IETF Mobile IP Working Group   David B. Johnson
INTERNET-DRAFT   Carnegie Mellon University
                                                 Charles Perkins
                                                 Sun Microsystems
                                                   4 August 1998

Mobility Support in IPv6

<draft-ietf-mobileip-ipv6-06.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.

Contents

[1](#). Introduction

   This document specifies the operation of mobile computers using
   Internet Protocol Version 6 (IPv6) [[5](#)]. 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 "macro"
   mobility management problem. More "micro" mobility management
   applications -- for example, handoff among wireless transceivers,
   each of which covers only a very small geographic area -- are
   possibly more suited to other solutions. For example, in many
   current wireless LAN products, link-layer mobility mechanisms allow a
   "handoff" of a mobile node from one cell to another, reestablishing
   link-layer connectivity to the node in each new location. As long
   as such handoff occurs only within cells of the mobile node's home
   link, such link-layer mobility mechanisms are likely to offer faster
   convergence and lower overhead than Mobile IPv6. Extensions to the
   Mobile IPv6 protocol are also possible 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, such as typical
    wireless networks. Some aspects of this problem are addressed
    by the movement detection procedure described in Section 10.3,
    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 untrusted node is allowed
    to connect to any link layer. It is independent 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) [15, 14, 16], 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" [17] is now built in as a fundamental part
      of the protocol, rather than being added on as a 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 [15]. This integration also allows the
      Mobile IPv4 "registration" functionality and the Mobile IPv4
      Route Optimization functionality to be 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" [6]. 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 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 the enhanced features of IPv6, such
   as Neighbor Discovery [13] and Address Autoconfiguration [22],
   to operate in any location away from home without any special
   support required from its local router.

- Unlike Mobile IPv4, Mobile IPv6 utilizes IPsec [8, 9, 10] for
   all security requirements (sender authentication, data integrity
   protection, and replay protection) for Binding Updates (which
   serve the role of both registration and Route Optimization in
   Mobile IPv4). Mobile IPv4 relies on its own security mechanisms
   for these functions, based on statically configured "mobility
   security associations".

- 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 tunneled 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 tunneling.

- 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 [13] rather than ARP [18] 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 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 and since 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.

- 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.

[3](). Terminology

[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.

[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.

3.3. Specification Language

   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].

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 [22] or
   stateful (e.g., DHCPv6 [2]) address autoconfiguration, according
   to the methods of IPv6 Neighbor Discovery [13]. 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.

Section 10.15 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 which of possibly many care-of
addresses to which to tunnel each intercepted packet, leaving the
mobile node entirely in control of this policy by which of its
care-of addresses it registers 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 care-of address
while away from home. The mobile node sends a Binding Update to the
"Home-Agents anycast address" for its own home subnet prefix and thus
reaches one of the (possibly many) routers on its home link currently
operating as a home agent. This home agent rejects the mobile
node's Binding Update, but returns in the Binding Acknowledgement
in response a list of all 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 [5] (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 [5],
they may be included in any IPv6 packet. Any of these options can be
sent in either of two ways:

 - A Binding Update, Binding Acknowledgement, or Binding Request can
   be included within any IPv6 packet carrying any payload such as
   TCP [20] or UDP [19].

 - A Binding Update, Binding Acknowledgement, or Binding Request 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" [5].

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" [6] that do not allow forwarding of packets that
appear to have a Source Address that is not topologically correct.
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 discussed in general 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 also include either an AH [8] or

ESP [9] header providing sender authentication, data integrity
protection, and replay protection. The Binding Update option
is 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 also include either an AH [8] or
ESP [9] header providing sender authentication, data integrity
protection, and replay protection. The Binding Acknowledgement
option is 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. The Home Address option
is described in detail in Section 5.4.

Extensions to the format of these options MAY be included after the
fixed portion of the option data specified in this document. The
presence of such extensions 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 extensions. Currently, no extensions have been
defined.

4.3. **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. 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 [13].
      When sending a packet, the Binding Cache is searched before the
      Neighbor Discovery conceptual Destination Cache [13] (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 9.6, 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.

      - 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 16 bits long, and
  all comparisons between Sequence Number values MUST be
  performed modulo 2**16.

- 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 time at which a Binding Request was last sent for this
  entry, as needed to implement the rate limiting restriction
  for sending Binding Requests.

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. Any node's Binding Cache 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.

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, to the mobile
node's home agent, and to a previous default router of the
mobile node. 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. This 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 mobile node's home addresses for

most Binding Updates (Sections 10.5 and 10.7), but will
be the mobile node's previous care-of address for Binding
Updates sent to the mobile node's previous default router
(Section 10.8).

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

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

- 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 10.13.

Home Agents List

A list, maintained by each home agent, recording information
about each other home agent on a link on which this node
is serving as a home agent; each home agent maintains a
separate Home Agents List for each such link on which it is
serving. This list is used in the dynamic home agent address
discovery mechanism. 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 [13]. The Home Agents List
MAY be implemented in any manner consistent with the external
behavior described in this document. Each Home Agents List
entry conceptually contains the following fields:

- The IP address of another router on the home link that this
  node currently believes is operating as a home agent for
  this 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 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 this 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, for use in ordering the
  Home Agents List returned in a Binding Acknowledgement;
  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.

4.4. 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 assumes that the original sending
correspondent node has no Binding Cache entry for the mobile node,

since the correspondent node would otherwise have sent the packet
directly to the mobile node using a Routing header. The mobile node

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.

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 handoff 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.

5. New IPv6 Destination Options

5.1. Binding Update Option Format

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|C| Reserved| Prefix Length |       Sequence Number         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Lifetime                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Care-of Address                          +
|                  (only present if C bit set)                  |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   Option Type

      195 ???

   Option Length

      8-bit unsigned integer. Length of the option, in octets,
      excluding the Option Type and Option Length fields. For the
      current definition of the Binding Update option, the minimum
      value for this field is 8; the length is 24 if the Care-of
      Address Present (C) bit is set.

   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).

Care-of Address Present (C)

   The Care-of Address Present (C) bit indicates the presence of
   the Care-of Address field in the Binding Update. The care-of
   address for this binding is either the address in the Care-of
   Address field in the Binding Update, if this bit is set, or the
   Source Address in the packet's IPv6 header, if this bit is not
   set.

Reserved

   Sent as 0; ignored on reception.

Prefix Length

   The 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. Details of this operation are
   described in Section 9.3.

Sequence Number

   Used by the receiving node to sequence Binding Updates and by

the sending node to match a returned Binding Acknowledgement

with this Binding Update. Each Binding Update sent by a mobile
node MUST use a Sequence Number greater than the Sequence
Number value sent in the previous Binding Update (if any) to
the same destination address (modulo 2**16).

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
should be deleted.

Care-of Address

This field in the Binding Update is optional and is only
present when the Care-of Address Present (C) bit is set. If
present, it gives the care-of address of the mobile node for
this binding. For most Binding Updates sent, it is expected
that this field will not be present, and instead that the
care-of address for the binding will be given by the Source
Address field in the packet's IPv6 header.

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 indicated by the Home
Address field in the Home Address option in the packet.

Any packet that includes a Binding Update option MUST also include
either an AH [8] or ESP [9] header providing sender authentication,
data integrity protection, and replay protection.

If the care-of address in the binding (either the Care-of Address
field in the Binding Update option or 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.

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 [5]. 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.

Extensions to the Binding Update option format may be included after
the fixed portion of the Binding Update option specified above.
The presence of such extensions will be indicated by the Option
Length field. When the Option Length is greater than the length
defined above, the remaining octets are interpreted as extensions.
Currently, no extensions have been defined.

5.2. Binding Acknowledgement Option Format

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 included it 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 (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    |         Sequence Number       |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                            Lifetime                           |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                            Refresh                            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                              |
 +                                                              +
 .                                                              .
 .                       Home Agents List                       .
 .                                                              .
 +                                                              +
 |                                                              |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   Option Type

      2 ???

   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, except when the Status field is equal to 135
      (dynamic home agent address discovery response), in which case
      this field MUST be set to 11 + 16 * N, where N is the number of

IP addresses included in the Home Agents List field; the Home

Agents List field MUST NOT be included in the option if the
Status field is not set to 135.

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
   129   Poorly formed Binding Update
   130   Administratively prohibited
   131   Insufficient resources
   132   Home registration not supported
   133   Not home subnet
   134   Sequence Number field value too small
   135   Dynamic home agent address discovery response
   136   Incorrect interface identifier length
   137   Not home agent for this mobile node

Up-to-date values of the Status field are to be specified in
the most recent "Assigned Numbers" [21].

Sequence Number

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 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.

     Refresh

          The recommended interval 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.

     Home Agents List

          A list of home agents on the home link for the mobile node to
          which this Binding Acknowledgement is sent. This field MUST
          NOT be present (zero addresses listed) unless the Binding
          Acknowledgement is sent in response to an anycast Binding
          Update sent by this mobile node attempting dynamic home agent
          address discovery. In this case, the Status field MUST be
          set to 135 (dynamic home agent address discovery response).
          The construction of the Home Agents List field in a Binding
          Acknowledgement is defined in Section 9.2.

   Any packet that includes a Binding Acknowledgement option MUST
   also include either an AH [8] or ESP [9] header providing sender
   authentication, data integrity protection, and replay protection.

   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 to the mobile node are the same as for sending any packet to a
mobile node using a binding, and are described in Section 8.9. The

packet is sent using a Routing header, routing the packet to the
mobile node by way of its care-of address recorded in the Binding
Cache entry.

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" [5]).

The three highest-order bits of the Option Type are encoded to
indicate specific processing of the option [5]. 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.

[5.3](#). **Binding Request Option Format**

   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 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

      Option Type

         3 ???

      Option Length

         8-bit unsigned integer. Length of the option, in octets,
         excluding the Option Type and Option Length fields. For the
         current definition of the Binding Request option, this field
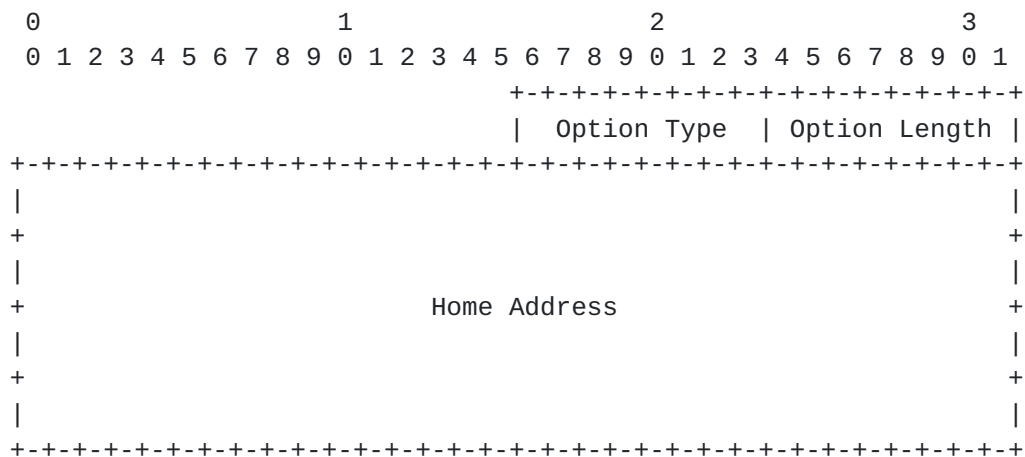   MUST be set to 0.

   The three highest-order bits of the Option Type are encoded to
   indicate specific processing of the option [[5](#)]. 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.

   Extensions to the Binding Request option format may be included after
   the fixed portion of the Binding Request option specified above.
   The presence of such extensions will be indicated by the Option
   Length field. When the Option Length is greater than 0 octets,
   the remaining octets are interpreted as extensions. Currently, no
   extensions have been defined.

[5.4](#). Home Address Option Format

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                          +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

     Option Type

        196 ???

     Option Length

        8-bit unsigned integer. Length of the option, in octets,
        excluding the Option Type and Option Length fields. For the
        current definition of the Home Address option, this field MUST
        be set to 16.

     Home Address

        The home address of the mobile node sending the packet.

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.

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. If the packet carries no IP authentication, then the
contents of the Home Address option, as well as the Source Address
field or any other field in the IPv6 header, may have been forged or
altered during transit.

Upon receipt of a packet containing a Home Address option, the
receiving node replaces the Source Address in the IPv6 header with
the Home Address in the Home Address option. 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
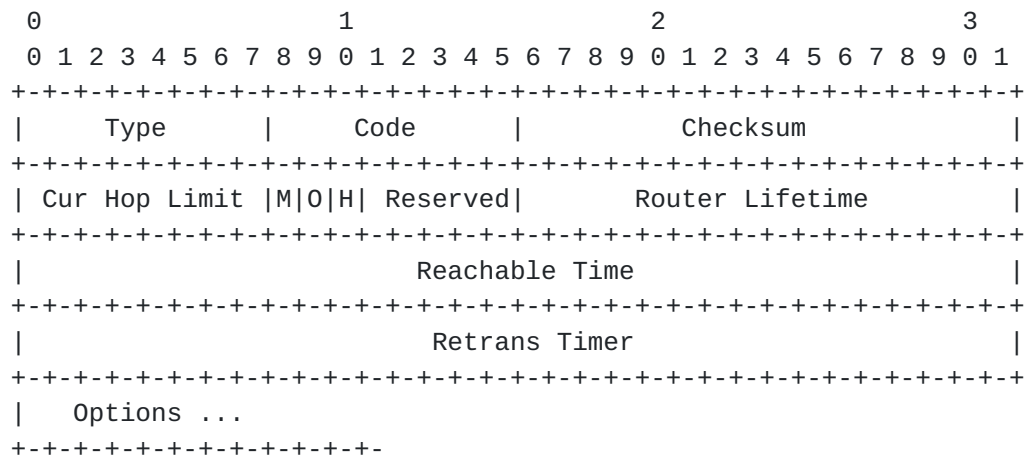issues related to the Home Address option are discussed further in
Section 13.

The three highest-order bits of the Option Type are encoded to
indicate specific processing of the option [5]. 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.

Extensions to the Home Address option format may be included after
the fixed portion of the Home Address option specified above.
The presence of such extensions will be indicated by the Option
Length field. When the Option Length is greater than 8 octets,
the remaining octets are interpreted as extensions. Currently, no
extensions have been defined.

6. **Modifications to IPv6 Neighbor Discovery**

6.1. **Modified Router Advertisement Message Format**

   Mobile IPv6 modifies the format of the Router Advertisement
   message [13] by the addition of a single flag bit for use in the
   dynamic home agent address discovery mechanism (Sections 9.2
   and 10.6). 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 [13]:

      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.

      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 proving home agent
    service, for use in building its Home Agents List as part of the
    dynamic home agent address discovery mechanism (Sections [9.2](#)
    and 10.6).

-   To allow a mobile node to send a Binding Update to its previous
    default router, after moving to a new subnet and acquiring a new
    care-of address ([Section 10.8](#)).

However, Neighbor Discovery [13] 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 [13]:

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 router MUST 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 [13]. In this case, at least one of these
multiple Advertisements begin 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

         6 ???

      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 [13], 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 10.3.

   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     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
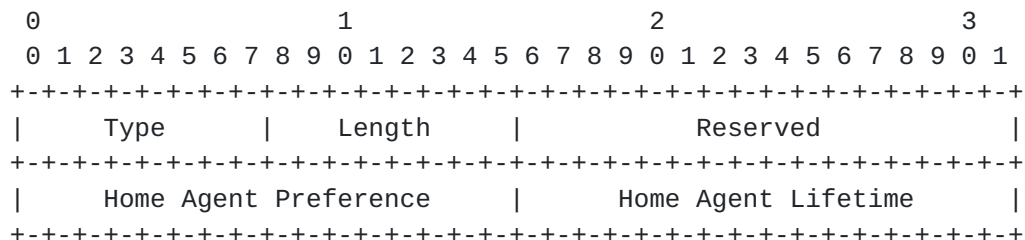
      Type

         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.

      Home Agent Preference

         16-bit signed, twos-complement integer. The preference
         for the home agent sending this Router Advertisement, for
         use in ordering the Home Agents List returned in a Binding
         Acknowledgement; 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.

      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 SHOULD 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 ([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 [13] 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 home agent 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   0.5 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, until its movement
      detection algorithm (Section 10.3) determines that it has moved
      and that its current care-of address might no longer be valid.

[7](). Requirements for 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.

[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 be able to accept packets addressed to the
  Home-Agents anycast address for the subnet on which it is serving
  as a home agent, and MUST be able to participate in dynamic home
  agent address discovery (Section 9.2).

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 10.5, 10.7, and 10.8; and MUST
    be able to receive and process Binding Acknowledgement options,
    as specified in Section 10.11.

  - Every IPv6 mobile node MUST support use of the dynamic home agent
    address discovery mechanism, as described in Section 10.6.

  - 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.

[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 copying the Home Address field from the Home Address
   option into the IPv6 header, replacing the original value of the
   Source Address field there.

   Further processing of such a packet (e.g., at the transport layer)
   thus need not 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 contains a valid AH [[8]()] or ESP [[9]()] header that
      provides sender authentication, integrity protection, and replay
      protection.

   - The packet MUST contain a valid Home Address option. The home
      address for the binding is specified by the Home Address field of
      the 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. The Sequence Number comparison is
      performed modulo 2^{16}.

Any Binding Update not satisfying all of these tests MUST be
silently ignored, and the packet carrying the Binding Update MUST be
discarded.

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

- If the Destination Address in the packet's IPv6 header is the
  Home-Agents anycast address for a local prefix and this address
  is assigned to one of this node's network interfaces, then the
  mobile node sending this Binding Update is attempting dynamic
  home agent address discovery. Processing for this type of
  received Binding Update is described in Section 9.2. (If the
  Destination Address is not assigned to one of this node's network
  interfaces, then the packet would have been forwarded as a normal
  packet and the Binding Update, as a destination option, would not
  be processed in any way by this node.)

- 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 (as given in the Home Address option in the
  packet), 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 9.3; 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 9.4; 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 home address of the mobile node is taken from the Home Address

field in the packet's Home Address option. The new Binding Cache

entry records the association between this home address and the
care-of address for the binding, as specified in either the Care-of
Address field of the Binding Update or in the Source Address field
in the packet's IPv6 header. Any Binding Cache entry created or
updated in response to processing this Binding Update MUST be deleted
after the expiration of the Lifetime period specified in the Binding
Update.

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. The home address of the
mobile node is taken from the Home Address field in the packet's Home
Address option.

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 SHOULD 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, the Status field in
the Binding Acknowledgement MUST be set to a value less than 128;
if the node rejects the Binding Update and does not create or
update an entry for this binding, 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" [21].

As described in Section 5.2, the packet in which the Binding
Acknowledgement is returned MUST include either an AH [8] or ESP [9]
header providing sender authentication, data integrity protection,
and replay protection; 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. The packet is routed first to the care-of
address contained in the Binding Update being acknowledged, and
then to the mobile node's home address. This use of the Routing
header ensures that the Binding Acknowledgement will be routed to the
current location of the node sending the Binding Update, whether the

Binding Update was accepted or rejected.

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.

   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 9.3) 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 (or
   can 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.

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 returned to
the mobile node's home agent (the source of the tunnel). By the
definition of IPv6 encapsulation [4], this 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 default router (e.g., the mobile node moved after the packet
was sent), the router will encapsulate and tunnel the packet to the
mobile node's new care-of address (if it has a Binding Cache entry
for the mobile node). As above, any ICMP error message caused by the
packet while in this tunnel will be returned to the previous default
router (the source of the tunnel), which MUST relay certain ICMP

error messages back to the correspondent node [4].

   Thus, in all cases, any meaningful ICMP error messages caused
   by packets from a correspondent node to a mobile node will be
   returned to the correspondent node. If the correspondent node
   receives persistent ICMP Destination Unreachable messages after
   sending packets to a mobile node based on an entry in its Binding
   Cache, the correspondent node SHOULD delete this Binding Cache
   entry. If the correspondent node subsequently transmits another
   packet to the mobile node, the packet will be routed to the mobile
   node's home link, intercepted by the mobile node's home agent, and
   tunneled to the mobile node's primary care-of address using IPv6
   encapsulation. The mobile node will then return a Binding Update to
   the correspondent node, allowing it to recreate a (correct) Binding
   Cache entry for the mobile node.

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 [5], 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 [5], 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 9.6. The mobile node will then send
a Binding Update to the sending node, as described in Section 10.7,
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. 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 9.2. 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 [13].

On receipt of a valid Router Advertisement, as defined in the processing algorithm specified for Neighbor Discovery [13], 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 [13]. Determine the global address of the router based on the Prefix Information option received from it in which the Router Address (R) bit is set (Section 6.2).

- 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 SHOULD 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 global 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, also 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 global 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 address 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.

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.

9.2. Dynamic Home Agent Address Discovery

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 indicates that the mobile node sending it is
attempting dynamic home agent address discovery.

As described in Section 10.6, a mobile node attempts dynamic home
agent address discovery by sending its "home registration" Binding
Update to the Home-Agents anycast address for its home IP subnet
prefix (the packet MUST also include a Home Address option). A home
agent receiving such a Binding Update that is serving this subnet
(the home agent is configured with this anycast address on one of its
network interfaces) MUST reject the Binding Update and SHOULD return
a Binding Acknowledgement indicating this rejection, with the Source
Address of the packet carrying the Binding Acknowledgement set to one
of the global unicast addresses of the home agent. The Status field
in the Binding Acknowledgement MUST be set to 135 (dynamic home agent
address discovery response).

In this Binding Acknowledgement rejecting the dynamic home agent
address discovery Binding Update, this home agent SHOULD set the Home
Agents List as follows:

- The Home Agents List in this Binding Acknowledgement SHOULD
  contain the IP address of all home agents currently listed in
  this home agent's own Home Agents List (Section 4.3). However,
  if this home agent's own 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 list in
  the Binding Acknowledgement. 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 Agents List should be placed in
     the Home Agents List in the Binding Acknowledgement 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, and the home agent with the lowest preference SHOULD be
     listed last.

   - Among home agents with equal preference, their IP addresses in
     the Home Agents List SHOULD be listed in an order randomized with
     respect to other home agents with equal preference, each time
     a Binding Acknowledgement with a non-empty Home Agents List is
     returned by this home agent.

   - The Option Length field in this Binding Acknowledgement
     MUST be set to 11 + 16 * N, where N is the number of IP
     addresses included in the Home Agents List field in the Binding
     Acknowledgement.

   The mobile node, upon receiving this Binding Acknowledgement, MAY
   then resend its Binding Update to the home agent address given as the
   IP Source Address of the packet carrying the Binding Acknowledgement
   or to any of the unicast IP addresses listed in the Home Agents List
   field in the Acknowledgement. For example, the mobile node may
   re-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 Agents List in the Binding Acknowledgement. If the home agent
   identified by the Source Address field in the IP header of the packet
   carrying the Binding Acknowledgement is not listed in the Home Agents
   List, it SHOULD be tried before the first address given in the list;
   otherwise, it SHOULD be tried in the in its listed order.

9.3. 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.

If the home agent does not reject the Binding Update as described
above, then it becomes the home agent for the mobile node. The new
home agent (the receiving node) 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 from the Home Address
field in the packet's Home Address option. The care-of address for
this Binding Cache entry is taken from the Care-of Address field of
the Binding Update (if the Care-of Address Present (C) bit is set in
the Binding Update) 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.

The lifetime for the Binding Cache entry MUST NOT be greater than the

remaining valid lifetime for the subnet prefix in the mobile node's
home address specified with the Binding Update. The remaining valid

lifetime for this prefix is determined by the home agent based on
its own Prefix List entry for this prefix [13]. 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 implemented by the home
agent. 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.

If the Acknowledge (A) bit is set in the Binding Update (it SHOULD
be), then the home agent MUST return a Binding Acknowledgement to the
mobile node, constructed as follows:

 - The Status field MUST be set to a value 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 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,
    this lifetime MUST NOT be greater than the remaining valid
    lifetime for the subnet prefix in the mobile node's home address.

 - 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 9.5 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.

9.4. 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.

If the Acknowledge (A) bit is set in the Binding Update (it SHOULD
be), then the home agent MUST return a Binding Acknowledgement to the
mobile node, constructed as follows:

 - The Status field MUST be set to a value 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 9.5).

9.5. 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
becomes 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 [13] 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 [13] on behalf of the mobile node, to
    advertise the home agent's own link-layer address for this IP
    address. The Target Address in the Neighbor Advertisement
    message MUST be set to this IP address for the mobile node, and
    the Advertisement MUST include a Target Link-layer Address option
    specifying the home agent's link-layer address. 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 [13].

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 [13]
to intercept unicast packets on the home link addressed 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 to 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. 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 to defend these addresses on the home link for
Duplicate Address Detection [13].

9.6. 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 9.5. 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 [8] or ESP [9] header present in the packet.

For forwarding 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 (which is an address of the mobile
node itself). 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 undefined 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 [7],
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) [7], 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 better defined in IPv6.

9.7. **Renumbering the Home Subnet**

IPv6 provides mechanisms through Neighbor Discovery [13] and Address
Autoconfiguration [22] to aid 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 while the renumbering takes place.

The IPv6 renumbering mechanisms are based on nodes on the link
receiving Prefix Information options in Router Advertisement messages
giving the valid lifetime and preferred lifetime for different
prefixes on the link [13]. Mobile IPv6 arranges to tunnel certain
Router Advertisements giving "important" Prefix Information options
to mobile nodes while away from home. To avoid the need to tunnel
all Router Advertisements from the home link to a mobile node away
from home, those Router Advertisements that are tunneled to the
mobile node are retransmitted until acknowledged. To avoid possible
security attacks from forged Router Advertisements tunneled to
the mobile node, all such tunneled Router Advertisements must be
authenticated to the mobile node by its home agent using AH [8] or
ESP [9].

Specifically, a home agent serving some mobile node SHOULD construct
and tunnel to the mobile node a new Router Advertisement when any of
the following conditions occur:

 - The preferred or valid lifetime for an existing prefix on the
    home link is reduced.

 - A new prefix is introduced on the home link.

 - The state of the home agent's AdvManagedFlag flag [13] changes
    from FALSE to TRUE or from TRUE to FALSE.

The home agent determines these conditions based on its own
configuration as a router and based on the Router Advertisements
that it receives on the home link. The home agent constructs a new
Router Advertisement message containing no options other than the
Prefix Information options describing the prefixes for which one of
the conditions above has occurred since the last Router Advertisement
tunneled to and acknowledged by the mobile node. When multiple
conditions occur at or near the same time, the home agent SHOULD
attempt to combine them into a single Router Advertisement message to
the mobile node.

In tunneling each such Router 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.

 - The packet MUST include either an AH [8] or ESP [9] header
    providing sender authentication, data integrity protection, and
    replay protection.

 - The packet MUST include a Binding Request destination option.

  - The packet MUST be tunneled to the mobile node's primary care-of
    address using a Routing header, in the same way as any 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 this
tunneled packet 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). If
while the mobile node is still retransmitting a Router Advertisement
to the mobile node, another condition as described above occurs on
the home link causing another Router Advertisement to be tunneled to
the mobile node, the home agent SHOULD combine any Prefix Information
options in the unacknowledged Router Advertisement into the new
Router Advertisement and then begin retransmitting the new Router
Advertisement rather than the old one.

In addition, as described in Section 9.3, the lifetime returned by a
mobile node's home agent in its Binding Acknowledgement in response
to registration of a new primary care-of address by the mobile node
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 10.7, 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 a binding lifetimes ensure that no node uses a mobile node's home
address beyond the time that 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.

[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 [[11](#), [12](#)]. 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.

If the mobile node uses one of its care-of addresses as the source
of some packet while away from home, no special Mobile IP processing

is required for sending this packet. The packet is simply addressed
and transmitted in the same way as any normal IPv6 packet, setting
the Source Address field in the packet's IPv6 header to this care-of
address.

On the other hand, if while away from home, the mobile node uses its
home address as the source of a packet from the point of view of
higher protocol layers or applications as described above, special
Mobile IP processing of this packet is required for the insertion of
the Home Address option. Specifically:

 - Since Mobile IP is transparent to higher protocol layers (e.g.,
   to TCP), the packet is initially constructed 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.

 - If the mobile node is at home, no special Mobile IP processing
   for this packet is required. The packet is sent normally and the
   following additional steps are not performed.

 - Likewise, if the Source Address field in the packet's IPv6 header
   is not the mobile node's home address, no special Mobile IP
   processing for this packet is required. The packet is sent
   normally and the following additional steps are not performed.

 - Otherwise, 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.

This addition of the Home Address option to a packet MUST be
performed before outgoing IPsec processing, such as the addition of
an AH [8] or ESP [9] header to the packet, is performed. Likewise,
IPsec processing for a received packet containing a Home Address
option MUST be performed before the packet is possibly modified as
part of processing the Home Address option. 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 [6].

10.2. **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 its previous default router when
      moving from this care-of address to another, and if the Binding
      Cache entry that was created from this Binding Update is still
      present in this router's Binding Cache, then such a packet
      will be intercepted by this router, encapsulated using IPv6
      encapsulation [4], and tunneled to the mobile node's primary
      care-of address (registered with this router, acting as a home
      agent for this out-of-date care-of address).

   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 10.7, subject to the
   rate limiting defined in Section 10.10. 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 [5], 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 [5]. 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.

10.3. 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. The description here is based on
the conceptual model of the organization and data structures defined
by Neighbor Discovery [13].

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 [13].
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) 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 10.4. The mobile node registers
its primary care-of address with its home agent, as described in

Section 10.5.

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 to 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 [13], 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,
a mobile node SHOULD consider receipt of any IPv6 packets from its
current default router as an indication that it is still reachable
from the router. Both packets from the router's IP address and
(IPv6) packets from its link-layer address (e.g., those forwarded but
not originated by the router) SHOULD be considered.

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 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.

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, it is possible that additional
indications about link-layer mobility can be obtained from
lower-layer protocol or device driver software within the mobile
node. However, a mobile node MUST NOT assume that all link-layer
mobility indications from lower layers 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.

10.4. 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 (not 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 10.15.

As described in Section 4, in order to form a new care-of address,
a mobile node MAY use either stateless [22] 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.

10.5. Sending Binding Updates to the Home Agent

After deciding to change its primary care-of address as described
in Sections 10.3 and 10.4, 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, or the Care-of Address
    Present (C) bit MUST be set in the Binding Update and the care-of
    address for the binding MUST be specified in the Care-of Address
    field in the Binding Update.

 - 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 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).

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.

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, since each
MUST contain an AH [8] or ESP [9] header to authenticate the Binding
Update as coming from the home address being bound.

10.6. **Dynamic Home Agent Address Discovery**

It is possible that 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 10.5, 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 SHOULD use the dynamic home agent
address discovery procedure to find the address of a suitable home
agent on its home link. To do so, the mobile node sends the packet,
as described above, with the Destination Address in the packet's IPv6
header set to the Home-Agents anycast address for its home subnet
prefix. As described in Section 9.2, the home agent on its home link
that receives this Binding Update will reject the Update, returning
to the mobile node the home agent's own global unicast IP address
along with a list of the global unicast IP addresses of each other
home agent operating on the home link. The mobile node SHOULD then
retransmit its Binding Update to one of these homes agent using the
provided global unicast address; the mobile node MAY re-attempt
this 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.

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 procedure described
above.

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

A mobile node MAY send a Binding Update to any correspondent node at
any time to allow it to cache its current care-of address (subject to
the rate limiting defined in [Section 10.10]). 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 field in 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
Lifetime value sent in the Binding Update MUST be no greater than
the remaining lifetime of the mobile node's home registration of its
primary care-of address at its home agent.

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 remaining lifetime of the binding, initialized from the
    Lifetime field sent in the Binding Update.

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.

In general, when a mobile node sends a Binding Update to its home
agent to register a new primary care-of address (as described in
[Section 10.5]), the mobile node will also send a Binding Update to
each other node for which an entry exists in the mobile node's
Binding Update List. 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 has
no Binding Cache entry for the mobile node, or for which the mobile
node can deduce that the original sender of the packet has an
out-of-date care-of address 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 10.10). 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, if the mobile node has an entry in its Binding
     Update List representing an unexpired Binding Update sent to
     a previous default router for this previous care-of address
     (Section 10.8).

  - 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.

10.8. Sending Binding Updates to the Previous Default Router

After switching to a new default router (and thus also changing its
primary care-of address), a mobile node MAY send a Binding Update to
its previous default router, giving its new care-of address. The
packet carrying the Binding Update MUST be addressed to the mobile
node's previous default router's global unicast address, learned
by the mobile node based on Prefix Information options received in
Router Advertisements from it in which the Router Address (R) bit is
set.

If the mobile node sends such a Binding Update, the home address
for the binding, specified in the Home Address option included in
the packet carrying this Binding Update, MUST be set the mobile
node's old primary care-of address (that it used while using this
default router), and the care-of address for the binding (either the
Source Address in the packet's IPv6 header or the Care-of Address
field in the Binding Update) MUST be set to the mobile node's new
primary care-of address. In addition, the Home Registration (H)
bit MUST also be set in this Binding Update, to request the mobile
node's previous default router to temporarily act as a home agent
for the mobile node's old primary care-of address. The previous
default router will thus tunnel packets for the mobile node to its
new care-of address. All of the procedures defined for home agent
operation must be followed by this previous default router for this
registration. Note that the previous router does not necessarily
know the mobile node's (permanent) home address as part of this
registration.

[10.9](#). Retransmitting Binding Updates

   If, after sending a Binding Update in which the Acknowledge (A) bit
   is set, a mobile node fails to receive a Binding Acknowledgement
   within INITIAL_BINDACK_TIMEOUT seconds, the mobile node SHOULD
   retransmit the Binding Update until a Binding Acknowledgement
   is received. Such a retransmitted Binding Update MUST use the
   same Sequence Number value as the original transmission. 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.

[10.10](#). Rate Limiting for Sending Binding Updates

   A mobile node MUST NOT send Binding Updates more often than once per
   MAX_UPDATE_RATE seconds to any node. 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.

[10.11](#). 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 contains a valid AH [8] or ESP [9] header providing
     sender authentication, data integrity protection, and replay
     protection.

   - The Option Length field in the option is greater than or equal to
     11 octets.

   - 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.

- 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 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 10.10. In particular, if the Status field
  is equal to 135 (dynamic home agent address discovery response),
  then the mobile node MAY reattempt its home registration with
  the home agent address given in the Source Address field of the
  packet carrying the Binding Acknowledgement or with any of the
  home agent IP addresses listed in the Home Agents List field in
  the Binding Acknowledgement. If any of these addresses is not a
  global unicast address or does not have a subnet prefix equal to
  the mobile node's own subnet prefix, then that particular address
  MUST be ignored and the mobile node MUST NOT reattempt its home
  registration with that home agent.

10.12. 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 returns 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.

[10.13](). 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.

[10.14](). Receiving Tunneled Router Advertisements

[Section 9.7]() describes the operation of a home agent to support
renumbering a mobile node's home subnet while the mobile node is
away from home. The home agent tunnels certain Router 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 tunneled Router Advertisement, it MUST
validate it according to the following tests:

  - The Source Address of the IP packet carrying the Router
     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.

  - The packet contains either an AH [[8]()] or ESP [[9]()] header providing
     sender authentication, data integrity protection, and replay
     protection.

- The packet contains a Binding Request destination option.

Any received tunneled Router Advertisement not meeting all of these
tests MUST be silently discarded.

If a received tunneled Router Advertisement is not discarded
according to the tests listed above, the mobile node MUST process the
Router Advertisement as if it were connected to its home link [13].
Such processing MAY result in the mobile node configuring a new home
address, although due to separation between preferred lifetime and
valid lifetime, such changes should not affect most communication by
the mobile node, in the same way as for nodes that are at home.

In addition, in processing the packet containing this Router
Advertisement, the mobile node SHOULD return to the home agent a
Binding Update in response to the Binding Request carried in the
packet. The correct formation of this Binding Update by the mobile
node and processing of it by the home agent will be viewed by the
home agent as an acknowledgement of this Router Advertisement,
confirming to it that this Router Advertisement was received by the
mobile node.

10.15. Using Multiple Care-of Addresses

As described in Section 10.4, 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 10.3. 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 10.5.

To assist with smooth handoffs, 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.

[10.16](). 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 its care-of
address sharing a subnet prefix with the multicast router, as
the source IPv6 address of its multicast group membership control
messages.

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

A mobile node that wishes to send packets to a multicast group
also has two options: (1) send directly on the foreign link being
visited; or (2) send via a tunnel to its home agent. Because
multicast routing in general depends upon the Source Address used in
the IPv6 header of the multicast packet, a mobile node that tunnels a
multicast packet to its home agent MUST use its home address as the
IPv6 Source Address of the inner multicast packet.

[10.17](). Returning Home

A mobile node detects that it has returned to its home link through
the movement detection algorithm in use ([Section 10.3]()), 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.

In addition, the mobile node MUST multicast onto the home link
(to the all-nodes multicast address) a Neighbor Advertisement
message [[13]()], 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 [13].

[11](). Constants

```
INITIAL_BINDACK_TIMEOUT    1 second

MAX_BINDACK_TIMEOUT        256 seconds

MAX_UPDATE_RATE            once per second

SLOW_UPDATE_RATE           once per 10 seconds

MAX_FAST_UPDATES           5 transmissions

MAX_ADVERT_REXMIT          3 transmissions
```

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

- The Home Address option, described in Section 5.4

In addition, this document defines two new Neighbor Discovery [13]
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.

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

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 Home-Agents anycast address, used in the dynamic home agent
  address discovery procedure described in Sections 9.2 and 10.6.

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 was 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. The Binding Request option does open
   some issues with binding privacy, but those issues can be dealt with
   either through existing IPsec encryption mechanisms or through use of
   firewalls.

   The existing IPsec replay protection mechanisms allow a "replay
   protection window" to support receiving packets out of order.
   Although appropriate for many forms of communication, Binding Updates
   MUST be applied only in the order sent. The Binding Update option
   thus includes a Sequence Number field to provide this necessary
   sequencing. The use of this Sequence Number together with IPsec
   replay protection is similar in many ways, for example, to the the
   sequence number in TCP. IPsec provides strong replay protection but
   no ordering, and the sequence number provides ordering but need not
   worry about replay protection such as through the sequence number
   wrapping around.

13.2. 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 [6]. 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.

However, if a node receiving a packet that includes a Home Address
option implements the processing of this option by physically
copying the Home Address field from the option into the IPv6 header,
replacing the Source Address field there, then the ability to
trace the true location of the sender is removed once this step
in the processing is performed. This diminishing of the power of
ingress filtering only occurs once the packet has been received at
its ultimate destination, and does not affect the capability of
ingress filtering while the packet is in transit. Furthermore, this
diminishing can be entirely eliminated by appropriate implementation
techniques in the receiving node. For example, the original contents
of the Source Address field (the sending care-of address) could be
saved elsewhere in memory with the packet, until all processing of
the packet is completed.

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 do not wish others to have
access to should use additional mechanisms (such as encryption) to
provide privacy protection, but 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 can create a tunnel to its home
agent. Then, packets destined for correspondent nodes will appear

to emanate from the home subnet, and it may be more difficult to

pinpoint the location of the mobile node. Such mechanisms are all
beyond the scope of this document.

Changes from Previous 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-ipv6-05.txt:

    - Clarified that the Advertisement Interval option in Section 6.3
       MAY be included in Router Advertisements by any router, not just
       by home agents.

    - Modified Section 6.5 to document a required change to the
       MaxRtrAdvInterval limit, in addition to the change to the
       MinRtrAdvInterval limit, and clarified that these new limits MAY
       be used by any router, not just by home agents.

    - Added Section 6.6 to document new limits on sending Router
       Solicitations by a mobile node while away from home. These
       changes are related to the MAX_RTR_SOLICITATIONS and
       RTR_SOLICITATION_INTERVAL Neighbor Discovery constants.

    - Added Section 6.2 documenting a modification to the format of
       a Prefix Information option for use in Router Advertisement
       messages. This modification allows a router to easily and
       efficiently advertise its own global unicast address.

    - Defined a new Home Agent Information Option for Router
       Advertisements (Section 6.4). This option allows those routers
       functioning as a home agent to optionally specify a preference
       (relative to other home agents on this link) and a lifetime for
       this advertisement for providing home agent service. Use of this
       option by home agents is optional.

    - Added Section 10.2, defining the general procedures to be used
       by a mobile node in receiving packets while away from home. In
       particular, for packets received with a Routing header, this
       section defines an exception for any use of a Routing header
       automatically derived by "reversing" the received Routing header,
       for any response packets sent by upper-layer protocols.

    - Changed the treatment of packets addressed to a mobile node's
       site-local address while the mobile node is away from home. The
       current consensus of the Mobile IP Working Group is that such
       packets 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 undefined in IPv6, and this default behavior might
       change at some point in the future.

    - Added a definition of the treatment of multicast packets

addressed to a multicast group to which a mobile node is

       subscribed, for which the multicast scope is link-local,
       site-local, organization-local, etc. As with packets sent to a
       mobile node's link-local and site-local addresses, link-local
       multicast packets MUST NOT be tunneled to the mobile node, and
       multicast packets addressed to a multicast address with scope
       larger than link-local but smaller than global (e.g., site-local
       and organization-local) SHOULD be tunneled to the mobile node by
       default, but this behavior MUST be configurable to disable it.

   -   Added Section 7.2, detailing Mobile IP requirements on all IPv6
       routers. They SHOULD be able to send an Advertisement Interval
       option in their Router Advertisements, and SHOULD be able to
       support sending unsolicited multicast Router Advertisements at
       the faster rate described in Section 6.5.

   -   Added Section 10.14 describing the mobile node side of
       renumbering the home network, matching the home agent processing
       described in Section 9.7.

   -   Simplified the sequence of tests in Section 9.4 performed by a
       home agent being requested to no longer serve as the sending
       mobile node's home agent.

   -   Clarified in Section 10.5 that if a mobile node has multiple home
       addresses using different interface identifiers, then it SHOULD
       send a separate Binding Update to its home agent for each.

   -   Finally filled in Section 2, giving a comparison of Mobile IPv6
       with Mobile IP for IPv4.

Acknowledgements

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). Internet-Draft,
       draft-ietf-dhc-dhcpv6-10.txt, May 1997. 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. Internet-Draft,
       draft-ietf-ipngwg-ipv6-tunnel-07.txt, December 1996.
       Work in progress.

   [5] Stephen E. Deering and Robert M. Hinden. Internet
       Protocol version 6 (IPv6) specification. Internet-Draft,
       draft-ietf-ipngwg-ipv6-spec-v2-00.txt, July 1997. Work in
       progress.

   [6] Paul Ferguson and Daniel Senie. Network ingress filtering:
       Defeating denial of service attacks which employ IP source
       address spoofing. RFC 2267, January 1998.

   [7] Robert M. Hinden and Stephen E. Deering. IP Version 6
       addressing architecture. Internet-Draft,
       draft-ietf-ipngwg-addr-arch-v2-06.txt, January 1998. Work in
       progress.

   [8] Stephen Kent and Randall Atkinson. IP Authentication header.
       Internet-Draft, draft-ietf-ipsec-auth-header-02.txt, October
       1997. Work in progress.

   [9] Stephen Kent and Randall Atkinson. IP Encapsulating Security
       Payload (ESP). Internet-Draft, draft-ietf-ipsec-esp-v2-01.txt,
       October 1997. Work in progress.

  [10] Stephen Kent and Randall Atkinson. Security architecture for
       the Internet Protocol. Internet-Draft,
       draft-ietf-ipsec-arch-sec-02.txt, November 1997. Work in
       progress.

  [11] P. Mockapetris. Domain Names -- concepts and facilities.
       RFC 1034, November 1987.

  [12] P. Mockapetris. Domain Names -- implementation and
       specification. RFC 1035, November 1987.

[13] Thomas Narten, Erik Nordmark, and William Allen Simpson.
     Neighbor Discovery for IP version 6 (IPv6). Internet-Draft,
     draft-ietf-ipngwg-discovery-v2-00.txt, July 1997. Work in
     progress.

[14] Charles Perkins. IP encapsulation within IP. RFC 2003, October
     1996.

[15] Charles Perkins, editor. IP mobility support. RFC 2002,
     October 1996.

[16] Charles Perkins. Minimal encapsulation within IP. RFC 2004,
     October 1996.

[17] Charles Perkins and David B. Johnson. Route optimization in
     Mobile IP. Internet-Draft, draft-ietf-mobileip-optim-07.txt,
     November 1997. Work in progress.

[18] 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.

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

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

[21] Joyce K. Reynolds and Jon Postel. Assigned numbers. RFC 1700,
     October 1994.

[22] Susan Thomson and Thomas Narten. IPv6 stateless address
     autoconfiguration. Internet-Draft,
     draft-ietf-ipngwg-addrconf-v2-00.txt, July 1997.

Chair's Address

    The Working Group can be contacted via its current chairs:

        Jim Solomon
        RedBack Networks
        1389 Moffett Park Drive
        Sunnyvale, CA 94089-1134
        USA

        Phone: +1 408 548-3583
        Fax: +1 408 548-3599
        E-mail: solomon@rback.com

        Erik Nordmark
        Sun Microsystems, Inc.
        2550 Garcia Avenue
        Mt. View, CA 94041
        USA

        Phone: +1 415 786-5166
        Fax: +1 415 786-5896
        E-mail: nordmark@sun.com

Authors' Addresses

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

        David B. Johnson
        Carnegie Mellon University
        Computer Science Department
        5000 Forbes Avenue
        Pittsburgh, PA 15213-3891
        USA

        Phone: +1 412 268-7399
        Fax: +1 412 268-5576
        E-mail: dbj@cs.cmu.edu

        Charles Perkins
        Sun Microsystems, Inc.
        Technology Development Group
        Mail Stop MPK15-214
        Room 2682
        901 San Antonio Road
        Palo Alto, CA 94303
        USA

        Phone: +1 415 786-6464
        Fax: +1 415 786-6445
        E-mail: cperkins@eng.sun.com