IETF Mobile IP Working Group   David B. Johnson
INTERNET-DRAFT   Rice University
                                                   Charles Perkins
                                             Nokia Research Center
                                                      2 July 2000

Mobility Support in IPv6
<draft-ietf-mobileip-ipv6-14.txt>

Status of This Memo

Abstract

   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 four new IPv6 destination options,
   including one that MUST be supported in packets received by any node,
   whether mobile or stationary.

                              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 operation defined here, 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. Some
   aspects of this problem are addressed by the movement detection
   procedure described in Section 10.4, but no attempt has been made
   to fully solve this problem in its general form. Most aspects of
   this problem can be solved by the workaround of restricting such
   networks to only one router per link, although there are still
   possible hidden terminal problems when two nodes on the same
   link (on opposite sides of the router) attempt to communicate
   directly.

 - Access control on a link being visited by a mobile node. This
   is a general problem any time an unauthenticated node is allowed
   to connect to any link layer. It is independent of whether the
   connecting node uses Mobile IP, DHCP [2], or just "borrows" an IP
   address on the link.

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) [19, 18, 20], 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" [21] 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 [19]. 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 mobile nodes and Mobile IP to coexist
      efficiently with routers that perform "ingress filtering" [7]. A
      mobile node now 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 nor stationary,
      whether host or router.

   - The use of IPv6 destination options allows all Mobile IPv6
      control traffic to be piggybacked on any existing IPv6 packets,
      whereas in Mobile IPv4 and its Route Optimization extensions,
      separate UDP packets were required for each control message.

   - 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 [17] and Address Autoconfiguration [27], to operate in
  any location away from home without any special support required
  from its 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 [17] rather than ARP [23] 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 simplifies implementation
  of Mobile IP due to the ability to not be concerned with any
  particular link layer as is required 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 [10] and returns a single reply to the mobile
       node, rather than the corresponding Mobile IPv4 mechanism that
       used IPv4 directed broadcast and returned 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 need be sent back to the mobile node. The mobile node is
       less likely to lose one of the replies because no "implosion" of
       replies is required by the protocol.

   -   Mobile IPv6 defines an Advertisement Interval option on
       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.

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, as defined above).

Security Policy Database (SPD)
                A database of security associations selectable by

rulesets (policies) that determine the packets for
which each security association is to be applied.

[3.2](). Mobile IPv6 Terms

home address   An IP address assigned to a mobile node within 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. Standard IP routing mechanisms will
               deliver packets destined for a mobile node's home
               address to its home link.

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.

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.

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 a time (e.g., with different subnet

prefixes), the one registered with the mobile node's
home agent is called its "primary" 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 Key
                     a key used for authenticating Binding Update
                     messages.

    Binding Security Association (BSA)
                     a security association established specifically
                     for the purpose of producing and verifying
                     authentication data passed with a Binding Update
                     destination option.

[4]. Overview of Mobile IPv6

[4.1]. Basic Operation

   A mobile node is always addressable by 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 never mobile. Since the subnet prefix
   of a mobile node's home address is the subnet prefix (or one of the
   subnet prefixes) on the mobile node's home link (it is the mobile
   node's home subnet prefix), packets addressed to it will be routed to
   its home link.

   While a mobile node is attached to some foreign link away from home,
   it is also addressable by 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 the subnet prefix
   (or 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 [27] or
   stateful (e.g., DHCPv6 [2]) Address Autoconfiguration, according
   to the methods of IPv6 Neighbor Discovery [17]. 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.

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. This binding
registration is done by the mobile node sending to the home agent
a packet containing a "Binding Update" destination option; the
home agent then replies to the mobile node by returning a packet
containing a "Binding Acknowledgement" destination option. The
care-of address in this binding registered with its home agent 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.

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 care-of
address. Since the purpose of a Binding Update is to establish
exactly this kind of tunneling, it is specified to 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 10.10 describes the
use of the Binding Update for this purpose.

Section 10.18 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 mobile node, and always tunnels a mobile
node's packets 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.

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 [10] and

thus reaches one of the (possibly many) 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 list of home
agents is maintained by each home agent on the home link through use
of the Home Agent (H) bit in each home agent's periodic unsolicited
multicast Router Advertisements.

The Binding Update and Binding Acknowledgement destination options,
together with a "Binding Request" destination option, are also used
to allow IPv6 nodes communicating with a mobile node, to dynamically
learn and cache the mobile node's binding. 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 an IPv6 Routing
header [6] (instead of IPv6 encapsulation) 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.

Since a Binding Update, Binding Acknowledgement, and Binding Request
are each represented in a packet as an IPv6 destination option [6],
they may be included in any IPv6 packet. Any of these options can be
sent in either of two ways:

  - the messages can be included within any IPv6 packet carrying any
    payload such as TCP [25] or UDP [24].

  - the messages can be sent as a separate IPv6 packet containing
    no payload. In this case, the Next Header field in the last
    extension header in the packet is set to the value 59, to
    indicate "No Next Header" [6].

Mobile IPv6 also defines one additional IPv6 destination option.
When a mobile node sends a packet while away from home, it will
generally set the Source Address in the packet's IPv6 header to one
of its current care-of addresses, and will also 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
that have a Source Address which 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,

yet 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 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 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 option in
a packet.

4.2. New IPv6 Destination Options

As mentioned in Section 4.1, the following four new IPv6 destination
options are defined for Mobile IPv6:

Binding Update

A Binding Update option 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". Any packet that includes a Binding
Update option MUST be protected by some authentication data
(see section 5.1), as defined in Section 4.4, to guard against
malicious Binding Updates. The Binding Update option and
its specific IPsec requirements are described in detail in
Section 5.1.

Binding Acknowledgement

A Binding Acknowledgement option is used to acknowledge receipt
of a Binding Update, if an acknowledgement was requested
in the Binding Update. Any packet that includes a Binding
Acknowledgement option MUST be protected by some authentication
data (see section 5.2), as defined in Section 4.4, to guard
against malicious Binding Acknowledgements. The Binding
Acknowledgement option and its specific IPsec requirements are
described in detail in Section 5.2.

Binding Request

A Binding Request option is used to request a mobile node to
send to the requesting node a Binding Update containing the
mobile node's current binding. This option 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. No authentication
is required for the Binding Request option. The Binding
Request option is described in detail in Section 5.3.

Home Address

> A Home Address 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. 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 10.2
> and 5.4 for additional details about requirements for the
> calculation and verification of the authentication data. The
> Home Address option is described in detail in Section 5.4.

Mobile IPv6 also defines a number of "sub-options" for use within
these destination options; if included, any sub-options MUST
appear after the fixed portion of the option data specified in this
document. The presence of such sub-options will be indicated by the
Option Length field within the option. When the Option Length is
greater than the length required for the option specified here, the
remaining octets are interpreted as sub-options. The encoding and
format of defined sub-options are described in Section 5.5.

4.3. Alignment Requirements for New Destination Options

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]. Mobile IPv6 sub-options have similar
alignment requirements, so that multi-octet values within the
Sub-Option Data field of each sub-option fall on natural boundaries.
The alignment requirement of an option or sub-option is specified in
this document using the standard notation used elsewhere for IPv6
alignment requirements [6]. Specifically, the notation xn+y means
that the Option Type or Sub-Option Type field must fall at an integer
multiple of x octets from the start of the header, plus y octets.
For example:

   2n   means any 2-octet offset from the start of the header.

8n+2 means any 8-octet offset from the start of the header,
      plus 2 octets.

[4.4](). Authentication Requirements for New Destination Options

   Any packet that includes a Binding Update or Binding Acknowledgement
   option has to contain some Authentication Data to guard against
   malicious Binding Updates or Acknowledgements. The way that the
   Authentication Data is computed has to provide sender authentication,
   data integrity protection, and replay protection.

   Mobile IPv6 requires that the Authentication Data covering a Binding
   Update or MUST be computed over a bitstring containing the following
   fields of the IPv6 header and destination options, in order:

      Destination IP Address of the IPv6 header
      Care-of Address, in the Source IP Address of the IPv6 header
      Home Address, from the Home Address destination option
      Option Type of the Binding Update destination option
      Option Length of the Binding Update destination option
      All flags of the Binding Update destination option
      Reserved Field of the Binding Update destination option
      7-bit Prefix Length of the Binding Update destination option
      Authentication Data Length of the Binding Update
      Lifetime of the Binding Update destination option
      Security Parameters Index (SPI) of the Binding Update
      Sequence Number Field of the Binding Update
      The entire data from all Binding Update Sub-Options, if any

   Mobile IPv6 requires that the Authentication Data covering a Binding
   Acknowledgement MUST be computed over a bitstring containing the
   following data, in order:

      Destination IP Address of the IPv6 header
      Source IP Address of the IPv6 header
      Option Type of the Binding Acknowledgement destination
      option
      Option Length of the Binding Acknowledgement
      Status of the Binding Acknowledgement
      Authentication Data Length of the Binding Acknowledgement
      Lifetime of the Binding Acknowledgement destination option
      Security Parameters Index (SPI) of the Binding
      Acknowledgement
      Sequence Number Field of the Binding Acknowledgement
      The entire data from all Binding Acknowledgement
      Sub-Options, if any

   If a Security Association applied to the packet for other reasons
   requires use of ESP [[12]], for example to encrypt the transport layer
   data carried in the packet, this use of ESP is not sufficient to
   satisfy the authentication requirements of Mobile IPv6.

4.5. 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 5.6.

      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 5.7.

   The next two message types are used for network renumbering
   and address configuration on the mobile node, as described in
   Section 9.6:

      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 5.8.

      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 as specified in [Section 5.9](#)

[4.6](). 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 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 [[17]()]. When sending a packet, the Binding
      Cache is searched before the Neighbor Discovery conceptual
      Destination Cache [[17]()] (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 8.9](), for packets originated by this node, or in
         [Section 9.4](), 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 on 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 value of the Prefix Length field received in the Binding Update that created or last modified this Binding Cache entry. 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 8 bits long, and all comparisons between Sequence Number values MUST be performed modulo 2**8. For example, using an implementation in the C programming language, a Sequence Number value A is greater than another Sequence Number value B if ((int)((a) - (b)) > 0), if the "int" data type is a 8-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 Request should be sent when the lifetime on this entry nears expiration.

- The Binding Security Association (BSA) to be be used when authenticating Binding Updates that are received for this Binding Cache entry.

- The Binding Security Association (BSA) to be be used when calculating authentication data for inclusion in Binding Acknowledgements in response to Binding Updates that are received for this Binding Cache entry.

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 and SHOULD NOT be deleted by the home agent until the expiration of its binding lifetime. Other Binding Cache entries 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.

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. 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. That node might still have a Binding Cache entry
    created or updated from this Binding Update, if the Binding
    Update was successfully received by that node (e.g., not
    lost by the network) and 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:

     * the mobile node's home addresses for typical Binding
        Updates (Sections 10.7 and 10.9), or

     * the mobile node's previous care-of address for Binding
        Updates sent to establish forwarding from the mobile
        node's previous care-of address by a home agent from
        this previous care-of address (Section 10.10).

 - 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 8 bits long, and all comparisons between

Sequence Number values MUST be performed modulo 2**8. For
example, using an implementation in the C programming

language, a Sequence Number value A is greater than another
Sequence Number value B if ((int)((a) - (b)) > 0), if the
"int" data type is a 8-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 2,
  error message in response to a Binding Update sent to that
  destination, as described in Section 10.15.

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 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 [17], 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 [17].

        -   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 [17].

                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?

4.7. 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. If the
mobile node has a Binding Security Association (BSA) with that
correspondent node, the mobile node thus returns a Binding Update
to the correspondent node, allowing it to cache the mobile node's
binding for routing future packets to it. Although the mobile node
may request an acknowledgement for this Binding Update, it need not,
since subsequent packets from the correspondent node will continue
to be intercepted and tunneled by the mobile node's home agent,
effectively causing any needed Binding Update retransmission.

If the mobile node receives such a tunneled packet but does not have
a BSA with the correspondent node, the mobile node SHOULD initiate
the process of establishing the necessary security association by
following the procedures outlined in [?].

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 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 Request, it replies by
returning a Binding Update to the node sending the Binding Request.

A mobile node may use more than one care-of address at the same time,
although only one care-of address may be registered for it at its
home agent as its primary care-of address. The mobile node's home
agent will tunnel all intercepted packets for the mobile node to its
(single) registered primary care-of address, but the mobile node
will accept packets that it receives at any of its current care-of
addresses. 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 essential for
scalability and reliability, and for minimizing overall network load.
By caching the care-of address of a mobile node, optimal routing 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.

4.8. Mobile Routers

If a router is itself mobile, and it has acquired a new care-of
address, then that new care-of address should be used by the home
agent for the mobile router, and also to tunnel packets for any home
address that matches the routing prefixes advertised by the mobile
router. The simplest way to do this is for the mobile router to
tell the home agent about the prefix length of the network (and,
consequently, subnets with longer prefixes) being served by the
mobile router. For this purpose, the Mobile Router Prefix Length
Sub-option has been specified (see section 5.5).

This information may be supplied by the mobile router to any
correspondent node; there is no restriction that it be sent only
to Home Agents. However, unless the recipient is itself a router,
it may not have the necessary processing capabilities to make the
entries into its Binding Cache to cover all the matching necessary
for the implied range of Home Addresses. Thus, the sender MUST
be prepared to cease supplying the Mobile Router Prefix Length
Sub-Option to nodes that send back a negative status as part of a
Binding Acknowledgement.

5. New IPv6 Destination Options and Message Types

5.1. Binding Update Option

   The Binding Update destination option is used by a mobile node
   to notify other nodes of a new care-of address for itself. As a
   destination option, it MAY be included in any existing packet being
   sent to this same destination or MAY be sent in a packet by itself;
   a packet containing a Binding Update is sent in the same way as any
   packet sent by a mobile node (Section 10.1).

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                            +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                            | Option Type | Option Length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|A|H|R|D| Reservd |Prefix Length|AuthData Length|   Sequence #  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Lifetime                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Security Parameters Index (SPI)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
=                                                              =
=             Authentication Data (variable length)           =
=                                                              =
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Sub-Options...
+-+-+-+-+-+-+-+-+-+-
```

      Option Type

         198 = 0xC6

      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 8 plus the total length of all sub-options
         present, including their Sub-Option Type and Sub-Option Len
         fields.

      Acknowledge (A)

         The Acknowledge (A) bit is set by the sending mobile node to
         request a Binding Acknowledgement (Section 5.2) 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 the receiving node to act as this node's home agent.
   The destination of the packet carrying this option MUST be that
   of a router sharing the same subnet prefix as the home address
   of the mobile node in the binding (given by the Home Address
   field in the Home Address option in the packet).

Router (R)

   The Router (R) bit, when set, indicates that the sending
   mobile node is a router. This bit is only valid when the
   Home Registration (H) bit is also set, and MUST NOT be set
   otherwise. This bit is saved in the home agent's "home
   registration" Binding Cache entry for the mobile node, and
   is copied into the corresponding bit in all proxy Neighbor
   Advertisement messages sent on behalf of this mobile node by
   the home agent using this Binding Cache entry.

Duplicate Address Detection (D)

   The Duplicate Address Detection (D) bit is set by the sending
   mobile node to request the receiving node (the mobile node's
   home agent) to perform Duplicate Address Detection [27] 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).

Reservd

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

Prefix Length

   The 7-bit Prefix Length field is valid only for a "home
   registration" Binding Update; this field MUST be zero if the
   Home Registration (H) bit is not set in the Binding Update.
   The Prefix Length field is set by the sending mobile node to
   the (nonzero) length of its subnet prefix in its home address
   (given in the Home Address option in the packet) to request
   its home agent to use the interface identifier in the mobile
   node's home address (the remaining low-order bits after the
   indicated subnet prefix) to form all other home addresses for

the mobile node on the home link. The home agent becomes the
home agent not only for the individual home address given in

this binding, but also for all other home addresses for this
mobile node formed from this interface identifier. That is,
for each on-link prefix on the home link, the home agent uses
the interface identifier to form other valid addresses for
the mobile node on the home link, and acts as a home agent
also for those addresses. In addition, the home agent forms
the link-local address and site-local address corresponding
to this interface identifier, and defends each for purposes
of Duplicate Address Detection. The home agent also performs
Duplicate Address Detection on at least one such address as
part of the home registration processing (before returning
the Binding Acknowledgement), if the Duplicate Address
Detection (D) bit is set in the Binding Update; it is not
necessary to perform Duplicate Address Detection individually
on each of these addresses, since address uniqueness here is
determined solely by the interface identifier [27]. Details of
this operation are described in Section 9.1.

AuthDataLength

The length of the Authentication Data field in octets.

Sequence #

An 8-bit number sed 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**8, as
defined in Section 4.6). There is no requirement, however,
that the Sequence Number value strictly increase by 1 with each
new Binding Update sent or received.

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.

Security Parameters Index (SPI)

The SPI is an arbitrary 32-bit value that, in combination with
the destination IP address, uniquely identifies the Binding
Security Association (BSA) for this datagram. The set of
SPI values in the range 1 through 255 are reserved by the
Internet Assigned Numbers Authority (IANA) for future use;

a reserved SPI value will not normally be assigned by IANA
unless the use of the assigned SPI value is specified in an

RFC. It is ordinarily selected by the destination system upon
establishment of an BSA.

The SPI value of zero (0) is reserved for local,
implementation-specific use and MUST NOT be sent on the
wire. For example, a key management implementation MAY use the
zero SPI value to mean "No Binding Security Association Exists"
during the period when the implementation has requested that
its key management entity establish a new SA, but the SA has
not yet been established.

Authentication Data

This is a variable-length field that contains the
Authentication Data necessary to secure this Binding Update.
The field must be an integral multiple of 32 bits in length.
The details of the authentication calculation are given
in Section 4.4. This field may include explicit padding,
depending upon the requirements of the algorithm selected by
the SPI.

Sub-Options

Additional information, associated with this Binding Update
option, that need not be present in all Binding Updates sent.
This use of sub-options also allows for future extensions to
the format of the Binding Update option to be defined. The
encoding and format of defined sub-options are described in
Section 5.5. The following sub-options are valid in a Binding
Update option:

 - Unique Identifier Sub-Option

 - Mobile Router Prefix Length Sub-Option

 - Alternate Care-of Address Sub-Option

The alignment requirement [6] for the Binding Update option is 4n+2.

Any packet that includes a Binding Update option MUST also include
a Home Address option. The home address of the mobile node in the
binding given in the Binding Update option is that which was received
as the value of the Home Address field in the Home Address option in
the packet.

The care-of address for the binding given in the Binding Update
option 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 option. However, a care-of address different from the Source

Address MAY be specified by including an Alternate Care-of Address
sub-option in the Binding Update option.

If the care-of address for the binding (specified either in an
Alternate Care-of Address sub-option in the Binding Update option, if
present, or in the Source Address field in the packet's IPv6 header)
is equal to the home address of the mobile node, the Binding Update
option indicates that any existing binding for the mobile node MUST
be deleted. Likewise, if the Lifetime field in the Binding Update
option is equal to 0, the Binding Update option indicates that any
existing binding for the mobile node MUST be deleted. In each of
these cases, a Binding Cache entry for the mobile node MUST NOT be
created in response to receiving the Binding Update.

When the care-of address is NOT equal to the home address,
what if we just delete that particular care-of address?

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; the last 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. Thus, the mobile
node's and the correspondent node's knowledge of the last sequence
number expire at the same time. If the sending mobile node has no
Binding Update List entry, the Sequence Number may start at any
value; if the receiving correspondent node has no Binding Cache entry
for the sending mobile node, it MUST accept any Sequence Number value
in a received Binding Update from this mobile node.

The three highest-order bits of the Option Type are encoded to
indicate specific processing of the option [6]. For the Binding
Update 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.

[5.2](). Binding Acknowledgement Option

The Binding Acknowledgement destination option is used to acknowledge
receipt of a Binding Update option ([Section 5.1]()). When a node
receives a packet containing a Binding Update option, with this
node being the destination of the packet (only the destination node
processes the option since it is a destination option), this node
MUST return a Binding Acknowledgement to the source of the packet,
if the Acknowledge (A) bit is set in the Binding Update. As a
destination option, this node MAY include the Binding Acknowledgement
in any existing packet being sent to the mobile node or MAY send it
in a packet by itself. A packet containing a Binding Acknowledgement
is sent in the same way as any packet to a mobile node, using a
Routing header to route the packet to the mobile node by way of the
care-of address in the binding ([Section 8.9]()).

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                                +-+-+-+-+-+-+-+-+
                                                | Option Type   |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | Option Length |    Status     |AuthData Length|   Sequence #  |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                           Lifetime                            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                 Security Parameters Index (SPI)               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                           Refresh                            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                              |
 =              Authentication Data (variable length)          =
 |                                                              |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |   Sub-Options...
 +-+-+-+-+-+-+-+-+-+-+-+-+-
```

   Option Type

       7

   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 11 plus the total length of all sub-options

present, including their Sub-Option Type and Sub-Option Len
fields.

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
      136   Incorrect interface identifier length
      137   Not home agent for this mobile node
      138   Duplicate Address Detection failed
      139   No security association
      140   Mobile Router Prefix Length Sub-Option Rejected
      141   Sequence number too small

   Up-to-date values of the Status field are to be specified in
   the most recent "Assigned Numbers" [26].

AuthDataLength

   The length of the Authentication Data field in octets.

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 will
   attempt to retain the entry for this mobile node in its Binding
   Cache. 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.

Security Parameters Index (SPI)

   The SPI is an arbitrary 32-bit value that, in combination
   with the destination IP address, uniquely identifies the
   BSA for this datagram. The set of SPI values in the range
   1 through 255 are reserved by the Internet Assigned Numbers
   Authority (IANA) for future use; a reserved SPI value will not
   normally be assigned by IANA unless the use of the assigned
   SPI value is specified in an RFC. It is ordinarily selected by
   the destination system upon establishment of an SA (see the
   Security Architecture document for more details).

   The SPI value of zero (0) is reserved for local,
   implementation- specific use and MUST NOT be sent on
   the wire.

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.

Authentication Data

   This is a variable-length field that contains the
   Authentication Data necessary to secure this Binding Update.
   The field must be an integral multiple of 32 bits in length.
   The details of the authentication data computation are
   described in Section 4.4. This field may include explicit

padding, depending upon the requirements of the algorithm
selected by the SPI.

Sub-Options

Additional information, associated with this Binding
Acknowledgement option, that need not be present in all Binding
Acknowledgements sent. This use of sub-options also allows for
future extensions to the format of the Binding Acknowledgement
option to be defined. Currently, no valid sub-options are
defined for a Binding Acknowledgement option.

The alignment requirement [6] for the Binding Acknowledgement option
is 4n+3.

Any packet that includes a Binding Acknowledgement option MUST
contain authentication data to guard against malicious Binding
Updates. The computation for this authentication data must follow
the rules in Section 4.4.

If the node returning the Binding Acknowledgement accepted the
Binding Update for which the Acknowledgement is being returned (the
value of the Status field in the Acknowledgement is less than 128),
this node will have an entry for the mobile node in its Binding
Cache and MUST use this entry (which includes the care-of address
received in the Binding Update) in sending the packet containing the
Binding Acknowledgement to the mobile node. The details of sending
this packet (using a Routing header) to the mobile node are the same
as for sending any packet to a mobile node using a binding, as are
described in Section 8.9.

If the node returning the Binding Acknowledgement instead
rejected the Binding Update (the value of the Status field in the
Acknowledgement is greater than or equal to 128), this node MUST
similarly use a Routing header in sending the packet containing the
Binding Acknowledgement, as described in Section 8.9, but MUST NOT
use its Binding Cache in forming the IP header or Routing header
in this packet. Rather, the care-of address used by this node in
sending the packet containing the Binding Acknowledgement MUST be
copied from the care-of address received in the rejected Binding
Update; this node MUST NOT modify its Binding Cache in response
to receiving this rejected Binding Update and MUST ignore its
Binding Cache in sending the packet in which it returns this Binding
Acknowledgement. The packet is sent using a Routing header, routing
the packet to the home address of the rejected Binding Update by
way of the care-of address indicated in the packet containing the
Binding Update. When sending a Binding Acknowledgement to reject a
Binding Update, the Binding Acknowledgement MUST be sent in an IPv6
packet containing no payload (with the Next Header field in the last
extension header in the packet set to indicate "No Next Header" [6]).

The three highest-order bits of the Option Type are encoded to
indicate specific processing of the option [6]. For the Binding
Acknowledgement option, these three bits are set to 000, indicating

that any IPv6 node processing this option that does not recognize the
Option Type must skip over this option and continue processing the
header, and that the data within the option cannot change en-route to
the packet's final destination.

If the mobile node sends a sequence number which is not greater than
the sequence number from the last successful Binding Update, 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.

5.3. **Binding Request Option**

   The Binding Request destination option is used to request a mobile
   node's binding from the mobile node. As a destination option, it
   MAY be included in any existing packet being sent to the mobile
   node or MAY be sent in a packet by itself; a packet containing a
   Binding Request option is sent in the same way as any packet to a
   mobile node (Section 8.9). When a mobile node receives a packet
   containing a Binding Request option, it SHOULD return a Binding
   Update (Section 5.1) to the source of the Binding Request.

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

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

      Option Type

         8

      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 0 plus the total length of all sub-options
         present, including their Sub-Option Type and Sub-Option Len
         fields.

      Sub-Options

         Additional information, associated with this Binding Request
         option, that need not be present in all Binding Requests sent.
         This use of sub-options also allows for future extensions to
         the format of the Binding Request option to be defined. The
         encoding and format of defined sub-options are described in
         Section 5.5. The following sub-options are valid in a Binding
         Request option:

           - Unique Identifier Sub-Option

   There is no requirement for alignment [6] of the Binding Request
   option.

   The three highest-order bits of the Option Type are encoded to
   indicate specific processing of the option [6]. For the Binding

Request option, these three bits are set to 000, indicating that any
IPv6 node processing this option that does not recognize the Option

   Type must skip over this option and continue processing the header,
   and that the data within the option cannot change en-route to the
   packet's final destination.

[5.4](#). Home Address 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 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.

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                            +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                            | Option Type  | Option Length |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 +                                                               +
 |                                                               |
 +                        Home Address                           +
 |                                                               |
 +                                                               +
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |   Sub-Options...
 +-+-+-+-+-+-+-+-+-+-+-
```

      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 plus the total length of all sub-options
         present, including their Sub-Option Type and Sub-Option Len
         fields.

      Home Address

         The home address of the mobile node sending the packet.

   Sub-Options

      Additional information, associated with this Home Address
      option, that need not be present in all Home Address options
      sent. This use of sub-options also allows for future
      extensions to the format of the Home Address option to be
      defined. Currently, no valid sub-options are defined for use
      in a Home Address option.

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

The inclusion of a Home Address 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.

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

No 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 13. 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 10.2.

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 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.

5.5. **Mobile IPv6 Destination Option Sub-Options**

   In order to allow optional fields that may not be needed in every
   use of any given Mobile IPv6 destination option, and to allow future
   extensions to the format of these destination options to be defined,
   any of the Mobile IPv6 destination options defined in this document
   MAY include one or more sub-options.

   Such sub-options are included in the data portion of the destination
   option itself, after the fixed portion of the option data specified
   for that particular destination option (Sections 5.1 through 5.4).
   The presence of such sub-options will be indicated by the Option
   Length field. When the Option Length is greater than the standard
   length defined for that destination option, the remaining octets are
   interpreted as sub-options.

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

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

      Sub-Option Type

         8-bit identifier of the type of sub-option. When processing
         a Mobile IPv6 destination option containing a sub-option for
         which the Sub-Option Type value is not recognized by the
         receiver, the receiver SHOULD quietly ignore and skip over the
         sub-option, correctly handling any remaining sub-options in the
         option.

      Sub-Option Length

         8-bit unsigned integer. Length of the Sub-Option Data field
         of this sub-option, in octets. The Sub-Option Len does not
         include the length of the Sub-Option Type and Sub-Option Len
         fields.

      Sub-Option Data

         Variable-length field. Sub-Option-Type-specific data.

   As with IPv6 options appearing in a Hop-by-Hop Options header
   or Destination Options header [6], individual sub-options within
   a Mobile IPv6 destination option may have specific alignment

requirements, to ensure that multi-octet values within Sub-Option
Data fields fall on natural boundaries. The alignment requirement

of each sub-option is specified as part of the definition of each
sub-option below.

Each section above defining the Mobile IPv6 destination options
specifies which of the defined sub-options is valid for that
destination option. In addition, there are two padding sub-options,
Pad1 and PadN (defined below), which are used when necessary to align
subsequent sub-options. The Pad1 and PadN sub-options are valid for
all Mobile IPv6 destination options. Unlike the padding options
used in Hop-by-Hop Options header or Destination Options header [6],
there is no requirement for padding the total size of any Mobile IPv6
destination option to a multiple of 8 octets in length, and the
Pad1 and PadN sub-options SHOULD NOT be used for this purpose. All
Mobile IPv6 sub-options defined in this document MUST be recognized
by all Mobile IPv6 implementations.

Currently, the following sub-option types are defined for use in
Mobile IPv6 destination options:

Pad1 Sub-Option   (alignment requirement: none)

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

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

   The Pad1 sub-option is used to insert one octet of padding
   into the Sub-Options area of a Mobile IPv6 option. If more
   than one octet of padding is required, the PadN sub-option,
   described next, should be used, rather than multiple Pad1
   sub-options.

PadN Sub-Option   (alignment requirement: none)

```
    0                   1
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -
   |       1       | Sub-Option Len| Sub-Option Data
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -
```

   The PadN sub-option is used to insert two or more octets of
   padding into the Sub-Options area of a Mobile IPv6 option.
   For N octets of padding, the Sub-Option Len field contains
   the value N-2, and the Sub-Option Data consists of N-2

zero-valued octets.

Unique Identifier Sub-Option   (alignment requirement: 2n)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       2       |       2       |      Unique Identifier        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The Unique Identifier sub-option is valid only in Binding
Request and Binding Update destination options. 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 Binding Update to identify
the specific Binding Request to which it responds. This
matching of Binding Updates to Binding Requests is required
in the procedure for renumbering the home subnet while a
mobile node is away from home (Section 9.6).

Mobile Router Prefix Length Sub-Option   (alignment requirement:
2n+1)

```
 0                   1                   2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       3       |       1       |x|Prefix Length|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The Mobile Router Prefix Length Sub-Option is valid only
in the Binding Update destination option. The Prefix
Length field contains a 7-bit value that serves to notify
the recipient that the care-of address may be used for
delivery of packets to any home address whose initial
Prefix-Length address bits match the corresponding bits of
the home address reported in the Home Address destination
option, which MUST also be present in the same message.
See section 4.8 for a discussion about the use of this
Sub-Option.

If a node receives the Mobile Router Prefix Length
Sub-Option, and it cannot carry out the necessary matching
operations with relevant Binding Cache entries, the node
MUST return a Binding Acknowledgement message including
status code 140.

Alternate Care-of Address Sub-Option   (alignment requirement: 8n+6)

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

The Alternate Care-of Address sub-option is valid only in
Binding Update destination options. 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.

5.6. **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 9.8 and 10.8. 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 [10], and one of the home agents there responds to the mobile
   node 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.

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

      Type

         <To Be Assigned by IANA>

      Code

         0
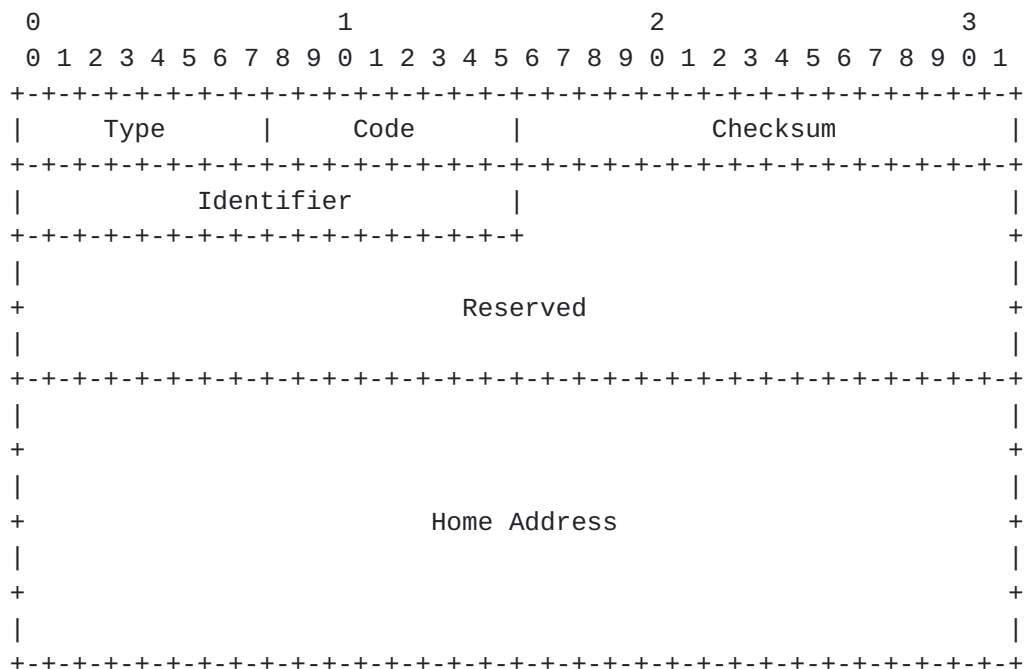
      Checksum

         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.

Home Address

> The home address of the mobile node sending the Home Agent
> Address Discovery Request message.

The Source Address of the Home Agent Address Discovery Request
message packet MUST be one of the mobile node's current care-of
addresses, and the mobile node MUST NOT include a Home Address
option in this packet; the home agent then MUST return the Home
Agent Address Discovery Reply message directly to this care-of
address. These restrictions are necessary, since at the time of
performing this dynamic home agent address discovery, the mobile node
is generally not registered with its home agent; using the mobile
node's care-of address simplifies the return of the Reply message to
the mobile node.

If the mobile node does not have a home address, then the Home
Address field MUST be set to the unspecified address (0::0).

5.7. **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 9.8 and 10.8.
   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 [10], and one of the home agents there responds to the
   mobile node 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.

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

   Type

      <To Be Assigned by IANA>

   Code

      0
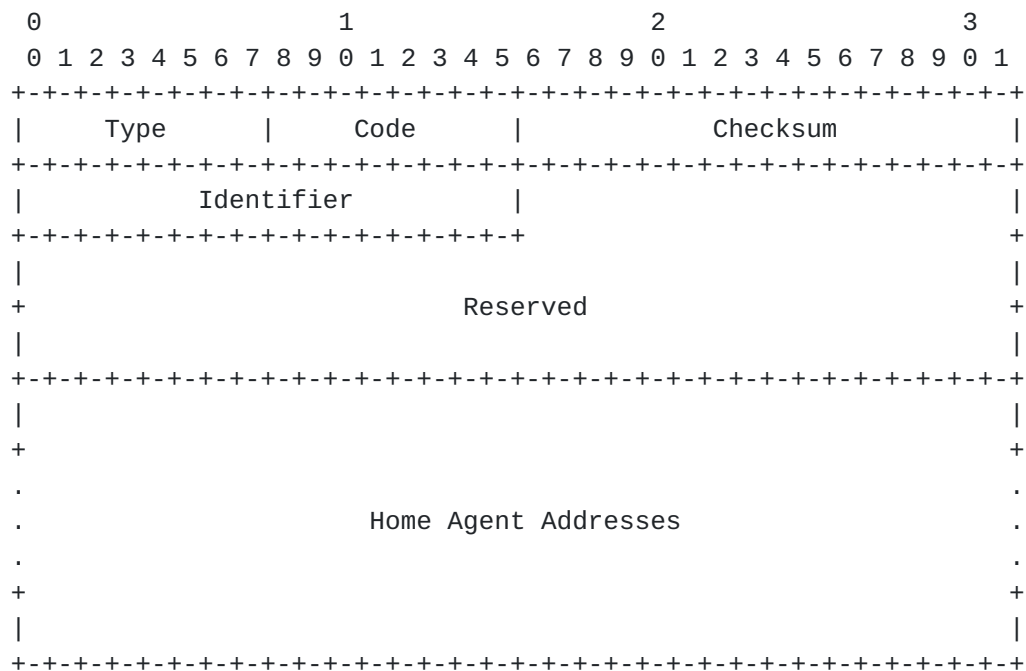
   Checksum

      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
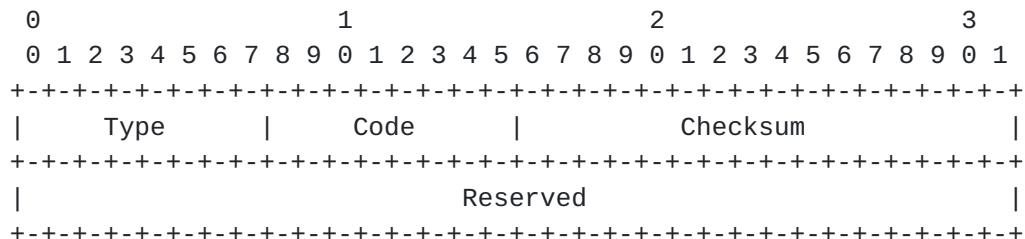   the Home Agent Address Discovery Reply message.

5.8. **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 [27],
   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 [17], 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.

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

   IP Fields:

      Source Address

         The mobile node's care-of address.

      Destination Address

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

      Hop Limit

         Set to an initial hop limit value, and this message is routed
         according to the rules of a typical unicast packet. A hop
         limit of 64 is currently suggested [26].

      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

    <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.

5.9. **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 5.9.

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

IP Fields:

   Source Address

              The home agent's address as the mobile node would
              expect to see it (i.e. same 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

              This header MUST be sent, unless the mobile node
              has not yet configured, and is using its care-of
              address. [subject to change]

ICMP Fields:

   Type

      <To Be Assigned by IANA>

   Code

      0

   Checksum

      The ICMP checksum [5].

Options:

Prefix Information

> Each message contains one or more Prefix Information options,
> which contain the prefix(es) the mobile node should configure
> its home address(es) with. Section 9.6 describes which
> prefixes should be advertised to the mobile node.
>
> The Prefix Information option is defined in Section 4.6.2
> of [17], with modifications defined in Section 6.2 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 9.8.1.

The Mobile Prefix Advertisement sent by the home agent MAY include
the Source Link-layer Address option defined in RFC 2461 [17], or the
Advertisement Interval option specified in Section 6.3.

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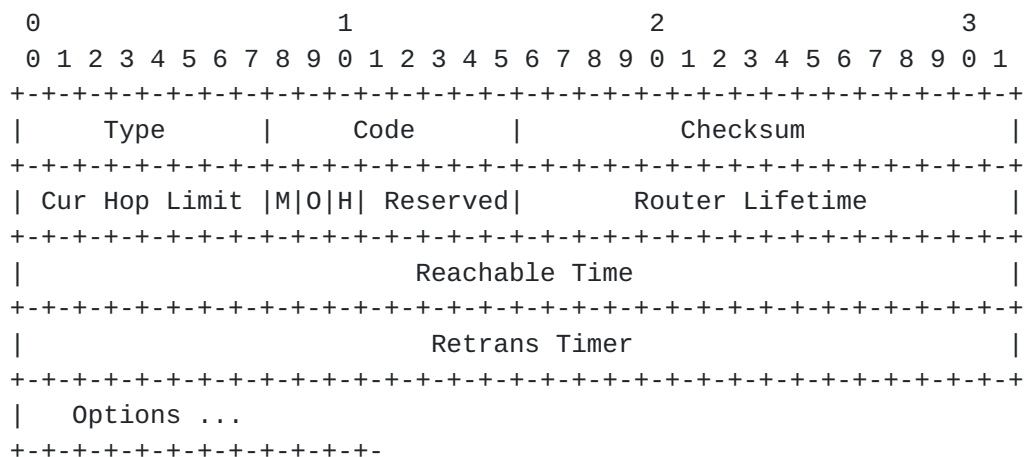continue processing the message.

6. Modifications to IPv6 Neighbor Discovery

6.1. Modified Router Advertisement Message Format

Mobile IPv6 modifies the format of the Router Advertisement
message [17] by the addition of a single flag bit to indicate that
the router sending the Advertisement message is serving as a home
agent on this link. The format of the Router Advertisement message
is as follows:

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

This format represents the following changes over that originally
specified for Neighbor Discovery [17]:

   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
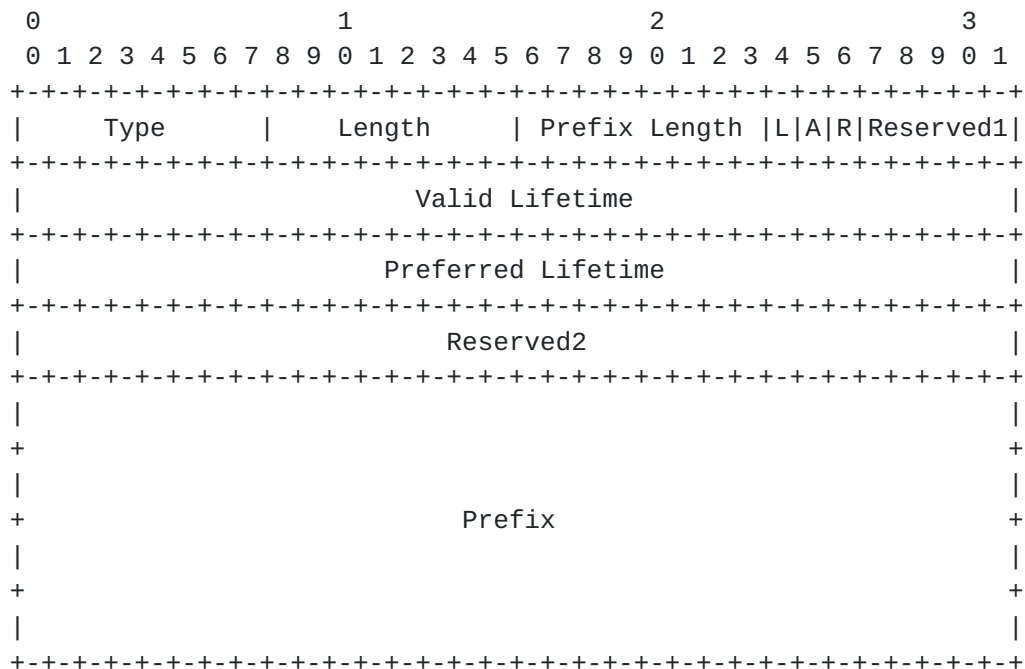   addition of the Home Agent (H) bit.

6.2. 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 9.8 and 10.8).

  - 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 10.10).

However, Neighbor Discovery [17] 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:

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

This format represents the following changes over that originally
specified for Neighbor Discovery [17]:

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 [17]. 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.

6.3. New Advertisement Interval Option Format

Mobile IPv6 defines a new Advertisement Interval option, used in
Router Advertisement messages to advertise the interval at which the
sending router sends unsolicited multicast Router Advertisements.
The format of the Advertisement Interval option is as follows:

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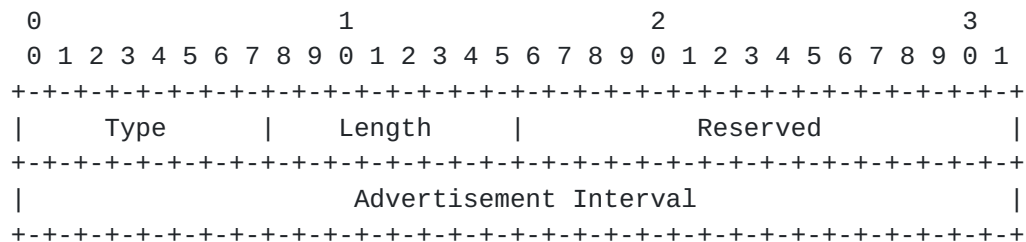
   Type

      7

   Length

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

   Reserved

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

   Advertisement Interval

      32-bit unsigned integer. The maximum time, in milliseconds,
      between successive unsolicited router Router Advertisement
      messages sent by this router on this network interface. Using
      the conceptual router configuration variables defined by
      Neighbor Discovery [17], 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
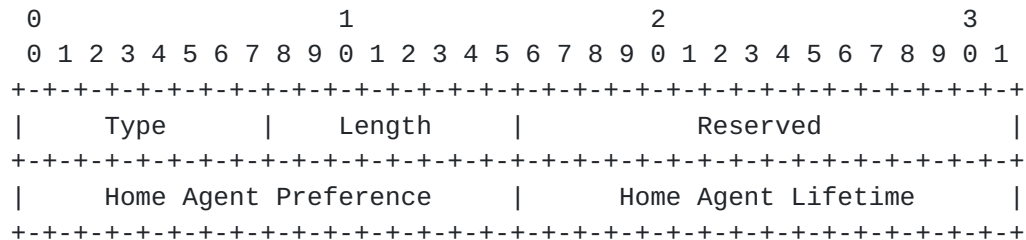in its movement detection algorithm, as described in Section 10.4.

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

6.4. 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:

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

      Type

         8

      Length

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

      Reserved

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

      Home Agent Preference

         16-bit signed, 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 7.3. 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 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. 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 specified in the main body of the
Router Advertisement message.

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 6.1) is not set.

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.

6.5. Changes to Sending Router Advertisements

   The Neighbor Discovery protocol specification [17] 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 6.2) in each.

6.6. Changes to Sending Router Solicitations

In addition to the limit on routers sending unsolicited multicast Router Advertisement messages (Section 6.5), 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 10.4](#)) determines that it has moved and that its current
care-of address might no longer be valid.

7. **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.

7.1. **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 process a Binding Update option
      received in a packet, 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.

7.2. **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 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 6.5. 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.

7.3. **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 be able to return a Binding Acknowledgement
    option 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 4.6.

-   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 [10], and MUST be
    able to participate in dynamic home agent address discovery
    (Section 9.8).

-   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.

7.4. 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

decapsulation [4].

- Every IPv6 mobile node MUST support sending Binding Update
  options, as specified in Sections 10.7, 10.9, and 10.10; and MUST
  be able to receive and process Binding Acknowledgement options,
  as specified in Section 10.13.

- Every IPv6 mobile node MUST support use of the dynamic home agent
  address discovery mechanism, as described in Section 10.8.

- 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 Request
  option, by responding with a Binding Update option.

- Every IPv6 mobile node MUST support sending packets containing a
  Home Address option; this option MUST be included in all packets
  sent while away from home, if 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 4.6.

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

8. **Correspondent Node Operation**

   A correspondent node is any node communicating with a mobile node.
   The correspondent node, itself, may be stationary or mobile, and may
   possibly also be functioning as a home agent for Mobile IPv6. The
   procedures in this section thus apply to all IPv6 nodes.

8.1. **Receiving Packets from a Mobile Node**

   Packets sent by a mobile node while away from home generally include
   a Home Address option. When any node receives a packet containing
   a Home Address option, 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 not
   be performed until after all processing of other options contained
   in the same Destination Options extension header is completed.
   Currently, no other such options are defined.

   Further processing of such a packet after all IPv6 options processing
   (e.g., at the transport layer) thus does not need 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.

8.2. **Receiving Binding Updates**

   Upon receiving a Binding Update option in some packet, the receiving
   node MUST validate the Binding Update according to the following
   tests:

   - The packet meets the specific authentication requirements for
      Binding Updates, defined in Section 4.4.

   - The packet MUST contain a Home Address option.

   - The Option Length field in the Binding Update option is greater
      than or equal to the length specified in Section 5.1.

   - The Sequence Number field in the Binding Update option is greater
      than the Sequence Number received in the previous Binding Update
      for this home address, if any. As noted in Section 4.6, this
      Sequence Number comparison MUST be performed modulo 2**8.

Any Binding Update not satisfying all of these tests 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 9.1; otherwise, it is processed
  according to the procedure specified in Section 8.3.

- 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 9.2; otherwise, it is processed
  according to the procedure specified in Section 8.4.

8.3. 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 8.2. 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 new 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 of this lifetime in the Binding Cache entry.

8.4. 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 8.2. 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. In this case, the receiving node MUST
delete any existing entry in its Binding Cache for this mobile node.

8.5. Sending Binding Acknowledgements

When any node receives a packet containing a Binding Update option
in which the Acknowledge (A) bit is set, it MUST return a Binding
Acknowledgement option 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, and the `A' bit
was set in the Binding Update, 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 sent, 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 5.2 and in the most
recent "Assigned Numbers" [26].

The packet in which the Binding Acknowledgement is returned MUST meet
the specific IPsec requirements for Binding Acknowledgements, defined
in Section 4.4; and the packet MUST be sent using a Routing header
in the same way as any other packet sent to a mobile node using a
care-of address (even if the binding was rejected), as described in
Section 8.9.

In response to a Binding Update, a node MAY send a Binding
Acknowledgement even when the 'A' bit is not set in the Binding
Update. This would happen, for instance, if a mobile node attempted
to send a Binding Update with the 'H' bit set to a correspondent
node.

8.6. Sending Binding 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 Request option to the mobile node in
an attempt to avoid this overhead and latency due to deleting and
recreating the Binding Cache entry. Since a Binding Request is a
destination option, it may, for example, be included in any packet
already being sent to the mobile node, such as a packet that is part
of ongoing TCP communication with the mobile node. When the mobile
node receives a packet from some sender containing a Binding Request
option, it returns a Binding Update option to that sender, giving its
current binding and a new lifetime.

8.7. Cache Replacement Policy

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. 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. When a Binding Cache entry's timer
expires, the node deletes the entry.

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 9.1) MUST NOT be deleted from the cache until
the expiration of its lifetime period. When attempting to add a
new "home registration" entry in response to a Binding Update with
the Home Registration (H) bit set, if insufficient space exists
(and sufficient space cannot be reclaimed) in the node's Binding
Cache, the node MUST reject the Binding Update and SHOULD 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 a "home registration" entry, 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 a "home registration"

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. As when a Binding
Cache entry is initially created, 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 add an entry again for this destination mobile
node to its Binding Cache.

8.8. 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 10.10 (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 MUST 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.

8.9. 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 0 Routing header [6], 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 0 Routing header [6], 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). Normal processing of
the Routing header by the mobile node will then proceed as follows:

 - The mobile node swaps the Destination Address in the packet's
   IPv6 header and the Address specified in the Routing header.
   This results in the packet's IP Destination Address being set to
   the mobile node's home address.

 - The mobile node then resubmits the packet to its IPv6 module for
   further processing, "looping back" the packet inside the mobile
   node. Since the mobile node recognizes its own home address as
   one of its current IP addresses, the packet is processed further

within the mobile node, in the same way then as if the mobile
node was at home.

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 9.4. The mobile node will then send
a Binding Update to the sending node, as described in Section 10.9,
allowing the sending node to create a Binding Cache entry for its use
in sending subsequent packets to this mobile node.

9. **Home Agent Operation**

9.1. **Primary Care-of Address Registration**

When a node receives a Binding Update, it MUST validate it and
determine the type of Binding Update according to the steps described
in Section 8.2. 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
  SHOULD 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 Prefix Length field is nonzero in the Binding Update
  and this length differs from the length of the home agent's own
  knowledge of the corresponding subnet prefix on the home link,
  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 136 (incorrect subnet prefix length).

- 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.

- Finally, if the Duplicate Address Detection (D) bit is set in
  the Binding Update, this home agent MUST perform Duplicate
  Address Detection [27] on the mobile node's home link for the
  home address in this binding (before returning the Binding
  Acknowledgement); if the 7-bit Prefix Length field is nonzero
  in the Binding Update, the home agent SHOULD perform Duplicate
  Address Detection for only one of the addresses formed from the
  interface identifier for this binding, and if so, 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 [17, 27]; 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 SHOULD return a Binding Acknowledgement to the
mobile node, in which the Status field is set to 138 (Duplicate
Address Detection failed).

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 for this mobile node, 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 sub-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 8.7) and MUST NOT be
removed from the Binding Cache until the expiration of the Lifetime
period.

In addition, the home agent MUST copy the Router (R) bit from the
Binding Update into the corresponding bit in this Binding Cache entry
for this mobile node.

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 [17].

If the 7-bit Prefix Length field in the Binding Update is nonzero,
the Home Agent creates or updates Binding Cache entries for each of
possible several home addresses. The set of such home addresses
is formed by replacing the routing prefix (as determined by the
Prefix Length field value) 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. Furthermore, if the 7-bit Prefix
Length field in the Binding Update is nonzero, then 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.

The Prefix Length in the Binding Update MUST also be saved in the
Binding Cache entry.

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 indicating success; this
     value MUST be less than 128. The only currently defined success
     Status value is 0, indicating simply that the Binding Update was
     accepted.

  - 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 9.3 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.

9.2. **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 8.2. 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 in its Binding Cache for this
      mobile node that is marked as a "home registration", 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 indicating success (the
      value MUST be less than 128). The only currently defined success
      Status value is 0, indicating simply that the Binding Update was
      accepted.

   - 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 addressed to the mobile node (Section 9.3).

9.3. **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 addressed to the mobile node,
   and MUST tunnel each intercepted packet to the mobile node using
   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 [17] on
behalf of the mobile node. Specifically, the home agent performs the
following steps:

- The home agent examines the value of the Prefix Length field
  in the new "home registration" Binding Cache entry. If this
  value is zero, the following step is carried out only for the
  individual home address specified for this binding. If, instead,
  this field is nonzero, 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 indicated
  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 multicasts onto the
  home link (to the all-nodes multicast address) a Neighbor
  Advertisement message [17] on behalf of the mobile node, to
  advertise the home agent's own link-layer address for this IP
  address.

  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 [17], 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 copied from
    the corresponding bit in the home agent's Binding Cache entry
    for the mobile node.

  * 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 multicasts on the local link (such as
Ethernet) are 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 [17].

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 [17] 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". This check MUST include all possible
home addresses for the mobile node, based on the subnet prefixes
currently considered to be on-link by the home agent (including the
corresponding link-local address and site-local address), if the
Prefix Length in the Binding Cache entry for this mobile node (from
the Binding Update that created this Cache entry) is nonzero.

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 [17].

9.4. 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 8.9 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 9.3. 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 [11] or ESP [12] 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 prepended 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.

9.5. Handling Reverse Tunneled Packets from a Mobile Node

   A home agent MUST support decapsulating reverse tunneled packets
   sent to it from a mobile node's home address. Such reverse tunneled
   packets MAY be discarded unless accompanied by a valid AH. This
   support for reverse tunneling allows mobile nodes to defeat certain
   kinds of traffic analysis. Requiring AH on reverse tunneled packets
   allows the home agent to protect the home network against unwarranted
   intrusions by malicious nodes masquerading as a mobile node with a
   home address on the network served by the home agent.

9.6. Home Prefix Propagation

   IPv6 provides mechanisms as part of Neighbor Discovery [17] and
   Address Autoconfiguration [27] to aid in mobile node configuration
   when a mobile node turns on, and in renumbering a subnet, such as
   when a site switches to a new network service provider.

   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 for the case in which one or more mobile
   nodes using the old prefixes are away from home and registered at the
   home agent while the renumbering takes place.

   In the IPv6 renumbering mechanism, nodes on the visited link receive
   Mobile Prefix Advertisements messages with Prefix Information
   Options, which give the valid lifetime and preferred lifetime for
   available prefixes on the link [17].

   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. 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 [13, 11, 12] if a
   security associate exists (i.e. unless the mobile node does not yet
   have a home address configured).

9.7. 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 9.8.
   The information for the list is learned through receipt of the

periodic unsolicited multicast Router Advertisements from each other
home agent on the link, in which the Home Agent (H) bit is set, in a

manner similar to the Default Router List conceptual data structure
maintained by each host for Neighbor Discovery [17].

On receipt of a valid Router Advertisement, as defined in the
processing algorithm specified for Neighbor Discovery [17], 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,
  skip all of the following steps. There are no special processing
  steps required by Mobile IP for this Router Advertisement, since
  the Advertisement was not sent by a home agent.

- 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 [17].

- 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 6.2). 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.

9.8. Dynamic Home Agent Address Discovery

A mobile node, while away from home, MAY use the dynamic home agent
address discovery mechanism in section 10.8 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 10.8, 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 [10] 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 4.6). 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 4.6, 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.

9.8.1. Aggregate List of Home Network Prefixes

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 [17]). 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 [17].

  - 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 [17]) and section
    5.5.3 of RFC 2462 (Stateless Address Autoconfiguration [27]).

  - 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, possibly including Binding
Acknowledgement or Binding Request destination options, for delivery
to a mobile node for which it is maintaining a current binding.
It may be possible to construct an aggregate list by combining
information contained in the home agent's AdvPrefixList and its
Home Agent List used for Dynamic Home Agent Address Discovery
(Section 10.8).

9.8.2. 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
     changes

  - The mobile node requests the information with a Router
     Solicitation (see section 10.16).

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, and
     calculate RAND_ADV_DELAY in order to randomize the time at which
     the transmission is scheduled.

- If there are any uncknowledged changes to prefix information when
  a Binding Update arrives for the home registration, send a Mobile
  Prefix Advertisement to the mobile node immediately. The Mobile
  Prefix Advertisement SHOULD have the Binding Acknowledgement as a
  Destination Option. If an advertisement was previously scheduled
  for the mobile node, cancel that advertisement.

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

If the home agent already has scheduled the transmission of a Router
Advertisement to the mobile node, and if the freshly calculated
RAND_ADV_DELAY would cause another transmission BEFORE the Preferred
Lifetime of the mobile node's home address derived from the prefix
whose advertisement information has changed, then add the new
information to be transmitted to the existing scheduled transmission.
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.

If the mobile node's binding expires before the Preferred Lifetime,
then return. The mobile node will get the revised information wth
its next Binding Acknowledgement. Otherwise, continue with the
following computation.
    MAX_SCHEDULE_DELAY == min (MAX_PFX_ADV_DELAY, Preferred Lifetime)
for the newly advertised Preferred Lifetime.

Then compute RAND_ADV_DELAY ==
    MinRtrAdvInt + rand()*(MAX_SCHEDULE_DELAY - MinRtrAdvInt)

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.

9.8.3. 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 [13, 11, 12] 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.

   - The advertisement MUST include a Binding Request destination
      option 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 Request destination
      option MUST include a Unique Identifier Sub-Option (Section 5.5),
      with the unique identifier in the sub-option data set to a value
      different than that in any other Binding 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 Requests that contain a Unique
      Identifier Sub-Option, incremented each time a Binding Request
      containing a Unique Identifier Sub-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).

   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 Request in the packet (i.e., with matching
   Sequence Number). 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 Request if it specifies a
binding for the mobile node to which the Binding Request was sent
and contains a Unique Identifier Sub-Option matching the unique
identifier sent in the Unique Identifier Sub-Option in the Binding
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
sectino 9.8.2. The home agent MUST generate a new unique identifier
for use in the Unique Identifier Sub-Option in the Binding Request
tunneled with the new Mobile Prefix Advertisement.

9.8.4. Lifetimes for Changed Prefixes

As described in Section 9.1, the lifetime returned by the home
agent in a Binding Acknowledgement MUST be no greater than the
remaining valid lifetime for the subnet prefix in the mobile node's
home address. Furthermore, as described in Section 10.9, 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. These limits on the binding lifetime serve
to prohibit use of a mobile node's home address after it becomes
invalid. The mobile node SHOULD further limit the lifetimes that it
sends on any Binding Updates to be within the remaining preferred
lifetime 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 ndoe MUST issue a Binding Update to all such correspondent
nodes.

[10]. Mobile Node Operation

[10.1]. 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. Doing
      so also makes the node's mobility---and the fact that it is
      currently away from home---transparent to the correspondent nodes
      with which it communicates. 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 in this
      way. 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, Mobile IP will modify
      the packet to move the home address into a Home Address option
      and will set the IPv6 header's Source Address field to one of
      the mobile node's care-of addresses; these modifications to
      the packet are then reversed in the node receiving the packet,
      restoring the mobile node's home address to be the packet's
      Source Address before processing by higher protocol layers and
      applications.

   - 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 [[15], [16]]. 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
for the insertion of the Home Address option. 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., to 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].

10.2. 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 [13] 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 10.1):

  - 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 (SPD) to
     determine what processing is required for the packet [13].

   - 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 node inserts
     a Home Address 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 10.1. The Destination Options header in which the Home
     Address option is inserted MUST appear in the packet after the
     Routing Header, if present, and before the AH [11] (or ESP [12])
     header, so that the Home Address option is processed by the
     destination node (and, possibly, intermediate routing nodes)
     before the AH or ESP header is processed.

   - If a Binding Update is being included in the packet, it is
     also added to a Destination Options header in the packet. The
     Destination Options header in which the Binding Update option is
     inserted MUST appear after the AH or ESP header.

   - 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 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 5.4) contains the new care-of address.

     This allows, but does not require, the receiver of the packet
     containing the Binding Update 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 remain the same.

   In addition, when using any automated key management protocol [13]

(such as IKE [8]) to create any 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, 13], 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 10.1).

  - 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 [14] in the IKE
    exchange, giving the mobile node's home address as the initiator
    of the Security Association [22].

10.3. 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 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 be sent by the correspondent
    node using a 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 10.10), 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 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 10.9, subject to the
rate limiting defined in Section 10.12. The mobile node SHOULD
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 Routing
header), the mobile node SHOULD process the received packet in the
manner defined for the type of IPv6 Routing header used [6], which
will result in the 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.

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]. If this is done for upper-layer protocol response
packets sent by a mobile node while away from home, the mobile
node SHOULD NOT include its own care-of address, which appears in
the Routing header of the received packet, in the reversed route
for the response packet. If the received Routing header contained
no additional hops (other than the mobile node's home address and
care-of address), then any upper-layer protocol response packet
SHOULD NOT include a Routing header.

10.4. 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 [17].

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 [17].

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 SHOULD select 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 10.6. The mobile node registers
its primary care-of address with its home agent, as described in
Section 10.7.

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 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 [17], 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 link-level
addressed to it (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 (i.e., 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
new routers (and new on-link subnet prefixes) are present 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.

10.5. 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 10.10. On receipt of a valid Router
Advertisement, as defined in the processing algorithm specified for
Neighbor Discovery [17], 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,
    skip all of the following steps. Mobile IPv6 requires no special
    processing steps for this Router Advertisement.

  - 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 [17].

- 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 6.2). 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.

10.6. 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 10.18.

As described in Section 4, in order to form a new care-of address,
a mobile node MAY use either stateless [27] 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 [27] on that new address to confirm its
uniqueness. However, doing so represents a tradeoff 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 [17, 27];
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.

10.7. Sending Binding Updates to the Home Agent

After deciding to change its primary care-of address as described
in Sections 10.4 and 10.6, 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 option, 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 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 sub-option is included in the Binding Update option.

 - The Prefix Length field SHOULD be set to the length of the mobile
    node's subnet prefix in its home address, 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. Otherwise, this field MUST be set to zero.

 - 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 5.2, 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 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 10.11 for
information about retransmitting Binding Updates.

The Prefix Length field in the Binding Update allows the mobile node
to request its home agent to serve all home addresses for the mobile
node, as indicated by the interface identifier in the mobile node's
home address (the remaining low-order bits after the indicated subnet
prefix), together with each on-link subnet prefix on the home link.
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.

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 10.9.

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). These additional Binding
Updates MUST each be sent as a separate packet. Each care-of address
MUST be authenticated within the Binding Update as coming from the
home address being associated with the care-of address, as defined in
Section 4.4.

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 [17, 27]. 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 showing Status 138, Duplicate Address Detection
failed.

10.8. 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 10.7, 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 discovery 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 [10] for its home subnet
prefix. This packet MUST NOT contain a Home Address option and must
be sent using the mobile node's care-of address as the Source Address
in the packet's IP header (the packet is sent from the care-of
address, not using Mobile IP). As described in Section 9.8, 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.

[10.9](). Sending Binding Updates to Correspondent Nodes

A mobile node MAY send a Binding Update to any correspondent node at
any time to allow the correspondent node to cache the mobile node's
current care-of address (subject to the rate limiting defined in
[Section 10.12]). 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
Sub-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.

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 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.
A mobile node MAY set the care-of address differently for sending
Binding Updates to different correspondent nodes.

When sending any Binding Update, the mobile node MUST record in its
Binding Update List the following fields from the Binding Update:

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

 - The home address for which the Binding Update was sent (the value
    in the Home Address option in the packet carrying the Binding
    Update).

 - The initial lifetime of the binding, initialized from the

Lifetime field sent in the Binding Update.

- The remaining lifetime of the binding, also initialized from
  the Lifetime field sent in the Binding Update. This remaining
  lifetime value counts down and may also be reduced when the
  matching Binding Acknowledgement is received, based on the
  Lifetime value specified in that Binding Acknowledgement, as
  described in Section 10.13. When the remaining lifetime reaches
  zero, the Binding Update List entry MUST be deleted.

The mobile node MUST retain in its Binding Update List information
about all Binding Updates sent, for which the lifetime of the binding
has not yet expired. However, when sending a Binding Update, if an
entry already exists in the mobile node's Binding Update List for
an earlier Binding Update sent to that same destination node, the
existing Binding Update List entry is updated to reflect the new
Binding Update rather than creating a new Binding Update List entry.

When a mobile node sends a Binding Update to its home agent
to register a new primary care-of address (as described in
Section 10.7), the mobile node SHOULD also send a Binding Update
to each other node for which an entry exists in the mobile node's
Binding Update List, as detailed below. 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 send these Binding Updates
immediately after configuring a new care-of address. For example,
since the Binding Update is a destination option and can be included
in any packet sent by a mobile node, the mobile node MAY delay
sending a new Binding Update to any correspondent node for a
short period of time, in hopes that the needed Binding Update
can be included in some packet that the mobile node sends to that
correspondent node for some other reason (for example, as part of
some TCP connection in use). In this case, when sending a packet
to some correspondent node, the mobile node SHOULD check in its
Binding Update List to determine if a new Binding Update to this
correspondent node is needed, and SHOULD include the new Binding
Update in this packet as necessary.

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
return a Binding Update to the sender giving its current care-of
address (subject to the rate limiting defined in Section 10.12).
In particular, the mobile node SHOULD return a Binding Update 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 10.10).

   - 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 Binding Update should be sent
   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.

   A mobile node MAY choose to keep its location private from certain
   correspondent nodes, and thus need not 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 5.1. No other IPv6 nodes are authorized to send Binding
   Updates on behalf of a mobile node.

10.10. Establishing 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.

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

  - The Home Address field in the Home Address 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
    sub-option in the Binding Update option, 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 6.2) 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 4.6). Alternatively,
the mobile node MAY use dynamic home agent address discovery
(Section 10.8) 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 5.1), the
Binding Update packet to this home agent MUST meet the authentication
requirements for Binding Updates, defined in Section 4.4.

10.11. Retransmitting Binding Updates

When the mobile node sends a Binding Update, 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 10.7.

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.

10.12. Rate Limiting for Sending Binding Updates

A mobile node MUST NOT send Binding Updates about the same binding to
any individual node more often than once per MAX_UPDATE_RATE seconds.
After sending MAX_FAST_UPDATES consecutive Binding Updates to a
particular node with the same care-of address, the mobile node SHOULD
reduce its rate of sending Binding Updates to that node, to the rate
of SLOW_UPDATE_RATE per second. The mobile node MAY continue to send
Binding Updates 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.

10.13. 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 Section 4.4.

  - The Option Length field in the Binding Acknowledgement option is
    greater than or equal to the length specified in Section 5.2.

   - 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, although the remainder of the packet (i.e., other
options, extension headers, or payload) SHOULD be processed normally
according to any procedure defined for that part of the packet.

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 10.12.

[10.14](#). Receiving Binding Requests

   When a mobile node receives a packet containing a Binding Request,
   it SHOULD return to the sender a packet containing a Binding Update.
   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), except that this lifetime
   MUST NOT exceed the remaining lifetime for the mobile node's primary
   care-of address registration at its home agent. 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 keep its current
   binding private from the sender of the Binding 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 Request for which the Binding Update is being returned
   contains a Unique Identifer Sub-Option, the Binding Update MUST also
   include a Unique Identifier Sub-Option. The unique identifier in the
   Sub-Option Data field of the Unique Identifier Sub-Option MUST be
   copied from the unique identifier carried in the Binding Request.

[10.15](#). Receiving ICMP Error Messages

   The Option Type value for a Binding Update option specifies that
   any node receiving this option that does not recognize the Option
   Type SHOULD return an ICMP Parameter Problem, Code 2, message to
   the sender of the packet containing the Binding Update option. If
   a node 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.

   Likewise, although ALL IPv6 nodes (whether host or router, whether
   mobile or stationary) MUST implement the ability to correctly process
   received packets containing a Home Address option, all Option Type
   values in IPv6 include a specification of the behavior that a node
   receiving a packet containing this option performs if it does not
   implement receipt of that type of option. For the Home Address
   option, the Option Type value specifies that any node receiving
   this option that does not recognize the Option Type SHOULD return
   an ICMP Parameter Problem, Code 2, message to the sender of the
   packet containing the Home Address option. If a mobile node receives
   such an ICMP error message from some node indicating that it does

not recognize the mobile node's Home Address option, the mobile
node SHOULD log the error and then discard the ICMP message; this
error message indicates that the node to which the original packet

   was addressed (the node returning the ICMP error message) does not
   correctly implement this required part of the IPv6 protocol.

10.16. 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 9.6.

   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 11).

   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 [17], except that the initial retransmission
   interval is specified to be INITIAL_SOLICIT_TIMER (see section 11).

10.17. Receiving Mobile Prefix Advertisements

   Section 9.6 describes the operation of a home agent to support boot
   time configuration and renumbering a mobile node's home subnet while
   the mobile node is away from home. The home agent sends Mobile
   Prefix 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 [13, 11, 12] to guard
  against malicious prefix advertisements. 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 [17]. 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 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 [27] 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.

10.18. Using Multiple Care-of Addresses

As described in Section 10.6, 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 10.4. 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 10.7.

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.

10.19. Routing Multicast Packets

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

In order to receive packets sent to some multicast group, a mobile
node must join that multicast group. One method by which a mobile
node MAY join the group is via a (local) multicast router on the
foreign link being visited. The mobile node SHOULD use one of its
care-of addresses that shares a subnet prefix with the multicast
router, as the source IPv6 address of its multicast group membership
control messages. The mobile node MUST insert a Home Address
destination option in such outgoing multicast packets, so that any
multicast applications that depend on the address of the sending node
will correctly use the mobile node's home address for that value.

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.

10.20. Returning Home

A mobile node detects that it has returned to its home link through
the movement detection algorithm in use (Section 10.4), 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 [17] (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 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 [17], 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 multicasts on the local link (such as Ethernet) are 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 [17].

11. Protocol Constants

    INITIAL_BINDACK_TIMEOUT   1 second

    INITIAL_SOLICIT_TIMER 2 seconds

    MAX_BINDACK_TIMEOUT   256 seconds

    PREFIX_ADV_TIMEOUT 5 seconds

    PREFIX_ADV_RETRIES 3 retransmissions

    MAX_UPDATE_RATE   once per second

    SLOW_UPDATE_RATE   once per 10 second interval

MAX_FAST_UPDATES   5 transmissions

        MAX_ADVERT_REXMIT   3 transmissions

        MAX_PFX_ADV_DELAY   1,000 seconds

        HomeRtrAdvInterval   3,600 seconds

12. **IANA Considerations**

   This document defines four new types of IPv6 destination options,
   each of which must be assigned an Option Type value:

   - The Binding Update option, described in Section 5.1;

   - The Binding Acknowledgement option, described in Section 5.2;

   - The Binding Request option, described in Section 5.3; and

   - The Home Address option, described in Section 5.4.

   These destination options can sometimes take sub-options. The
   current sub-options are specified in section 5.5, "Mobile IPv6
   Destination Option Sub-Options", and include the following:

      0   Pad1 sub-option

      1   PadN sub-option

      2   Unique Identifier sub-option

      3   Mobile Router Prefix Length sub-option

      4   Alternate Care-of Address sub-option

   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 5.6;

   - The Home Agent Address Discovery Reply message, described in
      Section 5.7;

   - The Mobile Prefix Solicitation message, described in Section 5.8;
      and

   - The Mobile Prefix Advertisement message, described in
      Section 5.9.

   This document also defines two new Neighbor Discovery [17] options,
   which must be assigned Option Type values within the option numbering
   space for Neighbor Discovery messages:

   - The Advertisement Interval option, described in Section 6.3; and

- The Home Agent Information option, described in Section 6.4.

A new space of predefined SPIs for Binding Security Associations must
be created for use with Binding Updates and Binding Acknowledgements.
This space is to be managed in a way identical to that specified
for IPsec [13]. Assignment of new SPIs in the reserved range 1-255
requires working group approval.

Finally, this document defines a new type of anycast address, which
must be assigned a reserved value for use with any subnet prefix to
define this anycast address on each subnet:

 - The "Mobile IPv6 Home-Agents" anycast address [10], used in the
    dynamic home agent address discovery mechanism described in
    Sections 9.8 and 10.8.

13. Security Considerations

13.1. Binding Updates, Acknowledgements, and Requests

   The Binding Update option described in this document will result in
   packets addressed to a mobile node being delivered instead to its
   care-of address. This ability to change the routing of these packets
   could be a significant vulnerability if any packet containing a
   Binding Update option were not authenticated. Such use of "remote
   redirection", for instance as performed by the Binding Update option,
   is widely understood to be a security problem in the current Internet
   if not authenticated [1].

   The Binding Acknowledgement option also requires authentication,
   since, for example, an attacker could otherwise trick a mobile node
   into believing a different outcome from a registration attempt with
   its home agent.

   No authentication is required for the Binding Request option, since
   the use of this option does not modify or create any state in either
   the sender or the receiver. Issues with binding privacy stemming
   from use of the Binding Request option can be dealt with either
   through existing IPsec encryption mechanisms or through use of
   firewalls.

   After the Sequence Number space of the Binding Update and Binding
   Acknowledgement options has been exhausted, the mobile node and the
   home agent SHOULD renegotiate their security association in order to
   prevent any possibility of replay attacks.

13.2. Security for the Home Address Option

   No special 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
   (Section 5.4), 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.

   The use of the Home Address 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. A node receiving a packet
that includes a Home Address option MAY implement the processing of
this option by physically exchanging the Home Address option field
with the source IPv6 address in the IPv6 header.

13.3. General Mobile Computing Issues

The mobile computing environment is potentially very different from
the ordinary computing environment. In many cases, mobile computers
will be connected to the network via wireless links. Such links
are particularly vulnerable to passive eavesdropping, active replay
attacks, and other active attacks. Furthermore, mobile computers
are more susceptible to loss or theft than stationary computers.
Any secrets such as authentication or encryption keys stored on the
mobile computer are thus subject to compromise in ways generally not
common in the non-mobile environment.

Users who have sensitive data that they wish to keep private
SHOULD protect the data using additional mechanisms (such as
encryption [12]); such mechanisms are beyond the scope of this
document. Users concerned about traffic analysis SHOULD consider
appropriate use of link encryption. If stronger location privacy
is desired, the mobile node MAY create a tunnel to its home agent.
Then, packets destined for correspondent nodes will appear to emanate
from the home subnet, making it more difficult to pinpoint the
location of the mobile node. Such mechanisms are all beyond the
scope of this document.

Whether or not the mobile node is away from home is likely to
influence the choice of security policy from the SPD. For instance,
if a mobile node is connected to its home network and it communicates
with a correspondent node on its home network, no security may be
needed. If, on the other hand, the mobile node is attached to
foreign network and has sent a Binding Update to its home agent, then
the mobile node may need to make use of security features in order to
communicate with that same correspondent node.

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 at Santa Barbara), Vijay Devarapalli

(Nokia Research Center), Rich Draves (Microsoft Research), Francis
Dupont (ENST Bretagne), Thomas Eklund (Xelerated), Jun-Ichiro Itojun

References

   [1] S. M. Bellovin. Security Problems in the TCP/IP Protocol Suite.
       ACM Computer Communications Review, 19(2), March 1989.

   [2] Jim Bound and Charles Perkins. Dynamic Host Configuration
       Protocol for IPv6 (DHCPv6), February 1999. Work in progress.

   [3] Scott Bradner. Key words for use in RFCs to Indicate
       Requirement Levels. RFC 2119, March 1997.

   [4] Alex Conta and Stephen Deering. Generic Packet Tunneling in
       IPv6 Specification. RFC 2473, December 1998.

   [5] Alex Conta and Stephen Deering. Internet Control Message
       Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)
       Specification. RFC 2463, December 1998.

   [6] Stephen E. Deering and Robert M. Hinden. Internet Protocol
       Version 6 (IPv6) Specification. RFC 2460, December 1998.

   [7] Paul Ferguson and Daniel Senie. Network Ingress Filtering:
       Defeating Denial of Service Attacks which employ IP Source
       Address Spoofing. RFC 2267, January 1998.

   [8] Dan Harkins and Dave Carrel. The Internet Key Exchange (IKE).
       RFC 2409, November 1998.

   [9] Robert M. Hinden and Stephen E. Deering. IP Version 6
       Addressing Architecture. RFC 2373, July 1998.

  [10] David B. Johnson and Stephen E. Deering. Reserved IPv6 Subnet
       Anycast Addresses. RFC 2526, March 1999.

  [11] Stephen Kent and Randall Atkinson. IP Authentication Header.
       RFC 2402, November 1998.

  [12] Stephen Kent and Randall Atkinson. IP Encapsulating Security
       Payload (ESP). RFC 2406, November 1998.

  [13] Stephen Kent and Randall Atkinson. Security Architecture for
       the Internet Protocol. RFC 2401, November 1998.

  [14] Douglas Maughan, Mark Schneider, Mark Schertler, and Jeff
       Turner. Internet Security Association and Key Management
       Protocol (ISAKMP). RFC 2408, November 1998.

  [15] P. Mockapetris. Domain Names -- Concepts and Facilities.
       RFC 1034, November 1987.

[16] P. Mockapetris. Domain Names -- Implementation and
     Specification. RFC 1035, November 1987.

[17] Thomas Narten, Erik Nordmark, and William Allen Simpson.
     Neighbor Discovery for IP Version 6 (IPv6). RFC 2461, December
     1998.

[18] Charles Perkins. IP Encapsulation within IP. RFC 2003, October
     1996.

[19] Charles Perkins, editor. IP Mobility Support. RFC 2002,
     October 1996.

[20] Charles Perkins. Minimal Encapsulation within IP. RFC 2004,
     October 1996.

[21] Charles Perkins and David B. Johnson. Route Optimization in
     Mobile IP, February 1999. Work in progress.

[22] Derrell Piper. The Internet IP Security Domain of
     Interpretation for ISAKMP. RFC 2407, November 1998.

[23] David C. Plummer. An Ethernet Address Resolution Protocol:
     Or Converting Network Protocol Addresses to 48.bit Ethernet
     Addresses for Transmission on Ethernet Hardware. RFC 826,
     November 1982.

[24] J. B. Postel. User Datagram Protocol. RFC 768, August 1980.

[25] J. B. Postel, editor. Transmission Control Protocol. RFC 793,
     September 1981.

[26] Joyce K. Reynolds and Jon Postel. Assigned Numbers. RFC 1700,
     October 1994. See also http://www.iana.org/numbers.html.

[27] Susan Thomson and Thomas Narten. IPv6 Stateless Address
     Autoconfiguration. RFC 2462, December 1998.

A. Changes from Previous Version of the Draft

This appendix briefly lists some of the major changes in this
draft relative to the previous version of this same draft,
draft-ietf-mobileip-ipv6-13.txt:

 - 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 (BSA) 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.

   - Added the following protocol constants:

         INITIAL_SOLICIT_TIMER:

   - Created new ICMP messages for Mobile Prefix Solicitations and
      Advertisements (see sections 5.8 and 5.9).

   - Changed Network Renumbering (Section 9.6) 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 10.20) to describe
      how the Home Agent discovers the mobile node's link-layer address

   - Reworded parts of appendix B as needed.

   - Added the Mobile Router Prefix Length Sub-Option (section 5.5),
      along with text in Section 4.8 describing what a Mobile Router
      should do with it.

B. 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.

Chairs' Addresses

   The Working Group can be contacted via its current chairs:

        Phil Roberts
        Motorola
        1501 West Shure Drive
        Arlington Heights, IL 60004

        Phone: +1 847 632-3148
        E-mail: qa3445@email.mot.com

        Basavaraj Patil
        Nokia
        6000 Connection Drive
        M/S M8-540
        Irving, TX 75039
        USA

        Phone: +1 972 894-6709
        Fax: +1 972 894-5349
        E-mail: raj.patil@nokia.com

Authors' Addresses

    Questions about this document can also be directed to the authors:

        David B. Johnson
        Rice University
        Department 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
        313 Fairchild Drive
        Mountain View, CA 94043
        USA

        Phone: +1 650 625-2986
        Fax: +1 650 625-2502
        E-mail: charliep@iprg.nokia.com