Mobile IP Working Group
INTERNET-DRAFT

David B. Johnson
Carnegie Mellon University
Charles Perkins
IBM Corporation
13 June 1996

Mobility Support in IPv6

<draft-ietf-mobileip-ipv6-01.txt>

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 packets destined for the mobile node directly to it at this care-of address.

Status of This Memo

This document is a submission by the Mobile IP Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the Working Group mailing list at "mobile-ip@SmallWorks.COM". Distribution of this memo is unlimited.

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

To learn the current status of any Internet-Draft, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

Contents

1. Introduction

This document specifies the operation of mobile computers using Internet Protocol Version 6 (IPv6) [6]. 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, known as Mobile IPv6, allows transparent routing of IPv6 packets to mobile nodes using the mobile node's home IPv6 address, regardless of the mobile node's current point of attachment to the Internet.

The most important function needed to support such routing to mobile nodes is the reliable and timely notification of a mobile node's current location to those other nodes that need it. Correspondent nodes communicating with a mobile node need this location information in order to correctly deliver their own packets to a mobile node; Mobile IPv6 allows correspondent nodes to learn and cache a mobile node's location, and to use this cached information to route their own packets directly to a mobile node at its current location. The mobile node's "home agent", a router on the mobile node's home network, also needs this location information in order to forward intercepted packets from the home network to the mobile node, for correspondent nodes that have not yet learned the mobile node's location, and indeed, for correspondent nodes that do not even yet know that the mobile node is currently away from home.

A mobile node's current location is represented as a "care-of address", an IPv6 address assigned to the mobile node (in addition to its home IPv6 address) within the foreign network currently being visited by the mobile node. The association between a mobile node's home address and its care-of address, along with the remaining lifetime of that association, is known as a "binding", and the mobile node notifies other nodes about its current binding using a new destination option called a Binding Update. IPv6 correspondent nodes then use a Routing header to deliver subsequent packets to the mobile node's care-of address. All IPv6 nodes and routers MUST be able to cache mobile node bindings received in Binding Updates; this leads to dramatic simplifications in the required protocols, compared to the methods required for IPv4.

In this document, "movement" is considered to be a change in a mobile node's point of attachment to the Internet such that it is no longer link-level connected to the same IPv6 subnet (network prefix) as it was previously. If a mobile node is not currently link-level connected to its home IPv6 network, the mobile node is said to be "away from home".

1.1. Design Requirements

A mobile node must continue to be able to be addressed by its home IPv6 address, and to be able to communicate with other IPv6 nodes using its home address, after changing its link-level point of attachment from one IPv6 subnet to another.

All messages used to update another node as to the location of a mobile node must be authenticated in order to protect against remote redirection attacks.

1.2. Goals

The number of administrative messages sent over the link by which a mobile node is directly attached to the Internet should be minimized, and the size of these messages should be kept as small as is reasonably possible. This link may often be a wireless link, having a substantially lower bandwidth and higher error rate than traditional wired networks, and many mobile nodes are likely to operate on limited battery power. By reducing the number and size of administrative messages required for mobility support, network resources and mobile node battery resources are conserved.

1.3. Assumptions

This protocol places no additional constraints on the assignment of IPv6 addresses. That is, a mobile node may acquire its addresses using stateless address autoconfiguration [12], or alternatively using a stateful address configuration protocol such as DHCPv6 [3] or PPPv6 [7].

This protocol assumes that any mobile node will generally not change its link-level point of attachment from one IPv6 subnet to another more frequently than once per second.

This protocol assumes that IPv6 unicast packets are routed based on the Destination Address in the packet's IPv6 header (and not, for example, by source address).

1.4. Applicability

Mobile IPv6 is intended to enable nodes to move from one IPv6 subnet to another. It is just as suitable for mobility across homogeneous media as it is for mobility across heterogeneous media. That is, Mobile IPv6 facilitates node movement from one Ethernet segment to

another as well as it accommodates node movement from an Ethernet segment to a wireless LAN, as long as the mobile node's IPv6 address remains the same after such a movement.

One can think of Mobile IPv6 as solving the "macro" mobility management problem. It is less well suited for more "micro" mobility management applications -- for example, handoff amongst wireless transceivers, each of which covers only a very small geographic area. As long as node movement does not occur between link-level points of attachment on different IPv6 subnets, link-layer mechanisms for mobility management (i.e., link-layer handoff) may offer faster convergence and far less overhead than Mobile IPv6.

1.5. Terminology

This document uses the following special terms:

Binding

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

Binding Cache

A cache, maintained by each IPv6 node, of bindings for other nodes. 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 node until the expiration of its binding lifetime, whereas other Binding Cache entries MAY be replaced at any time by any reasonable local cache replacement policy. The Binding Cache is a conceptual data structure used in this document, which may be implemented in any manner consistent with the external behavior described here, for example by being combined with the node's Destination Cache as maintained through Neighbor Discovery [9].

Binding Update List

A list, maintained by each IPv6 mobile node, of the IPv6 address of each other node to which this node has sent a Binding Update giving its binding, such that the lifetime of the binding sent to that node has not yet expired. This is a conceptual data structure used in this document, which may be implemented in any manner consistent with the external behavior described here.

Care-of Address

An IPv6 address associated with a mobile node while visiting a foreign network, which uses the network prefix of that foreign network. Among the multiple care-of addresses that a mobile node may have at a time (with different network prefixes), the one registered with its home agent is called its "primary" care-of address.

Correspondent Node

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

Foreign Network

Any network other than the mobile node's home network.

Home Address

An IPv6 address that is assigned for an extended period of time to a mobile node. It remains unchanged regardless of the node's current link-level point of attachment to the Internet.

Home Agent

A router on a mobile node's home network that, while the mobile node is away from home, intercepts packets on the home network destined to the mobile node's home address, encapsulates them, and tunnels them to the mobile node's current care-of address. The home agent maintains a registry of the current binding for mobile nodes whose home address is on the home network routed by the home agent.

Home Network

A network, which may possibly be a virtual network, having a network prefix matching that of a mobile node's home address. Standard IPv6 routing mechanisms will deliver packets destined for a mobile node's home address to the mobile node's home network.

Link

A facility or medium over which nodes can communicate at the link layer. A link underlies the network layer.

Mobile Node

A node that can change its link-level point of attachment from one IPv6 subnet to another, while still being addressable via its IPv6 home address.

Node

A host or a router.

Tunnel

The path followed by a packet while it is encapsulated. The model is that, while it is encapsulated, a packet is routed to a knowledgeable decapsulating agent, which decapsulates the packet and then correctly delivers it to its ultimate destination.

Virtual Network

A network with no physical instantiation beyond a home agent (with a physical network interface on another network). The home agent generally advertises reachability to the network prefix of the virtual network using conventional routing protocols.

1.6. Specification Language

In this document, several words are used to signify the requirements of the specification. These words are often capitalized.

MUST

This word, or the adjective "required", means that the definition is an absolute requirement of the specification.

MUST NOT

This phrase means that the definition is an absolute prohibition of the specification.

SHOULD

This word, or the adjective "recommended", means that, in some circumstances, valid reasons may exist to ignore this item, but the full implications must be understood and carefully weighed

before choosing a different course. Unexpected results may result otherwise.

MAY

This word, or the adjective "optional", means that this item is one of an allowed set of alternatives. An implementation which does not include this option MUST be prepared to interoperate with another implementation which does include the option.

silently discard

The implementation discards the packet without further processing, and without indicating an error to the sender. The implementation SHOULD provide the capability of logging the error, including the contents of the discarded packet, and SHOULD record the event in a statistics counter.

2. Overview of Mobile IPv6 Operation

In addition to its (permanent) IPv6 home address, a mobile node while away from home will have assigned to its network interface(s) a "primary care-of address" and possibly other "care-of addresses". A care-of address is an IPv6 address assigned to a mobile node only while visiting a particular foreign network, typically acquired through stateless [12] or stateful (e.g., DHCPv6 [3]) address autoconfiguration. The decision about which manner of address autoconfiguration to use is made according to the methods of IPv6 Neighbor Discovery [9].

Each time a mobile node moves its link-level point of attachment from one IPv6 subnet to another, it will configure its primary care-of address at its new point of attachment, and will send a Binding Update containing that care-of address to its home agent. The care-of address for a mobile node registered with its home agent is known as the mobile node's "primary" care-of address, and the mobile node may also have additional care-of addresses, one for each of the network prefixes that it currently considers to be on-link. Each time it changes its primary care-of address, a mobile node also sends a Binding Update to each other (correspondent) node that may have an out-of-date care-of address for the mobile node in its Binding Cache.

A mobile node attached to the Internet can always be reached by sending packets to its home IPv6 address. If the mobile node is not present on its home network, any packet arriving there for it will be intercepted there by its home agent, which will tunnel the packet to the mobile node's current primary care-of address. The home agent uses IPv6 encapsulation [5] to tunnel the packet.

A correspondent node sending a packet checks its Binding Cache for an entry for the Destination Address of the packet, and uses a Routing header (instead of encapsulation) to route the packet to the destination mobile node's care-of address if a cached binding is found. Otherwise, the correspondent node sends the packet normally (with no Routing header), and the packet is then intercepted and tunneled by the mobile node's home agent as described above. When the tunneled packet reaches the mobile node, the mobile node returns a Binding Update to the correspondent node, allowing it to cache the mobile node's binding for future packets.

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 between the correspondent node and 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 network. In addition, the impact of of any possible failure of the home agent, the home network, or intervening networks leading to the home network is drastically reduced, since these components are not involved in the delivery of most packets to the mobile node.

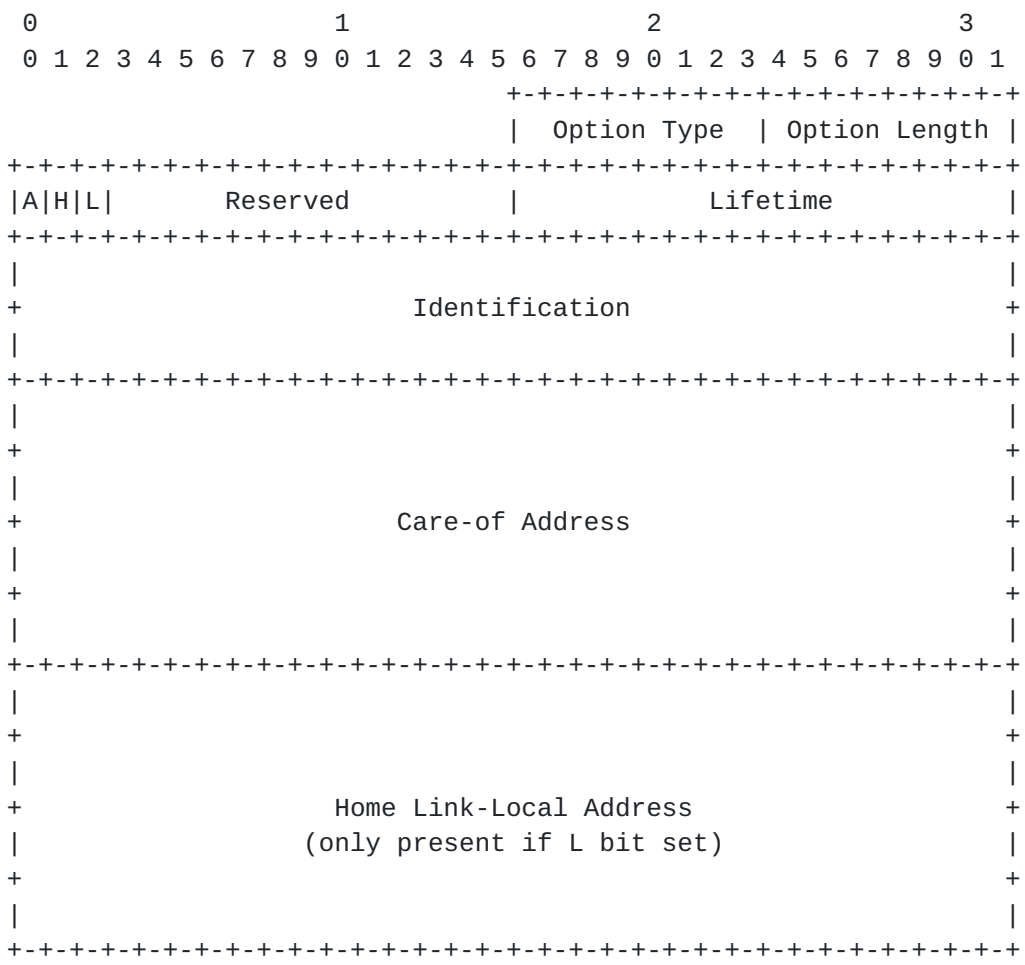
3. Message and Option Formats

3.1. Binding Update Option

A Binding Update is a new IPv6 destination option, used by a mobile node to notify a correspondent node or its home agent of its current care-of address. As a destination option, it can appear in a Destination Options header in any IPv6 packet [6], and thus can be included in any normal data packet or can be sent in a separate packet containing no data. The Binding Update contains the mobile node's care-of address, an identification for the Update (to sequence Updates and to protect against attempts to replay it), and a lifetime for the binding. The mobile node's IPv6 home address MUST be the source address of the packet containing the Binding Update, since the option does not contain space to separately represent the mobile node's home address.

Binding Updates should be considered a form of routing updates; handled incorrectly, they could be a source of security problems and routing loops. Therefore, packets which include Binding Updates MUST also include an IPv6 Authentication header [1]; sequencing and replay protection is then achieved by use of the Identification field in the Binding Update.

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



Option Type

16

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, this field must be set to 28.

Acknowledge (A)

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

Home Registration (H)

The Home Registration (H) bit is set by the sending node to request the receiving node to act as this node's home agent. The Destination Address in the IPv6 header of the packet carrying this option MUST be that of a router sharing the same network prefix as the mobile node's home IPv6 address.

Home Link-Local Address Present (L)

The Home Link-Local Address Present (L) bit indicates the presence of the Home Link-Local Address field in the Binding Update. This bit is set by the sending mobile node to request the receiving node to act as a proxy (for participating in the Neighbor Discovery Protocol) for the node while it is away from home. This bit MUST NOT be set unless the Home Registration (H) bit is also set in the Binding Update.

Reserved

Sent as 0; ignored on reception.

Lifetime

16-bit unsigned integer. The number of seconds remaining before the binding must be considered expired. A value of all ones (0xffff) indicates infinity. A value of zero indicates that the Binding Cache entry for the mobile node should be deleted.

Identification

a 64-bit number used to sequence Binding Updates and to match a returned Binding Acknowledgement message with this Binding Update. The Identification field also serves to protect against replay attacks for Binding Updates.

Care-of Address

The current care-of address of the mobile node. When set equal to the home address of the mobile node, the Binding Update option instead indicates that any existing binding for the mobile node should be deleted; no binding for the mobile node should be created.

Home Link-Local Address

The link-local address of the mobile node used by the mobile node when it was last attached to its home network. This field in the Binding Update is optional and is only present when the Home Link-Local Address (L) bit is set.

As with all IPv6 options, the highest-order three bits of the Option Type Field (16) of the Binding Update option specify the following properties of the option:

- The highest-order two bits are 00: Any node receiving this option that does not recognize the Option Type MUST skip over this option and continue processing the header.

- The third-highest-order bit is 0: The Option Data does not change en-route, and thus, when an Authentication header is present in the packet, the entire Binding Update option MUST be included when computing or verifying the packet's authenticating value.

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 28 octets, the remaining octets are interpreted as extensions. Currently no extensions have been defined.

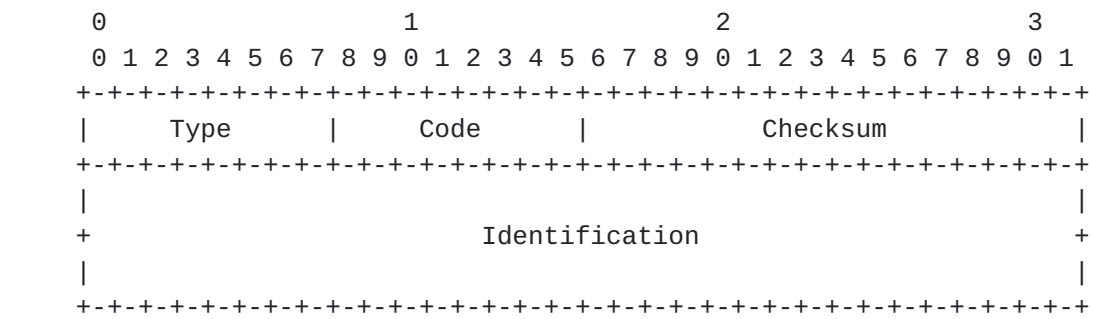
3.2. ICMP Binding Acknowledgement Message

A Binding Acknowledgement message is an informational ICMP message used to acknowledge acceptance of a Binding Update (Section 3.1) option, if that Binding Update has the Acknowledge (A) bit set.

Upon receipt of a Binding Update requesting an acknowledgement, the receiving node returns a Binding Acknowledgement message addressed to the care-of address in the Binding Update.

If a mobile node fails to receive an acceptable Binding Acknowledgement message within INITIAL_BINDACK_TIMEOUT seconds after transmitting the Binding Update, it SHOULD retransmit the Binding Update until a Binding Acknowledgement is received. Such a retransmitted Binding Update MUST use he same Identification value as the original transmission. The retransmissions by the mobile node MUST use an exponential back-off process, in which timeout period is doubled upon each retransmission until either the node receives a Binding Acknowledgement message or the timeout period reaches the value MAX_BINDACK_TIMEOUT.

The ICMP Binding Acknowledgement message has the following format:



Type

133

Code

8-bit unsigned integer indicating the disposition of the Binding Update. Values of the Code field less than 128 indicate that the Binding Update was accepted by the receiving node. The following such values are currently defined:

0 Binding Update accepted

Values of the Code field greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such 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 network
134	Identification field mismatch
135	Unknown home agent address

Checksum

The checksum of the message calculated as specified for ICMP for IPv6 [4].

Identification

The acknowledgement Identification is derived from the Binding Update option, for use by the mobile node in matching the acknowledgement with an outstanding Binding Update.

Up-to-date values of the Code field are to be specified in the most recent "Assigned Numbers" [10].

Extensions to the Binding Acknowledgement message format may be included after the fixed portion of the Binding Acknowledgement message specified above. The presence of such extensions will be indicated by the ICMP message length, derived from the IPv6 Payload Length field. When the Option Length is greater than 16 octets, the remaining octets are interpreted as extensions. Currently no extensions have been defined.

4. Requirements for IPv6 Nodes

Mobile IPv6 places some special requirements on the functions provided by different IPv6 nodes. This section itemizes those requirements, identifying the functionality each requirement is intended to support. Further details on this functionality is provided in the following sections.

Since any IPv6 node may at any time be a correspondent of a mobile node, all IPv6 nodes MUST support the following requirements:

- Every IPv6 node MUST be able to process a received Binding Update option, and to return a Binding Acknowledgement message if requested.

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

- Every IPv6 node MUST be able to maintain Security Associations for use in IPv6 Authentication Headers [2, 1, 6]. An IPv6 node receiving a packet containing a Binding Update option MUST verify, using the Authentication Header in the packet, the authenticity of the sender (the mobile node for which this binding applies) before modifying its Binding Cache in response to that Binding Update option.

Since any IPv6 router may at any time have a Binding Cache entry for a mobile node, all IPv6 router MUST support the following requirement:

- Every IPv6 router MUST be able to use its Binding Cache in forwarding packets; if the router has a Binding Cache entry for the Destination Address of a packet it is forwarding, then the router SHOULD encapsulate the packet and tunnel it to the care-of address in the Binding Cache entry.

In order for a mobile node to correctly operate while away from home, at least one IPv6 router in its home network must support functioning as a home agent for the mobile node. All IPv6 routers capable of serving as a home agent MUST support the following special requirements:

- Every home agent MUST be able to maintain a registry of mobile node bindings for those mobile nodes for which it is serving as the home agent.

- Every home agent MUST be able to intercept packets (e.g., using Neighbor Advertisements) on the local network addressed to

a mobile node for which it holds a binding in its registry indicating that the mobile node is currently away from home.

- Every home agent MUST be able to encapsulate such intercepted packets in order to tunnel them to the care-of address for the mobile node indicated in its binding.

- Every home agent MUST be able to issue Binding Acknowledgement messages in response to Binding Updates received from a mobile node.

- Every home agent MUST be able to maintain Security Associations for the mobile nodes from which it will accept Binding Updates.

Finally, all IPv6 nodes capable of functioning as mobile nodes MUST support the following requirements:

- Every IPv6 mobile node MUST be able to perform IPv6 decapsulation [5].

- Every IPv6 mobile node MUST support sending Binding Updates, as specified in Sections 6.3, 6.4, and 6.5; and MUST be able to receive and process Binding Acknowledgement messages, as specified in Section 6.7.

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

5. Binding Cache Management

The Binding Cache is the central data structure in Mobile IPv6. All IPv6 nodes MUST support maintenance of a Binding Cache, and MUST support processing of received Binding Updates. This section describes the management aspects of a Binding Cache common to all nodes.

5.1. Receiving Binding Updates

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

- The packet contains an IP Authentication header and the authentication is valid [1]. The Authentication header is assumed to provide both authentication and integrity protection.

- The length of the option specified in the Option Length field is greater than or equal to 28 octets.

- The Identification field is valid.

Any Binding Update 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.

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

- If the Lifetime specified in the Binding Update is nonzero and the specified Care-of Address differs from the Home Address, this is a request to cache a binding for the mobile node. Processing for this type of received Binding Update is described in Section 5.2.

- If the Lifetime specified in the Binding Update is zero or the specified Care-of Address matches the Home Address, then this is a request to delete the mobile node's binding. Processing for this type of received Binding Update is described in Section 5.3.

5.2. Requests to Cache a Binding

If a node receives a valid Binding Update requesting it to cache a binding for a mobile node, as specified in Section 5.1, then the node MUST examine the Home Registration (H) bit in the Binding Update

to determine how to further process the Binding Update. If the Home Registration (H) bit is set, the Binding Update is processed according to the procedure specified in Section 7.1.

If the Home Registration (H) bit is not set, then the receiving node SHOULD create a new entry in its Binding Cache for this mobile node's Home Address (or update its existing Binding Cache Entry for this Home Address) to record the Care-of Address as specified in the Binding Update, and begin a timer to delete this Binding Cache entry after the expiration of the Lifetime period specified in the Binding Update.

5.3. Requests to Delete a Binding

If a node receives a valid Binding Update requesting it to delete a binding for a mobile node, as specified in Section 5.1, then the node MUST examine the Home Registration (H) bit in the Binding Update to determine how to further process the Binding Update. If the Home Registration (H) bit is set, the Binding Update is processed according to the procedure specified in Section 7.2.

If the Home Registration (H) bit is not set, and if a node receives a valid Binding Update requesting it to delete a binding for a mobile node, as specified in Section 5.1, then it MUST delete any existing entry in its Binding Cache for this mobile node's Home Address.

5.4. Sending Binding Acknowledgements

When any node receives a packet containing a Binding Update option, it SHOULD return a Binding Acknowledgement message acknowledging receipt of the Binding Update. If the node accepts the Binding Update and adds the binding contained in it to its Binding Cache, the Code field in the Binding Acknowledgement MUST be set to a value less than 128; if the node rejects the Binding Update and does not add the binding contained in it to its Binding Cache, the Code field in the Binding Acknowledgement MUST be set to a value greater than or equal to 128. Specific values for the Code field are described in Section 3.2 and in the most recent "Assigned Numbers" [10].

The Destination Address in the IPv6 header for the Binding Acknowledgement MUST be set to the Care-of Address copied from the Binding Update option. This 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.

5.5. Cache Replacement Policy

Any entry in a node's Binding Cache MUST be deleted after the expiration the Lifetime specified in the Binding Update from which the entry was created. Conceptually, a node MUST maintain a separate timer for each entry in its Binding Cache. When creating or updating a Binding Cache entry in response to a received 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 MUST delete 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 7.1) SHOULD 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 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 message to the sending mobile node, in which the Code 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 the 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 is likely to work well.

If a packet is sent by a node to a destination for which it has dropped the cache entry from its Binding Cache, the packet will be routed normally, leading to the mobile node's home network, where it 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 will result in the mobile node sending a Binding Update to this sending node, allowing it to add this entry again to its Binding Cache.

5.6. 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 mobile node's address (its home address), then the correspondent node uses a Routing header to deliver the packet to the mobile node's care-of address, and then to the mobile node's home address. 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 network, where it will be intercepted by the mobile node's home agent, encapsulated, and tunneled to the mobile node's care-of address. Similarly, 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). Any ICMP error message caused by the packet on its way to the mobile node while in the tunnel, will be returned to the node that encapsulated the packet (the home agent or the previous default router, respectively). By the definition of IPv6 encapsulation [5], however, this encapsulating node MUST relay certain ICMP error messages back to the original sender of the packet (the correspondent node).

Thus, whether the correspondent node has a Binding Cache entry for the destination mobile node or not, the correspondent node will receive any meaningful ICMP error message that is caused by its packet on its way to the mobile node. If the correspondent node receives an ICMP Host Unreachable or Network Unreachable error message after sending a packet to a mobile node using its cached care-of address, the correspondent node SHOULD delete its Binding Cache entry for this mobile node. If the correspondent node subsequently transmits another packet to the mobile node, the packet will be routed to the mobile node's home network, intercepted by the mobile node's home agent, and tunneled to the mobile node's 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.

6. Mobile Node Considerations

6.1. Movement Detection

A mobile node MAY use any combination of mechanisms available to it to detect when its link-level point of attachment has moved from one IPv6 subnet 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 [9].

Mobile nodes SHOULD use Router Discovery to discover new routers and on-link network prefixes; a mobile node MAY send Router Solicitation messages, or MAY wait for unsolicited (periodic) Router Advertisement messages, as specified for Router Discovery [9]. 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 network prefix, that it currently considers to be on-link. Each entry in these lists has an associated invalidation timer value (extracted from the 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 network prefix advertised by that router from its Prefix List to use as the network prefix in its primary care-of address. A mobile node MAY also have associated additional care-of addresses, using other network prefixes from its Prefix List. The method by which a mobile node selects and forms a care-of address from the available network prefixes is described in Section 6.2. The mobile node registers its primary care-of address with its home agent, as described in Section 6.3.

While away from home and using some router as its default router, it is important for a 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 its default router, so that any correspondent nodes attempting to communicate with the mobile node can still reach it.

To detect when its default router becomes unreachable, a mobile node SHOULD use Neighbor Unreachability Detection. As specified in Neighbor Discovery [9], while the mobile node is actively

sending packets to (or through) its default router, the mobile node can detect that the router has become unreachable either through indications from upper layer protocols on the mobile node that a connection is not making "forward progress" (e.g., TCP timing out waiting for an acknowledgement after a number of retransmissions), or through the failure to receive a Neighbor Advertisement messages form its default router in response to retransmitted explicit Neighbor Solicitation messages to it. No exceptions to Neighbor Unreachability Detection are necessary for this aspect of movement detection in Mobile IPv6.

For a mobile node to detect when it has become unreachable to its default router, however, 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 IPv6 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 multicast Router Advertisement messages, the mobile node will have frequent opportunity to check if it is still reachable to its default router, even in the absence of other packets to it from the router. On some types of network interfaces, the mobile node MAY also supplement this by setting its network interface into "promiscuous" receive mode, so that is able to receive all packets on the link, including those not link-level addressed to it. 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 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 form the router for a period of time), then the mobile node SHOULD 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 Unreachability Detection 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's link-layer connection to a new IPv6 subnet, such that the mobile node would need to switch to a new default router and primary care-of address. Upon lower-layer indication of link-layer mobility, the mobile node SHOULD send Router Solicitation messages to determine if new routers (and new on-link network 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 network prefixes currently available through different default 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 default routers to decide when to switch to a new primary care-of address using that default 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.

6.2. Forming New Care-of Addresses

After detecting that its link-layer point of attachment has moved from one IPv6 subnet 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 network 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 (more often than once per MAX_UPDATE_RATE seconds).

In addition, after discovering a new on-link network prefix, a mobile node MAY form a new (non-primary) care-of address using that network 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 (registered with its home agent), but it MAY have an additional care-of address for each network prefix 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. For more information on using more than one care-of address at a time, see Section 6.8.

As described in Section 2, in order to form a new care-of address, a mobile node MAY use either stateless [12] or stateful (e.g., DHCPv6 [3]) 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 some cases, a mobile node may already know a (constant) IPv6 address that has been assigned to it for its use while visiting this network. For example, it may be statically configured with an IPv6 address assigned by the system administrator of the new network. If so, rather than using address autoconfiguration to form a new care-of address using this network prefix, the mobile node SHOULD use its own pre-assigned address as its care-of address on this network.

6.3. Sending Binding Updates to the Home Agent

After changing its primary care-of address as described in Sections 6.1 and 6.2, a mobile node SHOULD register its new primary care-of address with its home agent. To do so, the mobile node sends a packet to its home agent containing a Binding Update option with the Acknowledge (A) bit set, requesting the home agent to return a Binding Acknowledgement message in response to this Binding Update. As described in Section 3.2, the mobile node SHOULD retransmit this Binding Update to its home agent until it receives a matching Binding Acknowledgement message. 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.

It is useful for a mobile node to be able to send a Binding Update its home agent without explicitly knowing the home agent's address. For example, since the mobile node was last at home, it may have become necessary to replace the node serving as its home agent due to the failure of the original node or due to reconfiguration of the home network. It thus may not always be possible or convenient for a mobile node to know the exact address of its own home agent.

Mobile nodes can dynamically discover the address of a home agent by sending a Binding Update to the anycast address on their home network. Each router on the home network which receives this Binding Update MUST reject the Binding Update and include its address in the Binding Acknowledgement message indicating the rejection. The mobile node is assumed to know a proper anycast address on its home network

before making use of this method for determining a particular home agent's address.

6.4. Sending Binding Updates to Correspondent Nodes

A mobile node MAY also include a Binding Update in any normal data packet sent to a correspondent node. For each correspondent node to which it has sent a Binding Update, the mobile node MUST keep information to determine whether or not the correspondent node has been sent a fresh Binding Update since the last time the mobile node switched to a new primary care-of address. When a packet is to be sent to a correspondent node that has not been sent a fresh Binding Update, the mobile node SHOULD include the Binding Update within the packet. Thus, correspondent nodes are generally kept updated and can send almost all data packets directly to the mobile node using the mobile node's current binding. Such Binding Updates are not generally required to be acknowledged; however, if the mobile node wants to be sure, an acknowledgement can be requested, although in this case, 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 also send a Binding Update in any otherwise empty packet, whenever the mobile node wishes to update a correspondent node as to its current binding. This is normally done only if the mobile suspects that its home agent is not operational or is too far away, a correspondent node is not sending the traffic to the proper care-of address, or there is an immediate need for the correspondent node to obtain the binding. A mobile node can detect that a correspondent node is not sending packets to the proper care-of address because in that case the packets arrive at the mobile node's care-of address by encapsulation instead by inclusion in a routing header within the packet.

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 3.1. No other IPv6 nodes are authorized to send Binding Updates on behalf of a mobile node.

6.5. 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 SHOULD send a Binding

Update message to its previous default router, giving its new care-of address. If it sends such a Binding Update, the mobile node MUST set the Home Address field to its old primary care-of address (that it used while using this default router), and set the Care-of Address field to its new primary care-of address. Note that the previous router does not necessarily know the mobile node's home address as part of this sequence of events.

The mobile node's previous default router then, in effect, temporarily act as a home agent for the mobile node's old primary care-of address. If any subsequent packets arrive at this previous router for forwarding to the mobile node's old primary care-of address, the router SHOULD encapsulate each and tunnel it to the mobile node at its new primary care-of address. Moreover, the previous router should issue Neighbor Advertisement packets for the previous care-of address, so that on-link neighbors will send packets destined to the mobile node's old primary care-of address to the previous router for encapsulation and tunneling to its new care-of address.

6.6. Rate Limiting for Sending Binding Updates

A mobile node MUST NOT send Binding Update messages more often than once per MAX_UPDATE_RATE seconds to any correspondent node. After sending 5 consecutive Binding Updates to a particular correspondent node with the same care-of address, the mobile node SHOULD reduce its rate of sending Binding Updates to that correspondent node, to the rate of SLOW_UPDATE_RATE per second. The mobile node MAY continue to send Binding Updates at the slower rate indefinitely, in hopes that the correspondent node will finally be able to process a Binding Update and begin to route its packets directly to the mobile node at its current primary care-of address.

6.7. Receiving Binding Acknowledgements

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

- The packet contains an IP Authentication header and the authentication is valid [1]. The Authentication header is assumed to provide both authentication and integrity protection.

- The ICMP Checksum is valid.

- The length of the ICMP message (derived from the IPv6 Payload Length field) is greater than or equal to 16 octets.

- The Identification field is valid.

Any Binding Acknowledgement not satisfying all of these tests MUST be silently discarded.

If the Binding Acknowledgement is valid, the mobile node MUST examine the Code field as follows:

- If the Code field indicates that the Binding Update was accepted (the Code 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 SHOULD thus stop retransmitting the Binding Update.

- If the Code field indicates that the Binding Update was not accepted (the Code field is greater than or equal to 128), then the mobile node MUST delete the corresponding Binding Update List entry. Optionally, the mobile node MAY take steps to correct the cause of the error and retransmit the Binding Update, subject to the rate limiting restriction specified in Section 6.6.

6.8. Using Multiple Care-of Addresses

As described in Section 6.2, a mobile node MAY have more than one care-of address at a time. Particularly in the case of many wireless networks, a mobile node effectively may be reachable through multiple link-level points of attachment at the same time (e.g., with overlapping wireless cells), on which different on-link network 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 network prefixes, based on the movement detection mechanism in use (Section 6.1). When the mobile node selects a new primary care-of address, it MUST register it with its home agent through a Binding Update message with the Acknowledge (A) bit set, as described in Section 6.3.

To assist in smooth handoffs, a mobile node SHOULD retain its previous primary care-of address as a 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 [3], the mobile node may not wish

to release the address immediately upon switching to a new primary care-of address. The stateful address autoconfiguration server will allow mobile nodes to acquire new addresses while still using previously allocated addresses.

6.9. Returning Home

A mobile node detects that it has returned to its home network through the movement detection algorithm in use (Section 6.1), when the mobile node detects that its home network 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 field to its own IPv6 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 message is received.

The mobile node MUST also send out the appropriate Neighbor Advertisement packets with the Override flag set, so that its neighbors on its home network will update the relevant information for the mobile node in their Neighbor Caches. The mobile node MUST do this for both its link-local address and its home address. The Neighbor Advertisement packets can be repeated a small number of times to guard against occasional loss of packets on the home network.

7. Home Agent Considerations

7.1. Home Agent Care-of Address Registration

General processing of a received Binding Update that requests a binding to be cached, is described in Section 5.2. However, if the Home Registration (H) bit is set in the Binding Update, then the receiving node MUST process the Binding Update as specified in this section, rather than following the generall procedure specified in Section 5.2.

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 message to the mobile node, in which the Code field is set to 132 (Home registration not supported).

- Else, if the Home Address field in the Binding Update 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 message to the mobile node, in which the Code field is set to 133 (Not home network).

- 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 message to the mobile node, in which the Code 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 (or update the existing entry) in its Binding Cache for this mobile node's Home Address, as described in Section 5.2. In addition, 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" SHOULD be excluded from the normal cache replacement policy used for the Binding Cache (Section 5.5) and SHOULD NOT be removed from the Binding Cache until the expiration of the Lifetime period.

If the home agent was not already serving as a home agent for the Home Address specified in the Binding Update (the home agent did

not already have a Binding Cache entry for this address marked as a "home registration"), then the home agent MUST multicast onto the home network (to the all-nodes multicast address), a Neighbor Advertisement message on behalf of the mobile node, with the fields in the Neighbor Advertisement set as follows:

Router Flag (R)

1 -- the sending node (the home agent) is a router.

Solicited Flag (S)

0 -- the Neighbor Advertisement message is unsolicited.

Override Flag (O)

1 -- the advertisement SHOULD override any existing Neighbor Cache entry at the receiver, updating the receiver's cached link-layer address for this Target Address.

Target Address

The mobile node's home address, copied from the Home Address field of the Binding Update.

Options

The home agent MUST include at least a Target Link-layer Address option in the Neighbor Advertisement message, in which the Link-Layer Address gives the link-layer address of the home agent itself.

Any node on the home network receiving this Neighbor Advertisement message will thus update its Neighbor Cache to associate the mobile node's home address with the home agent's link layer address, causing it to transmit future packets for the mobile node 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 a small number of times to increase its reliability. It is still possible that some nodes on the home network 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 [9].

In addition, while this node is serving as a home agent to any mobile node (it has at least one entry marked as a "home registration" in its Binding Cache), it SHOULD act as a proxy for each such 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". If such an entry exists in its 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.

7.2. Home Agent Care-of Address De-registration

General processing of a received Binding Update that requests a binding to be deleted, is described in Section 5.3. However, if the Home Registration (H) bit is set in the Binding Update, then the receiving node MUST process the Binding Update as specified in this section, rather than following the generall procedure specified in Section 5.3.

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 message to the mobile node, in which the Code field is set to 132 (Home registration not supported).

- Else, if the Home Address field in the Binding Update is not an on-link IPv6 address with respect to the home agent's current Prefix List, then it MUST reject the Binding Update and SHOULD return a Binding Acknowledgement message to the mobile node, in which the Code field is set to 133 (Not home network).

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's Home Address, as specified in the Binding Update.

In addition, the home agent SHOULD multicast a Neighbor Advertisement message (to the all-nodes multicast address), giving the mobile node's home address as the Target Address, and specifying the mobile node's link-layer address in a Target Link-layer Address option in the Neighbor Advertisement message. The home agent MAY retransmit this Neighbor Advertisement message a small number of times to increase its reliability, and any nodes on the home network that miss all of these Neighbor Advertisements can also eventually detect the

link-layer address change for the mobile node's home address, through use of Neighbor Unreachability Detection [9].

7.3. Delivering Packets to a Mobile Node

Home agents cannot use Routing headers to deliver packets to the mobile node, because they can't modify the packet and add to it in flight. They must always use IPv6 encapsulation [5] for this purpose.

When a home agent encapsulates a packet for delivery to the mobile node, the home agent uses the care-of address as the destination address in the outer IPv6 header. Since the mobile node is presumed to be receiving packets at the care-of address, the delivery path from the care-of address to the mobile node's home address is then trivial.

Note that the home agent cannot insert a routing header, or modify the destination address of the mobile node, because of IPv6 authentication mechanisms [1]. The home agent is expected to be involved only rarely with the transmission of data to the mobile node, because the mobile node will send Binding Updates as soon as possible to its correspondent nodes.

7.4. Renumbering the Home Network

Neighbor Discovery [9] specifies a mechanism by which all nodes on a network can gracefully autoconfigure new addresses, say by combining a new routing prefix with their existing MAC address. As currently specified, this mechanism works when the nodes are on the same link as the router issuing the necessary multicast packets to advertise the new routing prefix(es) appropriate for the link.

However, for mobile nodes away from home, special care must be taken to allow the mobile nodes to renumber gracefully. The most direct method of insuring this is for the home agent to encapsulated and tunnel the multicast packets to the care-of address of the mobile node as necessary. The rules for this are as follows:

- A mobile node assumes that its routing prefix has not changes unless it receives authenticated router advertisement messages from its home agent that the prefix has changed.

- When the mobile node is at home, the home agent does not tunnel router advertisements to it.

- When a home network prefix changes, the home agent tunnels router advertisement packets to each mobile node which is currently away from home and using a home address with the affected routing prefix. Such tunneled router advertisements MUST be authenticated [1].

- When a mobile node receives a tunneled router advertisement containing a new routing prefix, it must perform the standard autoconfiguration operation to create its new address

- When a mobile node returns to its home network, it must again perform Duplicate Address Detection at the earliest possible moment after it has registered with its home agent.

- A mobile node may send a router solicitation to its home agent at any time, within the constraints imposed by rate control in the Neighbor Discovery specification [9]

Note that a mobile node is guaranteed that its home address is unique and used by no other mobile node. However, in some circumstances it may nevertheless be true that other nodes on its home network form the same link-local address as the mobile node during the time when the mobile node is away from its home network. Thus, there is the requirement above that the mobile node perform Duplicate Address Detection when it returns again to its home network.

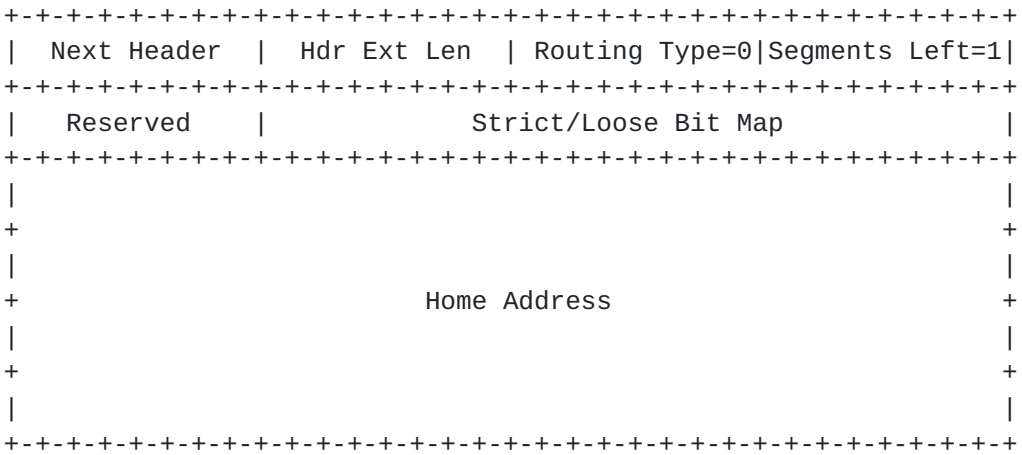
8. Correspondent Node Considerations

8.1. Delivering Packets to a Mobile Node

The routing infrastructure of the Internet will normally route a packet destined to a mobile node to the mobile node's home network, if the Destination Address in the packet's IPv6 header is the mobile node's home address. Once the packet reaches the home network, it will be intercepted by the mobile node's home agent if the mobile node is away from home, and will then be encapsulated using IPv6 encapsulation and tunneled to the mobile node's current primary care-of address. Using this delivery mechanism, the sender need not know that the node is mobile.

Correspondent nodes that have received and cached a Binding Update for a mobile node, MAY instead route packets directly to that mobile node's care-of address. To do so, the correspondent node includes a Routing header in each packet to the mobile node, to cause the packet to be routed to the mobile node's care-of address as the last intermediate routing point before reaching the final destination of the mobile node's home address. When the packet arrives at the care-of address (which the mobile node has associated with its network interface), normal processing of the Routing header by the mobile node will result in delivery of the packet to the mobile node as the final destination of the packet.

For example, assuming no other use of the Routing header in the packet, the sender initializes the Destination Address in the IPv6 header to the mobile node's care-of address, and includes a Type 0 Routing header [6] in the packet initialized as follows:



Next Header

8-bit selector. Identifies the type of header immediately following the Routing header.

Hdr Ext Len

8-bit unsigned integer. Length of the Routing header in 8-octet units, not including the first 8 octets. For this use of the Type 0 Routing header, Hdr Ext Len is equal to 2.

Routing Type

0

Segments Left

8-bit unsigned integer. Number of route segments remaining before reaching the final destination. For this use of the Type 0 Routing header, Segments Left is initialized to 1 by the sender.

Reserved

8-bit reserved field. Initialized to zero for transmission; ignored on reception.

Strict/Loose Bit Map

24-bit bit-map, numbered 0 to 23, left-to-right. For this use of the Type 0 Routing header, bit 0 of the Strict/Loose Bit Map is set to 1, indicating strict routing from the care-of address to the mobile node's home address (both addresses are associated with the mobile node itself).

Home Address

The home address of the destination mobile node.

If a correspondent node receives an ICMP Host Unreachable or Network Unreachable message after sending a packet to a mobile node using its cached care-of address, it SHOULD delete the cache entry from its Binding Cache until information about the mobile node's current care-of address becomes available (via a Binding Update).

9. Authentication and Replay Protection

When sending Binding Updates, a mobile node uses the Identification field in the option, in conjunction with the IPv6 Authentication Header, to protect against replays of the Binding Update. The style of replay protection specified for the IPv6 Binding Update involves the use of a timestamp as the Identification data. Accordingly the mobile node and the target of its Binding Update have to roughly agree on the current time. Stale Binding Updates MUST be rejected.

10. Routing Multicast Packets

A mobile node that is connected to its home network functions just like 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 network.

In order receive multicasts, a mobile node must join the multicast group. Mobile nodes MAY join multicast groups in order to receive transmissions in one of two ways. First, they MAY join the group via a (local) multicast router on the visited subnet. This option assumes that there is a multicast router present on the visited subnet. The mobile node SHOULD use its dynamically acquired care-of address (if it has acquired one) as the source IPv6 address of its multicast group membership control message packets. Otherwise, it MAY use its home address.

Alternatively, a mobile node which wishes to receive multicasts can join groups via a bi-directional tunnel to its home agent, assuming that its home agent is a multicast router. The mobile node tunnels the appropriate multicast group membership control packets to its home agent and the home agent forwards multicast packets down the tunnel to the mobile node. The home agent must tunnel the packet directly to the mobile node's dynamically acquired care-of address, or, the packet must be tunneled first to the mobile node's home address and then recursively tunneled to the mobile node's care-of address.

A mobile node which wishes to send packets to a multicast group also has two options: (1) send directly on the visited network; or (2) send via a tunnel to its home agent. Because multicast routing in general depends upon the IPv6 source address, a mobile node which sends multicast packets directly on the visited network MUST use a dynamically acquired care-of address as the IPv6 source address. Similarly, a mobile node which tunnels a multicast packet to its home agent MUST use its home address as the IPv6 source address of both the (inner) multicast packet and the (outer) encapsulating packet. This second option assumes that the home agent is a multicast router.

11. Constants

INITIAL_BINDACK_TIMEOUT	1 second
MAX_BINDACK_TIMEOUT	256 seconds
MAX_UPDATE_RATE	1 per second
SLOW_UPDATE_RATE	once per 10 seconds

Acknowledgements

We would like to thank Thomas Narten for contributing valuable discussion and reviewing this draft, and for helping to shape some of the recent changes relevant to the operation of Neighbor Discovery.

References

[1] R. Atkinson. IP Authentication Header. RFC 1826, August 1995.

[2] R. Atkinson. Security Architecture for the Internet Protocol. RFC 1825, August 1995.

[3] J. Bound and C. Perkins. Dynamic Host Configuration Protocol for IPv6. draft-ietf-dhc-dhcpv6-05.txt -- work in progress, June 1996.

[4] A. Conta and S. Deering. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6). RFC 1885, December 1995.

[5] A. Conta and S. Deering. Generic Packet Tunneling in IPv6. draft-ietf-ipngwg-ipv6-tunnel-01.txt - work in progress, February 1996.

[6] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 1883, December 1995.

[7] D. Haskin and E. Allen. IP Version 6 over PPP. draft-ietf-ipngwg-pppext-ipv6cp-03.txt - work in progress, June 1996.

[8] David B. Johnson and Charles E. Perkins. Route Optimization in Mobile-IP. draft-ietf-mobileip-optim-04.txt -- work in progress, February 1996.

[9] T. Narten, E. Nordmark, and W. Simpson. IPv6 Neighbor Discovery. draft-ietf-ipngwg-discovery-03.txt -- work in progress, November 1995.

[10] Joyce K. Reynolds and Jon Postel. Assigned Numbers. RFC 1700, October 1994.

[11] Fumio Teraoka. draft-teraoka-ipv6-mobility-sup-02.txt. Internet Draft -- work in progress, January 1996.

[12] S. Thomson and T. Narten. IPv6 Stateless Address Autoconfiguration. draft-ietf-addrconf-ipv6-auto-06.txt - work in progress, November 1995.

A. Open Issues

A.1. Session Keys with Local Routers

In the IPv4 route optimization proposal [8], a mechanism is outlined whereby a session key can be established between foreign agents and mobile nodes, without requiring any pre-established security relationship between them. A similar mechanism could be defined for IPv6, to avoid the need for a possibly time-consuming negotiation between routers and mobile nodes for the purpose of obtaining the session key, which under many circumstances would only be used once. This mechanism, if needed, can be specified completely outside the Mobile IPv6 protocol and would amount to a way of creating a dynamic security association between two nodes which do not share an existing trust relationship, but which need to agree on a key for some particular purpose (here, allowing the future authentication of a Binding Update). Hopefully, the work of the IP Security Working Group will allow this function to be performed appropriately for mobile nodes, say by a Diffie-Hellman key exchange.

A.2. Source Address Filtering by Firewalls

The current specification does nothing to permit mobile nodes to send their packets through firewalls which filter out packets with the "wrong" source IPv6 addresses in the IPv6 packet header. The mobile node's home address may be unlikely to fall within the ranges required to satisfy the firewall's criteria for further delivery.

As indicated by recent discussion, firewalls are unlikely to disappear. Any standardized solution [11] to the firewall problem based on hiding the non-local source address outside the source address field of the IPv6 header is likely to fail. Any vendor or facilities administrator wanting to filter based on the address in the IPv6 source address field would also quickly begin filtering on hidden source addresses.

Assume, for the moment, that a mobile node is able to establish a secure tunnel through a firewall protecting the domain in which a correspondent node is located. The mobile node could then encapsulate its packet so that the outer IPv6 header was addressed to the firewall and used the mobile node's care-of address as the source address. When the firewall decapsulates, it would be able to authenticate the inner packet based (correctly) on the mobile node's home address. After the authentication is performed, the firewall could forward the packet to the correspondent node as desired. This simple procedure has the feature that it requires the minimal amount of encapsulation, no assistance by routers or other agents, and that

the firewall can establish a security relationship with the mobile node based on its home (i.e., permanent) address.

Chair's Address

The Working Group can be contacted via its current chair:

Jim Solomon
Motorola, Inc.
1301 E. Algonquin Rd.
Schaumburg, IL 60196

Work: +1-847-576-2753
E-mail: solomon@comm.mot.com

Authors' Addresses

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

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

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

Charles Perkins
Room H3-D34
T. J. Watson Research Center
IBM Corporation
30 Saw Mill River Rd.
Hawthorne, NY 10532

Work: +1 914 789-7350
Fax: +1 914 784-6205
E-mail: perk@watson.ibm.com