet could send traffic through the home agent and escape ingress filtering limitations.

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.

10.7. Protecting Return Routability Packets

The return routability procedure described in Section 5 assumes that the confidentiality of the HoTI and HoT messages is protected as it is tunneled from the home agent to the mobile node. Therefore, the home agent MUST support IPsec ESP for the protection of packets belonging to the return routability procedure. Support for a non-null encryption transform MUST be available. In this case it

isn't necessary to distinguish between different kinds of packets within the return routability procedure.

The use of ESP for protection of the return routability procedure is optional and 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. One way to set up the security policy database is to have one rule for the Mobility Header traffic between the mobile node and the home agent addresses, and an optional rule following it for Mobility Header traffic between the mobile node and any other address.

10.8. 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 10.9. 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 [20]. 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 [20], 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 [20].

- Determine from the Router Advertisement 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 from the Router Advertisement 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, as determined above, is not already present in the Home Agents List maintained by the receiving home agent, and the lifetime for the sending home agent, as determined above, 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). For each such global address determined from this Advertisement, add this global address to the list of global addresses for this home agent in this Home Agents List entry.

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

10.9. Dynamic Home Agent Address Discovery

A mobile node, while away from home, MAY use the dynamic home agent address discovery mechanism in section 11.3.2 to attempt to discover the address of one or more routers serving as home agents on its home link. This discovery might become necessary, for example, if some nodes on its home link 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.

As described in Section 11.3.2, 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 [11] for its home IP subnet prefix, using its care-of address as the Source Address of the packet. A home agent receiving such a Home Agent Address Discovery Request message that is serving this subnet (the home agent is configured with this anycast address on one of its network interfaces) SHOULD return an ICMP Home Agent Address Discovery Reply message to the mobile node (at its care-of address that was used as the Source Address of the Request message), 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 4.5). However, if this home agent's own global IP address would be placed in the list (as described below) as the first entry in the list, 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 value, 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). The home agent with the highest preference SHOULD be listed first in the Home Agent Addresses field, and the home agent with the lowest preference SHOULD be listed last.

- 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. As described in Section 4.5, one Home Agents List entry, identified by the home agent's link-local address, exists for each home agent on the link; associated with that list entry is one or more global IP addresses for this home agent, learned through Prefix Information options with the Router Address (R) bit is set, received in Router Advertisements from this link-local address.

  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.

- In order to avoid the possibility of the Reply message packet being fragmented (or rejected by an intermediate router with an ICMP Packet Too Big message [5]), if the resulting total packet size containing the complete list of home agents in the Home Agent Addresses field would exceed the minimum IPv6 MTU [6], the home agent SHOULD reduce the number of home agent IP addresses returned in the packet to the number of addresses that will fit without exceeding this limit. The home agent addresses returned in the packet SHOULD be those from the complete list with the highest preference.

10.9.1. Aggregate List of Home Network Prefixes

IPv6 provides mechanisms for node configuration when it turns on, and in renumbering a subnet, such as when a site switches to a new network service provider. These mechanisms are a part of Neighbor Discovery [20] and Address Autoconfiguration [33].

In renumbering, new prefixes and addresses can be introduced for the subnet and old ones can be deprecated and removed. These mechanisms are defined to work while all nodes using the old prefixes are at home, connected to the link using these prefixes. Mobile IPv6 extends these mechanisms to work also with mobile nodes that are away from home when the renumbering takes place.

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.

To avoid possible security attacks from forged Mobile Prefix Advertisements all such Advertisements must be authenticated to the mobile node by its home agent using IPsec [14, 12, 13] if a security associate exists (i.e. unless the mobile node does not yet have a home address configured).

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, from network prefixes representing network addresses that are 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 (Neighbor Discovery [20]). Do not update the aggregate list with any information from received prefixes that fail this check.

- Check Router Advertisements which contain an `H' bit (from other home agents) for valid prefixes that are not yet in the aggregate list, and if they are usable for autoconfiguration (`A' bit set, and prefix length is valid for address autoconfiguration on the home subnet) add them and preserve the `L' flag value. Clear the `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 [20].

- 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 (Neighbor Discovery [20]) and section 5.5.3 of RFC 2462 (Stateless Address Autoconfiguration [33]).

- 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 11.3.2).

10.9.2. 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 11.3.3).

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 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.

Assume that the home agent already has scheduled the transmission of a Router Advertisement to the mobile node. New information should be added to the existing scheduled transmission, if the freshly calculated RAND_ADV_DELAY would cause another transmission before the expiration of the Preferred Lifetime of the mobile node's home address derived from the prefix whose advertisement information has changed. In this case, the home agent does not perform the following algorithm to schedule an advertisement to the mobile node.

Otherwise, the home agent uses the following algorithm to compute a fresh value for RAND_ADV_DELAY, the offset from the current time for the scheduled transmission. If there is already a scheduled transmission, add the data from the existing scheduled transmission to the newly scheduled transmission, deleting the previously scheduled transmission event.

RAND_ADV_DELAY is the offset from the current time to be used to schedule the necessary advertisement to the mobile node. The 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.

Calculate the newly advertised Preferred Lifetime as follows.

```
MAX_SCHEDULE_DELAY == min (MAX_PFX_ADV_DELAY, Preferred Lifetime)
```

Then compute RAND_ADV_DELAY ==

```
MinRtrAdvInt + rand()*(MAX_SCHEDULE_DELAY - MinRtrAdvInt)
```

The home agent SHOULD periodically continue to retransmit an unsolicited Advertisement to the mobile node, until it is acknowledged by the receipt from the mobile node of a Binding Update matching the Binding Refresh Request in the packet (i.e., with

matching Unique Identifier mobility option). The home agent MUST wait PREFIX_ADV_TIMEOUT before the first retransmission, and double the retransmission wait time for every succeeding retransmission, up until a maximum of PREFIX_ADV_RETRIES attempts. 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. After another Binding Update is received from the mobile node, and if the mobile node has not returned to the home network in the meantime, the home agent SHOULD begin the process again of transmitting the unsolicited Advertisement.

A Binding Update matches a Binding Refresh Request if it specifies a binding for the mobile node to which the Binding Refresh Request was sent and contains a Unique Identifier mobility option matching the unique identifier sent in the Unique Identifier option in the Binding Refresh Request. In the solicited case, the mobile node will retransmit solicitations until one is received; thus, the home agent SHOULD NOT retransmit the responding advertisement.

If while the home agent is still retransmitting a Mobile Prefix Advertisement to the mobile node, another condition as described above occurs on the home link causing another Prefix Advertisement to be sent to the mobile node, the home agent SHOULD combine any Prefix Information options in the unacknowledged Mobile Prefix Advertisement into the new Advertisement, discard the old Advertisement, and then begin retransmitting the new one. according to the algorithm in section 10.9.2. The home agent MUST generate a new unique identifier for use in the Unique Identifier Option in the Binding Refresh Request tunneled with the new Mobile Prefix Advertisement.

10.9.3. 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 a security association exists with the mobile node's address, the packet MUST be protected by IPsec [14, 12, 13] to guard against malicious Mobile Prefix Advertisements. The IPsec protection MUST provide sender authentication, data integrity protection, and replay protection, covering the Mobile Prefix

Advertisement.

- A separate Binding Refresh Request message MUST be sent in addition to the advertisement, if this is the first advertisement

for a home registration, or if there was a change in prefix information since the last acknowledged advertisement was sent to the mobile node for the home registration. The Binding Refresh Request message MUST include a Unique Identifier mobility option (Section 6.2.4), with the unique identifier in the option data set to a value different than that in any other Binding Refresh Request sent recently by this home agent. It is assumed that this requirement can be met by maintaining a simple 16-bit "wrap-around" counter to generate unique identifiers for Binding Refresh Requests that contain a Unique Identifier option, incremented each time a Binding Refresh Request containing a Unique Identifier option is sent.

- If the advertisement was solicited, it should be destined (and authenticated, if possible) 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.

- The packet MUST be sent as any other unicast IPv6 packet. If a care-of address is used, the packet will be delivered directly. If a binding exists, the home agent will send the packet with a routing header containing the care-of address, as any other packet sent to the mobile node originated by the home agent (rather than using IPv6 encapsulation, as would be used by the home agent for intercepted packets).

10.9.4. Lifetimes for Changed Prefixes

As described in Section 10.2, 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 and Home Agents List.

The rules for maintaining a Home Agents List are same for home agents and correspondent nodes, and have been described in Section 10.1.

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: those to correspondent nodes,

those to the mobile node's home agent, and those to a home agent on the link on which the mobile node's previous care-of address is located. 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 (e.g., to reclaim space in its Binding Cache for other entries).

- The home address for which that Binding Update was sent. This will be one of the following:

  * one the mobile node's home addresses for typical Binding Updates (Sections 11.6.1 and 11.6.2), or

  * the mobile node's previous care-of address for Binding Updates sent to establish forwarding from the mobile node's previous location (Section 11.6.6).

- 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. For example, using an implementation in the C programming language, a Sequence Number value A is greater than another Sequence Number value B if

((short)((a) - (b)) > 0), if the "short" data type is a 16-bit signed integer.

- 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 that, when set, indicates that future Binding Updates should not 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 11.7.

The Binding Update list also conceptually contains 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.

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

- Home and care-of cookies received from the correspondent node.

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

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

11.2. Packet Processing

11.2.1. 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:

- From the point of view of protocol layers and applications above Mobile IP (e.g., transport protocols), the mobile node will generally use its home address as the source of the packet for most packets, even while away from home, since Mobile IP is designed to make mobility transparent to such software. 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. When sending such packets, the delivery method depends on whether a binding exists with the correspondent node. 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.

- For short-term communication, particularly for communication that may easily be retried if it fails, the mobile node MAY choose to directly use one of its care-of addresses as the source of the packet, thus not requiring the use of a Home Address option in the packet. An example of this type of communication might be DNS queries sent by the mobile node [17, 18]. 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, and all packets can be routed normally, directly between their source and destination without relying on Mobile IP. If 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.

For packets sent by a mobile node while it is at home, no special Mobile IP processing is required for sending this packet. Likewise, if the mobile node uses any address other than its home address as the source of a packet sent while away from home (from the point of view of higher protocol layers or applications, as described above), no special Mobile IP processing is required for sending that packet.

In each case, the packet is simply addressed and transmitted in the same way as any normal IPv6 packet.

For each other packet sent by the mobile node (i.e., packets sent while away from home, using the mobile node's home address as the source, from the point of view of higher protocol layers and applications), special Mobile IP processing of the packet is required. This can be done in two ways, as described above. These ways are:

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 preserves the transparency of Mobile IP to higher protocol layers (e.g., TCP).

- 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 [7].

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 [4].
- 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.

11.2.2. Interaction with Outbound IPsec Processing

This section sketches the interaction between outbound Mobile IP 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 [14] 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 11.2.1):

- The packet is created by higher layer protocols and applications (e.g., by TCP) as if the mobile node were at home and Mobile IP

were not being used. Mobile IP is transparent to such higher layers.

- 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 [14].

- 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 11.2.1. 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 AH [12] (or ESP [13]) header, so that the Home Address destination option is processed by the destination node before the AH or ESP 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 AH or ESP 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. The mechanics of implementation do not absolutely require such an exchange to occur; other implementation strategies may be more appropriate, as long as the result of the authentication calculation remains the same.

In addition, when using any automated key management protocol [14] (such as IKE [8]) to create a new SA (or SA bundle) while away from home, a mobile node MUST take special care in its processing of the key management protocol. Otherwise, other nodes with which the mobile node must communicate as part of the automated key management protocol processing may be unable to correctly deliver packets to the mobile node if they and/or the mobile node's home agent do not then have a current Binding Cache entry for the mobile node. For the default case of using IKE as the automated key management protocol [8][14], such problems can be avoided by the following requirements on the use of IKE by a mobile node while away from home:

- The mobile node 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 IP for these packets, as suggested in Section 11.2.1).

- In addition, for all security associations bound to the mobile node's home address established by way of IKE, the mobile node MUST include an ISAKMP Identification Payload [16] in the IKE exchange, giving the mobile node's home address as the initiator of the Security Association [28].

11.2.3. 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 sent by the correspondent node in the same way as any normal IP packet. Such packets will then be intercepted by the mobile node's home agent, encapsulated using IPv6 encapsulation [4], and tunneled to the mobile node's primary care-of address.

- 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.

- Packets sent by a correspondent node that has a Binding Cache entry for the mobile node that contains an out-of-date care-of address for the mobile node, will also be sent by the correspondent node using a type 2 Routing header, as described above. If the mobile node sent a Binding Update to a home agent on the link on which its previous care-of address is located (Section 11.6.6), and if this home agent is still serving as a home agent for the mobile node's previous care-of address, then such a packet will be intercepted by this home agent, encapsulated using IPv6 encapsulation [4], and tunneled to the mobile node's new care-of address (registered with this home agent).

For packets received by the first of these methods, the mobile node MUST check that the IPv6 source address of the tunnel 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 11.6.2, subject to the rate limiting defined in Section 11.6.9. The mobile node MUST also process the received packet in the manner defined for IPv6 encapsulation [4], 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 RH is exactly 2.

- The segments left field in the RH is either 0 or 1.

- The Home Address field in the RH is one of the node's home addresses, if the segments left field was 1.

Once the above checks have been performed, the node swaps the IPv6 destination field with the Home Address field in the RH, 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.

/

11.2.4. 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. If the multicast applications depend on the address of the joining node, the mobile node MAY establish a binding with the router and use the Home Address destination option in the sent control messages.

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; or (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.

11.3. Home Agent and Prefix Management

11.3.1. Receiving Local Router Advertisement Messages

Each mobile node maintains a Home Agents List recording information about all home agents from which it receives a Router Advertisement, for which the home agent lifetime indicated in that Router Advertisement has not yet expired. This list is used by the mobile node to enable it to send a Binding Update to the global unicast address of a home agent on its previous link when it moves to a new link, as described in Section 11.6.6. On receipt of a valid Router Advertisement, as defined in the processing algorithm specified for Neighbor Discovery [20], the mobile node 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, and the sending node currently has an entry in the node's Home Agents List, delete the corresponding entry. Subsequently, skip all of the following steps.

- 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 [20].

- Determine from the Router Advertisement 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 from the Router Advertisement 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 mobile node'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 mobile node'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, as determined above, is not already present in the Home Agents List maintained by the receiving mobile node, and the lifetime for the sending home agent, as determined above, 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). For each such global address determined from this Advertisement, add this global address to the list of global addresses for this home agent in this Home Agents List entry.

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

11.3.2. 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 11.6.1, 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 [11] for its home subnet prefix. As described in Section 10.9, 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. 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 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 attempts. Each retransmission MUST be delayed by twice the time interval of the previous retransmission.

11.3.3. 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 10.9.1.

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).

If the mobile node does not have a valid home address available for use as the IP source address, it MAY use its care-of address, but there will not be a security association between the home agent and the care-of address for the corresponding Advertisement to be authenticated.

This solicitation follows the same retransmission rules specified for Router Solicitations [20], except that the initial retransmission interval is specified to be INITIAL_SOLICIT_TIMER (see section 12).

As described in Section 11.6.2, 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 preferred lifetime (see Section 10.9.2) 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.

11.3.4. Receiving Mobile Prefix Advertisements

Section 10.9.1 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 Advertisement messages 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.

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

- 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 be protected by IPsec [14, 12, 13] to guard against malicious prefix advertisements, if a security association exists (i.e. unless the mobile node does not yet have a home address configured). The IPsec protection MUST provide sender authentication, data integrity protection, and replay protection, covering the advertisement.

Any received Mobile Prefix Advertisement not meeting all of these tests MUST be silently discarded.

If a received Mobile Prefix Advertisement is not discarded according to the tests listed above, the mobile node MUST process the Prefix Information Options as if they arrived in a Router Advertisement on the mobile node's home link [20]. 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.

If the advertisement contains a Binding Refresh Request option, the mobile node SHOULD 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 processing of this Advertisement resulted in the mobile node configuring a new home address, and if the method used for this new home address configuration would require the mobile node to perform Duplicate Address Detection [33] 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.

11.4. Movement

11.4.1. Movement Detection

A mobile node MAY use any combination of mechanisms available to it to detect when it has moved from one link to another. The primary movement detection mechanism for Mobile IPv6 defined here uses the facilities of IPv6 Neighbor Discovery, including Router Discovery and Neighbor Unreachability Detection, although 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 [20].

Mobile nodes SHOULD use Router Discovery to discover new routers and on-link subnet prefixes; a mobile node MAY send Router Solicitation messages, or MAY wait for unsolicited (periodic) multicast Router Advertisement messages, as specified for Router Discovery [20]. Based on received Router Advertisement messages, a mobile node (in the same way as any other 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 (extracted from the Router Advertisement and Prefix Information options) used to expire the entry when it becomes invalid.

While away from home, a mobile node typically selects one router from its Default Router List to use as its default router, and one subnet prefix advertised by that router from its Prefix List 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 11.4.2. The mobile node registers its primary care-of address with its home agent, as described in Section 11.6.1.

While a mobile node is away from home and using some router as its default router, it is important for the mobile node to be able to quickly detect when that router becomes unreachable, so that it can switch to a new default router and (if needed, according to prefix advertisement) to a new primary care-of address. Since some links (notably wireless) do not necessarily work equally well in

both directions, it is likewise important for the mobile node to detect when it becomes unreachable for packets sent from its default router, so that the mobile node can take steps to ensure that any

correspondent nodes attempting to communicate with it can still reach it through some other route.

To detect when its default router becomes unreachable, a mobile node SHOULD use Neighbor Unreachability Detection. As specified in Neighbor Discovery [20], while the mobile node is actively sending packets to (or through) its default router, the mobile node can detect that the router (as its neighbor) is still reachable either through indications from upper layer protocols on the mobile node that a connection is making "forward progress" (e.g., receipt of TCP acknowledgements for new data transmitted), or through receipt of a Neighbor Advertisement message from its default router in response to an explicit Neighbor Solicitation messages to it. Note that although this mechanism detects that the mobile node's default router has become unreachable to the mobile node only while the mobile node is actively sending packets to it, this is the only time that this direction of reachability confirmation is needed. Confirmation that the mobile node is still reachable from the router is handled separately, as described below.

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 for a mobile node to continually probe its default router with Neighbor Solicitation messages even when it is not otherwise actively sending packets to it. 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 Advertisement messages, 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 Solicitation messages, even if it is not otherwise actively sending packets to the router. If it receives a solicited Neighbor Advertisement message 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 Solicitation messages 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.

11.4.2. 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 11.4.3.

As described in Section 4, in order to form a new care-of address, a mobile node MAY use either stateless [33] or stateful (e.g., DHCPv6 [2]) 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.

After forming a new care-of address, a mobile node MAY perform Duplicate Address Detection [33] on that new address to confirm its uniqueness. However, doing so represents a trade-off between safety (ensuring that the new address is not used if it is a duplicate address) and overhead (performing Duplicate Address Detection requires the sending of one or more additional packets over what may be, for example, a slow wireless link through which the mobile node is connected). Performing Duplicate Address Detection also in

general would cause a delay before the mobile node could use the new care-of address, possibly causing the mobile node to be unable to continue communication with correspondent nodes for some period of time. For these reasons, 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 (e.g., unless network bandwidth or battery consumption for communication is of primary concern) begin Duplicate Address Detection asynchronously when it begins use of the address, allowing the Duplicate Address Detection procedure to complete in parallel with normal communication using the address.

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 [20, 33]; 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.

11.4.3. Using Multiple Care-of Addresses

As described in Section 11.4.2, 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 11.4.1. When the mobile node selects a new primary care-of address, it MUST register it with its home agent by sending it a Binding Update with the Home Registration (H) and Acknowledge (A) bits set, as described in Section 11.6.1.

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 [2], the mobile node may not wish to release the address immediately upon switching to a new primary care-of address.

11.5. Return Routability Procedure

This section defines the rules that the mobile node must follow when performing the return routability procedure. Appendix A specifies also a (non-normative) state-machine that describes the same procedure. Section 11.6.2 describes the rules when the return routability procedure needs to be initiated.

11.5.1. 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. 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 for which the binding is desired. This value will appear in the Source Address field of the Home Test Init message.
- The time at which each of these messages was sent.
- The mobile cookie used in the messages.

11.5.2. 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.
- The Binding Update List indicates that no home cookie 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 Mobile 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 Cookie in the Binding Update List. If the Binding Update List entry does not have a Care-of Cookie, 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.

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

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

- The Mobile 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 Cookie in the Binding Update List. If the Binding Update List entry does not have a Home Cookie, 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 Cookies, the return routability procedure is complete. The mobile node SHOULD then proceed with sending a Binding Update message as described in Section 11.6.2.

Correspondent nodes from the time before this specification was published may not 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 can not provide route optimization, and revert back to the use of bidirectional routing.

11.5.3. Retransmitting in the Return Routability Procedure

The mobile node is responsible for retransmissions in the return routability procedure.

When the mobile node sends a Home Test Init or Care-of Test Init message, it has to determine a value for the initial retransmission timer. It should use the specified value of INITIAL_BINDACK_TIMEOUT for this initial retransmission timer.

If, after sending either a Home Test Init or Care-of Test Init message and the mobile node fails to receive a valid, matching Home Test or Care-of Test message within the selected initial retransmission interval, the mobile node SHOULD retransmit the original message, until a valid answer 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 valid response or the timeout period reaches the value MAX_BINDACK_TIMEOUT.

11.5.4. Rate Limiting for Return Routability Procedure

A mobile node MUST NOT send Home Test Init or Care-of Test Init messages to any individual node more often than once per MAX_UPDATE_RATE seconds. After sending MAX_FAST_UPDATES consecutive messages to a particular node with the same care-of address, the

mobile node SHOULD reduce its rate of sending these messages to that node, to the rate of SLOW_UPDATE_RATE per second. The mobile node MAY continue to send these messages at this slower rate indefinitely, in hopes that the node will eventually be able to complete the return routability procedure.

11.6. Processing Bindings

11.6.1. Sending Binding Updates to the Home Agent

After deciding to change its primary care-of address as described in Sections 11.4.1 and 11.4.2, a mobile node MUST register this care-of address with its home agent in order to make this its primary care-of address. To do so, the mobile node sends a packet to its home agent containing a Binding Update message, 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 message.
- The `S' bit is set to the zero to request the mobile node's home agent to serve as a home agent for all home addresses for the mobile node based on all on-link subnet prefixes on the home link; this is the default behavior. If the mobile node desires that only a single home address should be affected by this Binding Update, the `S' bit can be set to 1.
- 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 from its Home Agents List (see Section 11.3.2). If there is only one home agent in the Home Agents List, 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 11.6.8 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 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 5.4. The mobile node MUST use a Home Address destination option in Binding Updates sent to the home agent in order to allow the IPsec policies to be matched with the right home address. The home address in the Home Address destination option and the Binding Update message MUST be equal (and this will be checked by the home agent).

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 11.6.2.

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 141, 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 [20][33]. 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 `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 138, 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 138 was received, for instance by using the techniques described in Appendix B.

11.6.2. 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 11.6.9).

This section defines the rules that the mobile node must follow when performing the correspondent binding procedure. Appendix A specifies also a (non-normative) state-machine that describes the same procedure.

The mobile node can be assured that its home address is still valid, for example, by the home agent's use the 'D' bit of Binding Updates (see Section 10.2). 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, instead, the care-of address is set to the mobile node's home address, the Binding Update requests the correspondent node to delete any existing Binding Cache entry that it has for the mobile node.

When a mobile node sends a Binding Update to its home agent to register a new primary care-of address (as described in Section 11.6.1), the mobile node SHOULD also start a return routability procedure to each other node for which an entry exists

in the mobile node's Binding Update List, as detailed below. Upon successful return routability procedure, a Binding Update message is sent. 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's traffic to the correspondent node. This is particularly useful if the mobile node anticipates that it is not going to stay long in this location.

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 11.6.9). 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; or this Destination Address is equal to one of the mobile node's previous care-of addresses for which the mobile node has an entry in its Binding Update List, representing an unexpired Binding Update sent to a home agent on the link on which its previous care-of address is located (Section 11.6.6).

- 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.

Binding Updates sent to correspondent nodes are not generally required to be acknowledged. However, if the mobile node wants to be sure 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 message 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, including the authenticator field which is calculated based on the received Home and Care-of Cookies.

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.

11.6.3. 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 authenticator field MUST be present and have a valid value.

- The Header Len field in the Binding Acknowledgement message 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.

- 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 11.6.9.

11.6.4. 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 (see Section 5) if it believes the amount of traffic with the correspondent justifies the use of Route Optimization. Note that the mobile node SHOULD NOT respond Binding 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 11.6.2.

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.

Note, however, that the mobile node MAY choose to delete its binding from the sender of the Binding Refresh Request. In this case, the mobile node instead SHOULD return a Binding Update to the sender, in which the Lifetime field is set to zero and the care-of address is set to the mobile node's home address.

If the Binding Refresh Request for which the Binding Update is being returned contains a Unique Identifier mobility option, the resulting Home Test Init, Care-of Test Init, and Update messages MUST also include a Unique Identifier mobility option. The unique identifier in the Option Data field of the Unique Identifier mobility option MUST be copied from the unique identifier carried in the Binding Refresh Request.

11.6.5. 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 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 (Home Address destination option used without a binding), 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 5.5).

If the message Status field was 2 (received message had an unknown value for the MH Type field), 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.

11.6.6. Forwarding from a Previous Care-of Address

When a mobile node connects to a new link and forms a new care-of address, it MAY establish forwarding of packets from a previous care-of address to this new care-of address. To do so, the mobile node sends a Binding Update to any home agent on the link on which the previous care-of address is located, indicating this previous care-of address as the home address for the binding, and giving its new care-of address as the binding's care-of address. Such packet forwarding allows packets destined to the mobile node from nodes that have not yet learned the mobile node's new care-of address, to be forwarded to the mobile node rather than being lost once the mobile node is no longer reachable at this previous care-of address.

This Binding Update is sent to a home agent, albeit a temporary one. Nevertheless, the authentication requirements for Binding Updates from a mobile node to its home agent apply, as specified in Section 11.6.1. This means that the mobile node MUST employ IPsec ESP as specified further below.

In constructing this Binding Update, the mobile node utilizes the following specific steps:

- The Home Address field in the Home Address destination option in the packet carrying the Binding Update MUST be set to the previous care-of address for which packet forwarding is being established.

- The care-of address for the new binding MUST be set to the new care-of address to which packets destined to the previous care-of address are to be forwarded. Normally, this care-of address for the binding is specified by setting the Source Address of the packet carrying the Binding Update, to this address. However, the mobile node MAY instead include an Alternate Care-of Address

mobility option in the Binding Update message, with its Alternate Care-of Address field set to the care-of address for the binding.

- The Home Registration (H) bit MUST also be set in this Binding Update, to request this home agent to temporarily act as a home agent for this previous care-of address.

This home agent will thus tunnel packets for the mobile node (packets destined to its specified previous care-of address) to its new care-of address. All of the procedures defined for home agent operation MUST be followed by this home agent for this registration. Note that this home agent does not necessarily know (and need not know) the mobile node's (permanent) home address as part of this registration.

The packet carrying the Binding Update MUST be addressed to this home agent's global unicast address. Normally, this global unicast address is learned by the mobile node based on the Router Advertisements received by the mobile node (Section 7.2) while attached to the link on which this previous care-of address and this home agent are located; the mobile node obtains this home agent address from its Home Agents List (Section 4.4). Alternatively, the mobile node MAY use dynamic home agent address discovery (Section 10.9) to discover the global unicast address of a home agent on this previous link, but it SHOULD use an address from its Home Agents List if available for the prefix it used to form this previous care-of address.

As with any packet containing a Binding Update (see Section 6.1.7), the Binding Update packet to this home agent MUST meet the authentication requirements for Binding Updates, defined in Section 5.4. Each Binding Update MUST be authenticated as coming from the right mobile node. This means that the mobile node and the home agent MUST have a security association that employs IPsec ESP for protecting the Mobility Header with a non-null authentication algorithm. The mobile node MUST use a Home Address destination option in Binding Updates sent to the home agent in order to allow the IPsec policies to be matched with the right home address. The home address in the Home Address destination option and the Binding Update message MUST be equal (and this will be checked by the home

agent), that is, it MUST be the mobile node's previous care-of address for which forwarding is being established.

11.6.7. Returning Home

A mobile node detects that it has returned to its home link through the movement detection algorithm in use (Section 11.4.1), 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 Binding Update, the mobile node MUST set the care-of address for the binding (the Source Address field in the packet's IPv6 header) to the mobile node's own home address. As with other

Binding Updates sent to register with its home agent, the mobile node MUST set the Acknowledge (A) and Home Registration (H) bits, and SHOULD retransmit the Binding Update until a matching Binding Acknowledgement is received.

When sending this Binding Update to its home agent, the mobile node must be careful in how it uses Neighbor Solicitation [20] (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. 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 unicast 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). Since the solicitation is unicast, the home agent will be able to distinguish from a similar packet that would only be used 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.

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 message [20], to advertise the mobile node's own link-layer address for its own home address. The Target Address in this Neighbor Advertisement message 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 message 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 message. 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 Advertisement messages 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 [20].

11.6.8. Retransmitting Binding Updates

The mobile node is responsible for retransmissions in the binding procedure.

When the mobile node sends a Binding Update message, it has to determine a value for the initial retransmission timer. If the mobile node is changing or updating an existing binding at the home agent, it should use the specified value of INITIAL_BINDACK_TIMEOUT for this initial retransmission timer. If on the other hand the mobile node 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 that would be used by the mobile node. This longer retransmission interval will allow the the home agent to complete the DAD procedure which is mandated in this case, as detailed in Section 11.6.1.

If, after sending a Binding Update in which the care-of address has changed and the Acknowledge (A) bit is set, a mobile node fails to receive a valid, matching Binding Acknowledgement within the selected initial retransmission interval, the mobile node SHOULD retransmit the Binding Update, until a Binding Acknowledgement is received. Such a retransmitted Binding Update MUST use a Sequence Number value greater than that used for the previous transmission of

this Binding Update. 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 Binding Acknowledgement or the timeout period reaches the value MAX_BINDACK_TIMEOUT.

11.6.9. Rate Limiting Binding Updates

A mobile node MUST NOT send Binding Update messages for the same binding to any individual node more often than once per MAX_UPDATE_RATE seconds. After sending MAX_FAST_UPDATES consecutive messages to a particular node with the same care-of address, the mobile node SHOULD reduce its rate of sending these messages to that node, to the rate of SLOW_UPDATE_RATE per second. The mobile node MAY continue to send these messages at this slower rate indefinitely, in hopes that the node will eventually be able to process a Binding Update, and begin to route its packets directly to the mobile node at its new care-of address.

11.7. Receiving ICMP Error Messages

Any node receiving a Mobility header that does not recognize the protocol SHOULD return an ICMP Parameter Problem, Code 1, message to the sender of the packet. If a node performing the return routability procedure or sending a Binding Update receives such an ICMP error message in response, 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 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 the that the Home Address option, the mobile node SHOULD log the error and then discard the ICMP message.

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
MAX_COOKIE_LIFE	240 seconds
MAX_FAST_UPDATES	5 transmissions
MAX_PFX_ADV_DELAY	1,000 seconds
MAX_RR_BINDING_LIFE	300 seconds
MAX_UPDATE_RATE	once per second
PREFIX_ADV_RETRIES	3 retransmissions
PREFIX_ADV_TIMEOUT	5 seconds
SLOW_UPDATE_RATE	once per 10 second interval

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 [19].

Furthermore, each Mobility Header message may contain mobility options as described in Section 6.2. The current mobility options are defined in Sections 6.2.2 through 6.2.5, and include the following:

0 Pad1

1 PadN

2 Unique Identifier

3 Alternate Care-of Address

4 Nonce Indices

5 Authorization Data

Future values of the Option Type can be allocated using standards action [19].

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 must 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 message, described in Section 6.7; and
- The Mobile Prefix Advertisement message, described in Section 6.8.

This document also defines two new Neighbor Discovery [20] 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. Security for the Tunneling to and from the Home Agent

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, as well as attacks where 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.

It is possible to use IPsec ESP to protect payload packets tunneled to the mobile node and back. While this specification does not mandate the use of ESP, its use is recommended to protect the payload communications against attackers on the path between the home agent and the current location of the mobile node.

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 and the use of encrypted tunnels is particularly useful for this kind of home addresses.

14.2. Security for the Binding Updates to the Home Agent

The use of IPsec ESP to protect Mobility Header messages between the mobile node and the home agent protects the integrity of the Binding Updates and Binding Acknowledgements. Sequence numbers with the Mobile IPv6 messages ensure correct ordering (see Section 5.4). However, if a home agent reboots and loses its state regarding the sequence numbers, replay attacks become possible. If the home agent is vulnerable to this, the use of a key management mechanism together

with IPsec can be used to prevent replay attacks.

14.3. Security for the Binding Updates to the Correspondent Nodes

The use of home address and care-of-address based return routability tests prevents any off-path attacks beyond those that are already possible in basic IPv6 [23].

Protection against attackers on the home agent link and the correspondent node link, as well as on the path between, are roughly similar to the situation in existing IPv6 as well. However, one difference is that in basic IPv6 an on-path attacker must be constantly present on the link or the path (e.g., in order to perform a man-in-the-middle attack), whereas with Mobile IPv6 an attacker can leave an existing binding behind, even after it is no longer on the link or on the path [23]. For this reason, this specification limits the validity of bindings authorized by return routability to a maximum of MAX_COOKIE_LIFE + MAX_RR_BINDING_LIFE seconds after the last routability check has been performed.

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. Thus, the weakest points are typically on the links at either end, and their mechanisms for layer 2 security or IPv6 Neighbour and Router Discovery. If these were secured using some new technology in the future, this could make the key establishment mechanism specified in this document to be an easier route for attackers to use. For this reason, this specification should have a protection mechanism for selecting between return routability and potential other future mechanisms.

14.4. Security for the Home Address Destination Option

The use of the Home Address destination option allows packets sent by a mobile node to pass normally through routers implementing ingress filtering [7]. Since the care-of address used in the Source Address field of the packet's IPv6 header is topologically correct for the sending location of the mobile node, ingress filtering can trace the

location of the mobile node in the same way as can be done with any sender when ingress filtering is in use. As this location does not survive in replies sent by the correspondent node, this document restricts the use of the Home Address option to those situations where a binding has been established with the participation of the node at the home address. This prevents reflection attacks through the use of the Home Address option.

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.

14.5. Firewall considerations

The definition of Routing Header 2 in Section 6.4 and the associated processing rules have been chosen so that the header can not be used for what is traditionally viewed as source routing. In particular, the IPv6 destination and the Home Address in the routing header will always have to be assigned to the same node otherwise the packet will be dropped.

This means that the typical security concerns for source routing including the automatic reversal of unauthenticated source routes (which is an issue for IPv4 but not for IPv6 source routing) and the ability to use source routing to "jump" between nodes inside, as well as outside a firewall, are not at play.

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 8.2. This is necessary in order to allow Mobile IPv6 traffic while still having the option to filter out other uses of Routing headers.

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), 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), Krishna Kumar (IBM Research), T.J. Kniveton (Nokia Research), Jiwoong Lee (KTF), Aime Lerouzic (Bull S.A.), Thomas Narten (IBM), Erik Nordmark (Sun Microsystems), Simon Nybroe (Ericsson Telebit), David Oran (Cisco), Lars Henrik Petander (HUT), Basavaraj Patil (Nokia), Ken Powell (Compaq), Phil Roberts (Motorola), Patrice Romand (Bull S.A.), Jeff Schiller (MIT) Tom Soderlund (Nokia Research), Hesham Soliman (Ericsson), Jim Solomon (RedBack Networks), Tapio Suihko (Technical Research Center of Finland), Benny Van Houdt (University of Antwerp), Jon-Olov Vatn (KTH), Alper Yegin (Sun Microsystems), 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 (AIX), Ericsson Telebit (FreeBSD), NEC (FreeBSD), and INRIA (FreeBSD). 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.

Lastly, we must express our appreciation for the significant contributions made by members of the Mobile IPv6 Security Design Team, including (in alphabetical order) Gabriel Montenegro, Erik Nordmark, and Pekka Nikander, who have contributed volumes of text to

this specification.

References

[1] Tuomas Aura and Jari Arkko. MIPv6 BU Attacks and Defenses. Internet Draft draft-aura-mipv6-bu-attacks-01.txt (Work In Progress), IETF, February 2002.

[2] 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.

[3] 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.

[4] A. Conta and S. Deering. Generic Packet Tunneling in IPv6 Specification. Request for Comments (Proposed Standard) 2473, Internet Engineering Task Force, December 1998.

[5] 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.

[6] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. Request for Comments (Draft Standard) 2460, Internet Engineering Task Force, December 1998.

[7] 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.

[8] D. Harkins and D. Carrel. The Internet Key Exchange (IKE). Request for Comments (Proposed Standard) 2409, Internet Engineering Task Force, November 1998.

[9] R. Hinden and S. Deering. IP Version 6 Addressing Architecture.

Request for Comments (Proposed Standard) 2373, Internet Engineering Task Force, July 1998.

[10] 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.

[11] D. Johnson and S. Deering. Reserved IPv6 Subnet Anycast Addresses. Request for Comments (Proposed Standard) 2526, Internet Engineering Task Force, March 1999.

[12] S. Kent and R. Atkinson. IP Authentication Header. Request for Comments (Proposed Standard) 2402, Internet Engineering Task Force, November 1998.

[13] S. Kent and R. Atkinson. IP Encapsulating Security Payload (ESP). Request for Comments (Proposed Standard) 2406, Internet Engineering Task Force, November 1998.

[14] S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. Request for Comments (Proposed Standard) 2401, Internet Engineering Task Force, November 1998.

[15] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-Hashing for Message Authentication. Request for Comments (Informational) 2104, Internet Engineering Task Force, February 1997.

[16] 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.

[17] P. V. Mockapetris. Domain names - concepts and facilities. Request for Comments (Standard) 1034, Internet Engineering Task Force, November 1987.

[18] P. V. Mockapetris. Domain names - implementation and specification. Request for Comments (Standard) 1035, Internet Engineering Task Force, November 1987.

[19] 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.

[20] 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.

[21] NIST. Secure Hash Standard. FIPS PUB 180-1, April 1995.

[22] Erik Nordmark. Securing MIPv6 BUs using return routability (BU3WAY). Internet Draft draft-nordmark-mobileip-bu3way-00.txt (Work In Progress), IETF, November 2001.

[23] Erik Nordmark, Gabriel Montenegro, Pekka Nikander, and Jari Arkko. Mobile IPv6 Security Design Rationale. To appear, 2002.

[24] C. Perkins. IP Encapsulation within IP. Request for Comments (Proposed Standard) 2003, Internet Engineering Task Force, October 1996.

[25] C. Perkins. IP Mobility Support. Request for Comments (Proposed Standard) 2002, Internet Engineering Task Force, October 1996.

[26] C. Perkins. Minimal Encapsulation within IP. Request for Comments (Proposed Standard) 2004, Internet Engineering Task Force, October 1996.

[27] C. Perkins and D. Johnson. Route Optimization in Mobile IP (work in progress). Internet Draft, Internet Engineering Task Force.
draft-ietf-mobileip-optim-11.txt, September 2001.

[28] D. Piper. The Internet IP Security Domain of Interpretation for ISAKMP. Request for Comments (Proposed Standard) 2407, Internet Engineering Task Force, November 1998.

[29] D. C. Plummer. Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware. Request for Comments (Standard) 826, Internet Engineering Task Force, November 1982.

[30] J. Reynolds and J. Postel. Assigned Numbers. Request for Comments (Standard) 1700, Internet Engineering Task Force, October 1994.

[31] Michael Roe, Greg O'Shea, Tuomas Aura, and Jari Arkko. Authentication of Mobile IPv6 Binding Updates and Acknowledgments. Internet Draft draft-roe-mobileip-updateauth-02.txt (Work In Progress), IETF, February 2002.

[32] Pekka Savola. Security of IPv6 Routing Header and Home Address Options. Internet Draft draft-savola-ipv6-rh-ha-security-01.txt (Work In Progress), IETF, November 2001.

[33] S. Thomson and T. Narten. IPv6 Stateless Address Autoconfiguration. Request for Comments (Draft Standard) 2462, Internet Engineering Task Force, December 1998.

A. State Machine for the Correspondent Binding Procedure

Home agents and correspondent nodes are stateless until a binding is actually established.

The mobile node, however, is responsible for initiating the correspondent binding procedure, keeping track of its state, handle

retransmissions and failures, and completing the procedure.

Section 11.6.2 defines the normative rules that the mobile node must follow when performing the correspondent procedure. This appendix specifies an additional, non-normative, state-machine that illustrates the behaviour of the mobile node.

The mobile node will keep the following states in its Binding List:

- Idle: This is an abstract state that refers to the situation that the correspondent node in question does not appear in the Binding List. In this state, all RR and binding related messaging is silently ignored.

- WaitHC: In this state, the mobile node has sent the Home Test Init and CoT Init messages, and is waiting for the Home Test and CoT messages to come back. It will also be necessary to keep state of retransmissions for both.

- WaitH: In this state, the mobile node has a recent Care-of Cookie and is only waiting for the Home Test message to arrive.

- WaitC: In this state, the mobile node has a recent Home Cookie and is only waiting for the CoT message to arrive.

- WaitA: In this state, the mobile node has sent a Binding Update, and is only waiting for the Binding Acknowledgement message to arrive.

- WaitD: In this state, the mobile node has sent a de-registration Binding Update, and is only waiting for the Binding Acknowledgement message to arrive.

- WaitDH: In this state, the mobile node intends to send a de-registration Binding Update later but is first waiting for a home cookie before this can be done. Note that if the mobile node is at home, it can use a home cookie also as care-of cookie.

- Bound: In this state, the mobile node has established a binding with the correspondent node.

The following events are possible:

- Route Optimization desired. This is a decision taken by the mobile node based on observing traffic to and from the correspondent node.

- Route Optimization not needed. This is another decision taken by the mobile node, perhaps due to running out of resources or lack of sufficient traffic to justify route optimization with this particular correspondent node. Another reason for not needing Route Optimization any more is that the mobile node has returned home.

- Movement.

- Valid BRR received. A valid Binding Refresh Request message has been received.

- Valid HoT received. A valid Home Test message has been received.

- Valid CoT received. A valid Care-of Test message has been received.

- Valid BA received. A valid Binding Acknowledgement message has been received.

- Valid BE received. A valid Binding Error message has been received.

- ICMP Parameter Problem Code 1 received. This can happen if the peer does not support this specification.

- Invalid BRR received.

- Invalid HoT received.

- Invalid CoT received.

- Invalid BA received.

- Invalid BE received.

- Retransmission needed. A timer is set to expire when a retransmission of a packet needs to be made.

- Retransmission failed. A timer is set to expire when all retransmissions have failed.

The following additional conditions are also used:

- Acknowledgements are required. This is a local configuration on the mobile node side, and indicates whether acknowledgements are required to binding updates.

- Home cookie too old. A cookie is too old if it has been received MIN_COOKIE_LIFE or over seconds ago.

- Care-of cookie too old.

- Reason to believe forward progress is being made. Upper layer protocols such as TCP may provide hints to the IP layer regarding the successfullness of the recent communications.

- Tests of the Status values received in a BE or BA message.

- Binding lifetime left. The remaining lifetime field of a Binding Update List entry tells whether the binding currently registered at the correspondent node still has some lifetime left, even if we are trying to create a new one. This has relevance when an attempt at re-binding is aborted for some reason.

The state machine for the mobile node is as follows:

State	Event	Action	New State
Idle	Route Optimization desired	Send HoTI, Send CoTI, Start retrans-mission and failure timers	WaitHC
Idle	Valid HoT received	(None)	Idle
Idle	Valid CoT received	(None)	Idle
Idle	Valid BA received	(None)	Idle
Idle	Valid BRR received	(None)	Idle
Idle	ICMP Parameter Problem Code 1	(None)	Idle

	received		
Idle	Valid BE received and status = 1	(None)	Idle
Idle	Valid BE received and status = 2	(None)	Idle
Idle	Movement	(None)	Idle

State	Event	Action	New State

WaitHC	Valid HoT received	Store cookie and nonce index	WaitC
WaitHC	Valid CoT received	Store cookie and nonce index	WaitH
WaitHC	Valid BA received	(None)	WaitHC
WaitHC	Valid BRR received	(None)	WaitHC
WaitHC	Retransmission needed	Send HoTI, Send CoTI, Start timer TRetr	WaitHC
WaitHC	Valid BE received and status = 1	(None)	WaitHC
WaitHC	Valid BE received and status = 2	Stop timers	Idle
WaitHC	Movement	Send CoTI, Restart retransmission and failure	WaitHC

		timers	
WaitHC	Route Optimization not needed	(None)	WaitHC
WaitHC	ICMP Parameter Problem Code 1 received	Stop timers	Idle

State	Event	Action	New State
WaitH	Valid HoT received and acknowledgements required	Store cookie and nonce index, Send BU, Start retrans-mission timer	WaitA
WaitH	Valid HoT received and acknowledgements not required	Store cookie and nonce index, Send BU, Stop timers	Bound
WaitH	Valid CoT received	(None)	WaitH

WaitH	Valid BA received	(None)	WaitH
WaitH	Valid BRR received	(None)	WaitH
WaitH	Retransmission needed	Send HoTI, Start retrans-mission timer	WaitH
WaitH	Valid BE received and status = 1	(None)	WaitH
WaitH	Valid BE received and status = 2	Stop timers	Idle
WaitH	Movement	Send CoTI, Restart	WaitH

		retransmission and failure timers	
WaitH	Route Optimization not needed	(None)	WaitH
WaitH	ICMP Parameter Problem Code 1 received	(None)	WaitH

State	Event	Action	New State
WaitC	Valid CoT received and acknowledgements required	Store cookie and nonce index, Send BU, Start retrans-mission timers	WaitA
WaitC	Valid CoT received and acknowledgements not required	Store cookie and nonce index, Send BU, Stop timers	Bound
WaitC	Valid HoT received	(None)	WaitC
WaitC	Valid BA received	(None)	WaitC
WaitC	Valid BRR received	(None)	WaitC
WaitC	Valid BE received and status = 1	(None)	WaitC

WaitC	Valid BE received and status = 2	Stop timers	Idle
WaitC	Retransmission needed	Send CoTI, Start retrans-mission timer	WaitC

WaitC	Movement	Send CoTI, Restart retransmission and failure timers	WaitC
WaitC	Route Optimization not needed	(None)	WaitC
WaitC	ICMP Parameter Problem Code 1 received	(None)	WaitC

State	Event	Action	New State
WaitA	Valid BA received and status < 128	Stop timers	Bound
WaitA	Valid BA received and status = 141	Set sequence#, Send BU, Restart retransmission and failure timers	WaitA
WaitA	Valid BA received and status = 144 or 145	Send HoTI, Send CoTI, Restart retransmission and failure timers	WaitHC
WaitA	Valid BA received and status anything else	Stop timers	Idle
WaitA	Valid HoT received	(None)	WaitA
WaitA	Valid CoT received	(None)	WaitA
WaitA	Valid BRR received	(None)	WaitA
WaitA	Retransmission needed	Send BU, Start retrans-mission timer	WaitA

WaitA	Valid BE received and status = 1	(None)	WaitA
WaitA	Valid BE received and status = 2	Stop timers	Idle
WaitA	Movement	Send CoTI, Restart retransmission and failure timers	WaitC
WaitA	Route Optimization not needed	(None)	WaitA
WaitA	ICMP Parameter Problem Code 1 received	(None)	WaitA

State	Event	Action	New State
WaitD	Valid BA received and status < 128	Stop timers	Idle
WaitD	Valid BA received and status = 141	Set sequence#, Send BU, Restart retransmission and failure timers	WaitD
WaitD	Valid BA received and status = 144 or 145	Send HoTI, Restart retransmission and failure timers	WaitDH
WaitD	Valid BA received and status anything else	Stop timers	Idle
WaitD	Valid HoT received	(None)	WaitD
WaitD	Valid CoT received	(None)	WaitD
WaitD	Valid BRR received	(None)	WaitD
WaitD	Retransmission needed	Send BU, Start retrans-	WaitD

		mission timer	
WaitD	Valid BE received	Stop timers	Idle

WaitD	Movement	(None)	WaitD
WaitD	Route Optimization Desired	Send HoTI, Send CoTI, Restart retransmission and failure timers	WaitHC
WaitD	ICMP Parameter Problem Code 1 received	(None)	WaitD

State	Event	Action	New State
WaitDH	Valid HoT received and acknowledgements required	Send BU, Restart retransmission and failure timers	WaitD
WaitDH	Valid HoT received and acknowledgements not required	Send BU, Stop timers	Idle
WaitDH	Valid CoT received	(None)	WaitDH
WaitDH	Valid BA received	(None)	WaitDH
WaitDH	Valid BRR received	(None)	WaitDH
WaitDH	Retransmission needed	Send HoTI, Start retrans-mission timer	WaitDH
WaitDH	Valid BE received	Stop timers	Idle

WaitDH	Movement	(none)	WaitDH
WaitDH	Route Optimization Desired	Send HoTI, Send CoTI, Restart retransmission and failure timers	WaitHC
WaitDH	ICMP Parameter Problem Code 1 received	(None)	WaitDH

State	Event	Action	New State

Bound	Valid BRR received	Send HoTI, Send CoTI, Start retrans-mission timers	WaitHC
Bound	Valid HoT received	(None)	Bound
Bound	Valid CoT received	(None)	Bound
Bound	Valid BA received	(None)	Bound
Bound	Route Optimization not needed and home cookie not too old and acknowledgements not required	Send BU	Idle
Bound	Route Optimization not needed and home cookie not too old and acknowledgements required	Send BU, Start retrans-mission and failure timers	WaitD
Bound	Route Optimization not needed and home cookie too old	Send HoTI, Start retrans-mission and failure timers	WaitDH

Bound	ICMP Parameter Problem Code 1 received	(None)	Bound
Bound	Movement and home cookie not too old	Send CoTI, Start retrans-mission and failure timers	WaitC
Bound	Movement and home cookie too old	Send HoTI, Send CoTI, Start retrans-mission and failure timers	WaitHC
Bound	Valid BE received and status = 1 and reason to believe forward progress is being made	(None)	Bound
Bound	Valid BE received and status = 1 and no reason to believe forward progress is being made	Send HoTI, Send CoTI, Start retrans-mission and failure timers	WaitHC

Bound	Valid BE received and status = 2	(None)	Bound
Bound	ICMP Parameter Problem Code 1 received	(None)	Bound

State	Event	Action	New State
(Any)	Retransmission failed	Stop retrans-mission timer	Idle
(Any)	Invalid BRR received		(No change)
(Any)	Invalid HoT received		(No change)

(Any)	Invalid CoT received		(No change)
(Any)	Invalid BA received		(No change)
(Any)	Invalid BE received		(No change)
(Any)	Invalid MH Type received	Send BE with status 2	(No change)

B. 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-ipv6-15.txt:

B.1. Changes from Draft Version 16

- The "rest" of the document has been updated to correspond to the new packet formats and messages.
- Correspondent node operation has been updated to include the new security mechanisms.
- Procedures for reverse tunneling have been described for both home agents and mobile nodes, and these requirements have been take in account in Section 8.
- Terminology has been aligned throughout the document. Parameters are now mobility options. Binding Request is Binding Refresh Request. Capitalization of the terms has been aligned throughout the document.

- Overview section is now shorter, security issues are discussed elsewhere and data structures are fully described later.
- Parts of the mobile node requirements under Section 10.9 were moved to Section 11.3.3.
- A mechanism for Binding Acknowledgement authorization has been

clarified.

- Alignment rules, minimum lengths, and packet formats of Mobility Header message have been updated.

- Discussion on the use of Type 0 Routing header in addition to Type 2 Routing header has been removed from the correspondent node operation section, and we now rely only on the ordering requirements specified by the Routing Header Type 2 description.

- Type 2 Routing header rules have been rewritten to allow for Segments Left to be 0. Explanation on how AH works with Routing header has been clarified. Much of the text has been moved to the Mobile Node Operation and Correspondent Node Operation sections.

- The concept of "persistent" ICMP messages is no longer referred to by a MUST keyword in Section 9.7.

- References to the "Router (R)" bit have been changed to "Router Address (R)" bit.

- The Home Agent Information option now has to appear on all Prefix Advertisements, or on none of them.

- Sub-options have been removed.

- The Dynamic Home Agent Address Discovery procedures have been updated to not use piggybacking. Binding Refresh Requests are still sent during these procedures in certain cases, however. the Unique Identifier mobility option has been used to synchronize BRR and BU instead of the sequence number. The scheduling of the prefix deliveries has been changed to send new information even when the current binding is close to expiring.

- Section 11.7 now uses ICMP Parameter Problem Code 1 instead of 2.

- Sections 11.3.4 and 10.9 now agree that IPsec need not be used for the first advertisement.

- The rules regarding addresses for receiving and sending multicast traffic and control messages have been clarified for mobile nodes.

- The Binding Missing message has been renamed to Binding Error.

- Eliminated the use of symbols in the description of the return routability procedure.

- Wrote a new description of the return routability procedure.

B.2. Changes from Draft Version 15

- A binding update authorization mechanism suitable for use between previously unknown peers in the global Internet has been incorporated to the specification. As a result, Sections 5, 6.1, 14 and others have been substantially revised.

- A new IPv6 protocol has replaced IPv6 Destination Options for some of the MIPv6 signaling. This was done in order to enable the use of standard IPsec for the protection of binding updates between the mobile node and the home agent, the protection of return routability packets as they are forwarded to the mobile node from the home agent, and possibly in the future the protection of binding updates themselves to the correspondent nodes. This has resulted in substantial modifications in Section 6.

- The use of the Home Address destination option has been restricted to the situation where a binding already exists. This has been done in order to limit distributed Denial-of-Service attacks through reflections attacks that employ the Home Address Option.

- A new Binding Missing message has been added to signal the mobile node that it has used the Home Address destination option when the correspondent node has no existing binding to the node.

- The Authorization Data mobility option has been made a part of the Binding Update and Acknowledgement messages, and is now calculated in the specific manner required by the authorization mechanism (return routability).

- Sequence number length for Binding Update messages has been increased to 32 bits to protect home registrations against replay attacks.

- Mobile IPv6 uses now Routing Header type 2 instead of the general type 0, in order to limit potential dangers that general capabilities offers type 0 and to ensure that firewall

administrators want to allow the type of Routing Header that Mobile IPv6 uses through.

- Requirements for all IPv6 routers have also been updated in order to describe the considerations relating to the new Routing Header type.

- Processing rules for mobile nodes, correspondent nodes, and to some extent home agents have been substantially modified in order to explain the new authorization scheme.

- Piggybacking is no longer possible due to the use of a new IPv6 protocol and not a destination option. (However, a separate extension to this specification will allow piggybacking and takes in account the necessary IPsec policy considerations to avoid problems.)

- The security considerations in Section 14 have been revised to describe the threats that this specification protects against as well as any residual threats.

B.3. Changes from Earlier Versions of the Draft

- Strengthened mandates for mobile nodes so that now a mobile node MUST support decapsulation and processing for routing headers (section 11.2.3).

- Enabled ESP to be a valid way to secure reverse tunneled packets (section 10.6).

- Removed mandate that mobile node select a default router, and instead described it as typical behavior (section 11.4.1). Also made it clear that picking a new default router does not automatically mean picking a new primary care-of address.

- Modified mandated behavior from Home Agent upon reception of a `D' bit in a Binding Update. The home agent only has to make sure that DAD has been run, and that no other node on the home network could be using the mobile node's link-local address.

- Added provisional ICMP numbers for the new message types, which may be reassigned by IANA, but which will be useful for testing purposes.

- Removed the Mobile Router Prefix Length Sub-Option

- Removed the Prefix Length field from the Binding Update, and references to error number 136.

- Added the `S' bit so that the home agent can be instructed to *override* its default behavior. That is, with the `S' bit set, the home agent will not attempt to be helpful by changing

multiple Binding Cache entries, for multiple routing prefixes, after receiving only one Binding Update.

- Reworded the specification so that the Home Agent now has to perform Duplicate Address Detection for the mobile node's address on all the prefixes for which the router is performing home agent service.

- Removed the section about Mobile Routers

- Added the Authentication Data Sub-option; reorganized the section about computing authentication data.

- Specified that the Home Agent lifetime is by default the same as the Router lifetime, in a Router Advertisement.

- Specified that Binding Updates with zero lifetime and the 'A' bit set should cause a Binding Acknowledgement to be sent back to the Source IP address of the Binding Update.

- Qualified the allowable times when a mobile node can send a Binding Update to a correspondent node

- Added text allowing the correspondent node to extend an existing Routing Header by also including the care-of address as the entry of a routing header to be visited immediately before the home address. In this way, for instance, the mobile node can be an

intermediate node of a path along the way to some other node.

- Removed the Home Address field from the Home Agent Address Discovery Request Message.

- Noted that ICMP Unreachable forms a potential mechanism by which a malicious node can cause a correspondent node to delete a valid entry from its Binding Cache.

- Specified that, when a router stops offering home agent services by turning off the 'H' flag, the mobile node has to delete the corresponding entry from its Home Agent list.

- Clarified language about how the aggregate list of prefixes is built by the home agent, to include only prefixes with the 'H' bit set.

- Specified a new error status (141) to handle cases for sequence number mismatches (e.g., when a mobile node reboots).

- Moved this section to the appendix, and reorganized other appendix sections.

- Reorganized some related sections to be adjacent to each other.

- Changed the Prefix Length of the Binding Update to be 7-bit only, in order to reserve more flag bits for the future.

- Changed the Sequence Number of the Binding Update and Binding Acknowledgement to be 8-bit only.

- Inserted specification that, after returning home and sending a Neighbor Solicitation to the home agent, a mobile node should accept any Neighbor Advertisement from the home agent as an indication that the home agent is REACHABLE.

- Inserted new terminology for binding key and binding security association in anticipation of eliminating the use of AH

- Eliminated use of AH for authenticating Binding Update, and for authenticating Binding Acknowledgement

- Specified that all correspondent nodes MUST implement a base protocol for establishing a Binding Key; this has become the return routability procedure in this document.

- Added the following protocol constants:

  INITIAL_SOLICIT_TIMER: XXX

- Created new ICMP messages for Mobile Prefix Solicitations and Advertisements (see sections 6.7 and 6.8).

- Changed Network Renumbering (Section 10.9.1) to encompass mobile node configuration issues, remove unspecified address usage, simplify rules for prefix maintenance and sending, and use new ICMP message types noted above.

- Added a paragraph to Returning Home (section 11.6.7) to describe how the Home Agent discovers the mobile node's link-layer address

- Reworded parts of Appendix C as needed.

- Added the Mobile Router Prefix Length Sub-Option along with text describing what a Mobile Router should do with it.

C. 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 using stateless or stateful autoconfiguration.

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 message.

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 message 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 message 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.

D. Future Extensions

D.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 D.3).

The idea is to use the Flag field in the HoTI message so that the mobile node can indicate that it supports the receipt of piggybacked messages, use the Flag field in the HoT message for the correspondent node to indicate that it can support the receipt of piggybacked

messages, and then carry the piggybacked payload after the MH header by specifying a payload protocol type other than NO_NXTHDR (59).

Until such a separate specification exists implementations conforming to this specification MUST set the payload protocol type to NO_NXTHDR (59 decimal).

D.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.

D.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 14.3, future enhancements of IPv6 security may cause a need to improve also the security of the return routability procedure. The question is then what is the method to securely agree on the use of another method, while still allowing return routability procedure for some hosts during a transition period. In some cases, a third party can help to make this selection. But in general infrastructureless methods have little information beyond the exchanged messages and their contents. For these reasons, the final version of this specification requires a protection mechanism for selecting between the return routability procedure and potential other future mechanisms (see Section 14.3) but this isn't ready yet.

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.

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 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