Route Optimization in Mobile IP

draft-ietf-mobileip-optim-04.txt

Status of This Memo

This document is a product of the Mobile IP Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to working group mailing list at mobile-ip@tadpole.com.

Distribution of this document 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 "iid-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).
Abstract

This document defines extensions to the operation of the base Mobile IP protocol to allow for optimization of datagram routing from a correspondent node to a mobile node. Without Route Optimization, all datagrams destined to a mobile node are routed through that mobile node’s home agent, which then tunnels each datagram to the mobile node’s current location. The protocol extensions described here provide a means for correspondent nodes that implement them to cache the binding of a mobile node and to then tunnel their own datagrams for the mobile node directly to that location, bypassing the possibly lengthy route for each datagram to and from the mobile node’s home agent. Extensions are also provided to allow datagrams in flight when a mobile node moves, and datagrams sent based on an out-of-date cached binding, to be forwarded directly to the mobile node’s new binding.
9. Home Agent Considerations 36
   9.1. Rate Limiting 36
   9.2. Receiving Binding Warning Messages 36
   9.3. Receiving Binding Request Messages 37
   9.4. Receiving Registration Key Requests 37
   9.5. Receiving Special Tunnels 38

10. Foreign Agent Considerations 39
   10.1. Establishing a Registration Key 39
   10.2. Previous Foreign Agent Notification 40
   10.3. Receiving Tunneled Datagrams 41
   10.4. Rate Limiting 42
   10.5. Sending Special Tunnels 42

11. Mobile Node Considerations 43
   11.1. Establishing a Registration Key 43
   11.2. Notifying Previous Foreign Agents 43

References 45

Appendix A. Using a Master Key at the Home Agent 46

Chairs’ Addresses 47

Authors’ Addresses 48
1. Introduction

The base Mobile IP protocol [6] allows any mobile node to move about, changing its point of attachment to the Internet, while continuing to be addressed by its home IP address. Correspondent nodes sending IP datagrams to a mobile node address them to the mobile node’s home address in the same way as to any destination.

While the mobile node is connected to the Internet away from its home network, it is served by a "home agent" on its home network and is associated with a "care-of address" indicating its current location. The association between a mobile node’s home address and its care-of address is known as a "mobility binding". The care-of address is generally the address of a "foreign agent" on the network being visited by the mobile node, which forwards arriving datagrams locally to the mobile node. Alternatively, the care-of address may be temporarily assigned to the mobile node using DHCP [3] or other means. All IP datagrams addressed to the mobile node are routed by the normal IP routing mechanisms to the mobile node’s home network, where they are intercepted by the mobile node’s home agent, which then tunnels each datagram to the mobile node’s current care-of address. Datagrams sent by a mobile node use the foreign agent as a default router but require no other special handling or routing.

This scheme allows transparent interoperation with mobile nodes, but forces all datagrams for a mobile node to be routed through its home agent; datagrams to the mobile node are often routed along paths that are significantly longer than optimal. For example, if a mobile node, say MN1, is visiting some subnet, even datagrams from a correspondent node on this same subnet must be routed through the Internet to MN1’s home agent on MN1’s home network, only to then be tunneled back to the original subnet to MN1’s foreign agent for delivery to MN1. This indirect routing can significantly delay the delivery of the datagram to MN1 and places an unnecessary burden on the networks and routers along this path through the Internet. If the correspondent node in this example is actually another mobile node, say MN2, then datagrams from MN1 to MN2 must likewise be routed through MN2’s home agent on MN2’s home network and back to the original subnet for delivery to MN1.

This document defines extensions to the base Mobile IP protocol to allow for the optimization of datagram routing from a correspondent node to a mobile node. These extensions provide a means for nodes that implement them to cache the binding of a mobile node and to then tunnel their own datagrams directly to the care-of address indicated in that binding, bypassing the possibly lengthy route to and from that mobile node’s home agent. Extensions are also provided to allow datagrams in flight when a mobile node moves, and datagrams sent
based on an out-of-date cached binding, to be forwarded directly
to the mobile node’s new care-of address. These extensions are
collectively referred to as Route Optimization in this document.

All operation of Route Optimization that changes the routing of IP
datagrams to the mobile node is authenticated using the same type of
authentication mechanism used in the base Mobile IP protocol. This
authentication generally relies on a "mobility security association"
established in advance between the node sending a message and the
node receiving the message that must authenticate it. When the
required mobility security association has not been established, a
Mobile IP implementation using Route Optimization operates in the
same way as the base Mobile IP protocol.

Section 3 of this document provides an overview of the operation of
Route Optimization. Section 4 defines the message types used by
Route Optimization, and Section 5 defines the message extensions
used. Section 6 discusses the problem of managing the mobility
security associations needed to provide authentication of all
messages that affect the routing of datagrams to a mobile node.
The final four sections of this document define in detail the
operation of Route Optimization from the point of view of each of the
entities involved: considerations for nodes maintaining a binding
cache are presented in Section 8, mobile node considerations in
Section 11, foreign agent considerations in Section 10, and home
agent considerations in Section 9.
2. Terminology

This document introduces the following terminology, in addition to that used in the base Mobile IP protocol:

**Binding cache**

A cache of mobility bindings of mobile nodes, maintained by a node for use in tunneling datagrams to those mobile nodes. Presence of a binding cache entry is not required for correct operation of the Mobile IP protocol. Entries in the binding cache are dynamically created and MAY be deleted by the node at any time, such as to reclaim space in the cache.

**Binding update**

A notification to some node of a mobile node’s current mobility binding. A binding update is sent using a Binding Update message. All Binding Update messages MUST carry an authentication extension, similar to the authentication required in all registration messages in the base Mobile IP protocol.

**Registration key**

A secret key shared between a mobile node and a foreign agent, that MAY optionally be established during registration with that foreign agent. When later moving and registering a new care-of address elsewhere, the mobile node MAY use the registration key it shares with its previous foreign agent, to send an authenticated binding update to this foreign agent.

**Special tunnel**

A method of tunneling a datagram in which the "outer" destination address when encapsulating the datagram is set equal to the "inner" destination address (the original destination address of the datagram). Any router forwarding such a tunneled datagram MUST NOT re-tunnel the datagram even if it has a binding cache entry for the destination address. A special tunnel is used in Route Optimization for delivering a datagram, addressed to a mobile node, to the mobile node’s home agent while the mobile node is away from home, without knowing the home agent’s address. The "outer" source address allows the home agent to know the tunneling node’s address when it intercepts the datagram on the home network.
3. Route Optimization Overview

3.1. Binding Caching

Route Optimization provides a means for any node that wishes to optimize its own communication with mobile nodes to maintain a "binding cache" containing the mobility binding of one or more mobile nodes. When sending an IP datagram to a mobile node, if the sender has a binding cache entry for the destination mobile node, it may tunnel the datagram directly to the care-of address indicated in the cached mobility binding.

In the absence of any binding cache entry, datagrams destined for a mobile node will be routed to the mobile node’s home network in the same way as any other IP datagram, and are then tunneled to the mobile node’s current care-of address by the mobile node’s home agent. This is the only routing mechanism supported by the base Mobile IP protocol. With Route Optimization, as a side effect of this indirect routing of a datagram to a mobile node, the original sender of the datagram may be informed of the mobile node’s current mobility binding, giving the sender an opportunity to cache the binding.

A node may create a binding cache entry for a mobile node only when it has received and authenticated the mobile node’s mobility binding. Likewise, a node may update an existing binding cache entry for a mobile node, such as after the mobile node has moved to a new foreign agent, only when it has received and authenticated the mobile node’s new mobility binding.

A binding cache will, by necessity, have a finite size. Any node implementing a binding cache may manage the space in its cache using any local cache replacement policy. If a datagram is sent by a node to a destination for which it has dropped the cache entry from its binding cache, the datagram 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 care-of address. As when a binding cache entry is initially created, this indirect routing to the mobile node will result in the original sender of the datagram being informed of the mobile node’s current mobility binding, allowing it to add this entry again to its binding cache.

3.2. Foreign Agent Handoff

When a mobile node moves and registers with a new foreign agent, the base Mobile IP protocol does not notify the mobile node’s previous
foreign agent. IP datagrams intercepted by the home agent after the new registration are tunneled to the mobile node’s new care-of address, but datagrams in flight that had already been intercepted by the home agent and tunneled to the old care-of address when the mobile node moved are lost and are assumed to be retransmitted by higher-level protocols if needed. The old foreign agent eventually deletes the mobile node’s registration after the expiration of the lifetime period established when the mobile node registered there.

Route Optimization provides a means for the mobile node’s previous foreign agent to be reliably notified of the mobile node’s new mobility binding, allowing datagrams in flight to the mobile node’s previous foreign agent to be forwarded to its new care-of address. This notification also allows any datagrams tunneled to the mobile node’s previous foreign agent from correspondent nodes with out-of-date binding cache entries for the mobile node (that have not yet learned that the mobile node has moved), to be forwarded to its new care-of address. Finally, this notification allows any resources consumed by the mobile node’s binding at the previous foreign agent (such as radio channel reservations) to be released immediately, rather than waiting for the mobile node’s registration to expire.

Optionally, during registration with a new foreign agent, the mobile node and the foreign agent may establish a new shared secret key as a "registration key". When the mobile node later registers with a new foreign agent, if it established a registration key during registration with its previous foreign agent, it may use this key to notify the previous foreign agent that it has moved. This notification may also optionally include the mobile node’s new care-of address, allowing the previous foreign agent to create a binding cache entry for the mobile node to serve as a "forwarding pointer" to its new location. Any tunneled datagrams for the mobile node that arrive at this previous foreign agent after this binding cache entry has been created will then be re-tunneled by this foreign agent to the mobile node’s new location using the mobility binding in this binding cache entry. The registration key is used to authenticate the notification sent to the previous foreign agent. Other uses of the registration key are possible, such as for use as an encryption key for providing privacy over a wireless link between the mobile node and its foreign agent, but such uses are beyond the scope of this document. Once established, the registration key for a mobile node can be stored by the foreign agent with the mobile node’s visitor list entry.

In this document, we suggest four methods that a mobile node could use for dynamically establishing a registration key with a foreign agent when it registers with that foreign agent:

---

Johnson and Perkins
Expires 22 August 1996

[Page 5]
- The home agent chooses the new registration key, and returns a separate encrypted copy of the key to the foreign agent and to the mobile node in its Registration Reply message. For this method, the home agent must share a mobility security association with the foreign agent in addition to its required mobility security association with the mobile node.

- The mobile node and its foreign agent execute a Diffie-Hellman key exchange protocol [2] as part of the registration protocol.

- The mobile node includes its public key (such as RSA) in its Registration Request to the foreign agent, and the foreign agent chooses the new registration key and returns a copy of it encrypted with the mobile node’s public key.

- The foreign agent includes an MD5 digest of its public key (such as RSA) in its Agent Advertisement messages. The mobile node includes a copy of this digest in its Registration Request, and the foreign agent adds its full public key to the Registration Request when relaying it to the home agent. The home agent then chooses the new registration key and returns a separate encrypted copy of the key to the foreign agent (using this public key) and to the mobile node (using its mobility security association with the mobile node) in its Registration Reply message.

Section 7 discusses these methods of establishing a registration key in detail.

As part of the registration procedure, the mobile node may request that its new foreign agent attempt to notify its previous foreign agent on its behalf, by including a Previous Foreign Agent Notification extension in its Registration Request message sent to the new foreign agent. The new foreign agent then builds a Binding Update message and transmits it to the mobile node’s previous foreign agent as part of registration, requesting an acknowledgement from the previous foreign agent. The Previous Foreign Agent Notification extension includes only those values needed to construct the Binding Update message that are not already contained in the Registration Request message. The authenticator for the Binding Update message is computed by the mobile node based on its registration key shared with its previous foreign agent.

The mobile node is responsible for occasionally retransmitting a Binding Update message to its previous foreign agent until the matching Binding Acknowledge message is received, or until the mobile node can be sure of the expiration of its registration with that foreign agent.
The binding cache entry created at the mobile node’s previous foreign agent is treated in the same way as any other binding cache entry. In particular, it is possible that this binding cache entry will be deleted from the cache at any time. In this case, the foreign agent will be unable to re-tunnel subsequently arriving tunneled datagrams for the mobile node, directly to the mobile node’s new location.

3.3. Binding Cache Updates

When a mobile node’s home agent intercepts a datagram from the home network and tunnels it to the mobile node, the home agent may deduce that the original source of the datagram has no binding cache entry for the destination mobile node. In this case, the home agent MAY send a Binding Update message to the original source node, informing it of the mobile node’s current mobility binding. No acknowledgement for this Binding Update message is needed, since additional future datagrams from this source node intercepted by the home agent for the mobile node will cause transmission of another Binding Update. In order for this Binding Update to be authenticated by the original source node, the home agent and this source node must have established a mobility security association.

Similarly, when any node receives a tunneled datagram that was tunneled to this node, if it has a binding cache entry for the destination mobile node (and thus has no visitor list entry for this mobile node), the node receiving this tunneled datagram may deduce that the tunneling node has an out-of-date binding cache entry for this mobile node. In this case, the receiving node MAY send a Binding Warning message to the mobile node’s home agent, advising it to send a Binding Update message to the node that tunneled this datagram. The mobile node’s home agent can be determined from the binding cache entry (the home agent address is learned from the Binding Update that established this cache entry), and the address of the node that tunneled this datagram can be determined from the datagram’s header (the address of the node tunneling this datagram is the "outer" source address of the encapsulated datagram). As in the case of a Binding Update sent by the mobile node’s home agent, no acknowledgement of this Binding Warning is needed, since additional future datagrams for the mobile node tunneled by the same node will cause the transmission of another Binding Warning. However, unlike the Binding Update message, no authentication of the Binding Warning message is necessary, since it does not directly affect the routing of IP datagrams to the mobile node.

Finally, suppose a node receives a datagram that has been tunneled to this node, but this node is unable to deliver the datagram locally to the destination mobile node (the node is not the mobile node
itself, and it is not a foreign agent with a visitor list entry for the mobile node), and this node has no binding cache entry for the destination mobile node. To attempt delivery of the datagram in this case, the node must encapsulate the datagram as a "special tunnel" datagram (Section 10.5), destined to the mobile node. This use of a "special tunnel" avoids a possible routing loop in the case in which the case-of address registered at the home agent is the address of this node, but this node has forgotten that it is serving as the mobile node’s foreign agent, perhaps because the node has crashed and lost its visitor list state. The "special tunnel" allows the home agent to see the address of the node that tunneled the datagram, and to avoid tunneling the datagram back to the same node.

Each Binding Update message indicates the maximum lifetime of any binding cache entry created from the Binding Update. When sending the Binding Update message, the home agent SHOULD set this lifetime to the remaining service lifetime associated with the mobile node’s current registration. Any binding cache entry established or updated in response to this Binding Update message must be marked to be deleted after the expiration of this period. A node wanting to provide continued service with a particular binding cache entry may attempt to reconfirm that mobility binding before the expiration of this lifetime period. Such reconfirmation of a binding cache entry may be appropriate when the node has indications (such as an open transport-level connection to the mobile node) that the binding cache entry is still needed. This reconfirmation is performed by the node sending a Binding Request message to the mobile node’s home agent, requesting it to reply with the mobile node’s current mobility binding in a new Binding Update message.
4. Route Optimization Message Formats

Route Optimization defines four message types used for management of binding cache entries. Each of these messages begins with a one-octet field indicating the type of the message.

The following Type codes are defined in this document:

16 = Binding Warning message  
17 = Binding Request message  
18 = Binding Update message  
19 = Binding Acknowledge message

Route Optimization also requires one minor change to existing Mobile IP messages: a new flag bit must be added to the Registration Request message, replacing a previously unused, reserved bit in the message.

This section describes each of the new Route Optimization messages and the change to Registration Request message.
4.1. Binding Warning Message

A Binding Warning message is used to advise a mobile node’s home agent that another node appears to have either no binding cache entry or an out-of-date binding cache entry for some mobile node. When any node receives a datagram tunneled to itself, if it is not the current foreign agent for the destination mobile node, it MAY send a Binding Warning message to the mobile node’s home agent.

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>++++++---------------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>++++++---------------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>++++++---------------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Type

16

Reserved

Sent as 0; ignored on reception.

Mobile Node Home Address

The home address of the mobile node to which the Binding Warning message refers.

Target Node Address

The address of the node tunneling the datagram that caused the Binding Warning message. This node should be the target of the Binding Update message sent by the home agent.
4.2. Binding Request Message

A Binding Request message is used by a node to request a mobile node’s current mobility binding from the mobile node’s home agent.

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| +--------------------------------------------------+
| | Type | Reserved |
| +--------------------------------------------------+
| | +--------------------------------------------------+
| | Mobile Node Home Address |
| +--------------------------------------------------+
| +--------------------------------------------------+
| | Identification |
| +--------------------------------------------------+
| +--------------------------------------------------+

Type

17

Reserved

Sent as 0; ignored on reception.

Mobile Node Home Address

The home address of the mobile node to which the Binding Request refers.

Identification

A 64-bit sequence number, assigned by the node sending the Binding Request message, used to assist in matching requests with replies, and in protecting against replay attacks.
4.3. Binding Update Message

The Binding Update message is used to notify another node of a mobile node’s current mobility binding. It MAY be sent by the mobile node’s home agent in response to a Binding Request message or a Binding Warning message. It MAY also be sent by a mobile node, or by the foreign agent with which the mobile node is registering, when notifying the mobile node’s previous foreign agent that the mobile node has moved.

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |A|I|M|G|  Rsvd |            Lifetime           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Mobile Node Home Address                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Care-of Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Identification                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Extensions ...                                                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

18

Acknowledge (A)

The Acknowledge (A) bit is set by the node sending the Binding Update message to request a Binding Acknowledge message be returned acknowledging its receipt.

Identification Present (I)

The Identification Present (I) bit is set by the node sending the Binding Update message to indicate that the Identification field is present in the message.

Minimal Encapsulation (M)

If the Minimal Encapsulation (M) bit is set, datagrams may be tunneled to the mobile node using the minimal encapsulation protocol used in the base Mobile IP protocol.
GRE Encapsulation (G)

If the GRE Encapsulation (G) bit is set, datagrams may be tunneled to the mobile node using the GRE encapsulation protocol [5].

Reserved (Rsvd)

Sent as 0; ignored on reception.

Lifetime

The number of seconds remaining before the binding cache entry must be considered expired. A value of all ones indicates infinity. A value of zero indicates that no binding cache entry for the mobile node should be created and that any existing binding cache entry (and visitor list entry, in the case of a mobile node’s previous foreign agent) for the mobile node should be deleted. The lifetime is typically equal to the remaining lifetime of the mobile node’s registration.

Mobile Node Home Address

The home address of the mobile node to which the Binding Update message refers.

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 message instead indicates that no binding cache entry for the mobile node should be created, and any existing binding cache entry (and visitor list entry, in the case of a mobile node’s previous foreign agent) for the mobile node should be deleted.

Identification

If present, a 64-bit number, assigned by the node sending the Binding Request message, used to assist in matching requests with replies, and in protecting against replay attacks.

The Route Optimization Authentication extension (Section 5.2) is required.
4.4. Binding Acknowledge Message

A Binding Acknowledge message is used to acknowledge receipt of a Binding Update message. It SHOULD be sent by a node receiving the Binding Update message if the Acknowledge (A) bit is set in the Binding Update message.

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>N</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>Mobile Node Home Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identification +</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reserved</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Type 19**

Negative Acknowledge (N)

If the Negative Acknowledge (N) bit is set, this acknowledgement is negative. For instance, if the binding update was not accepted, but the incoming datagram has the Acknowledge flag set, then the Negative Acknowledge (N) bit SHOULD be set in this Binding Acknowledge message.

DISCUSSION: Alternatively, we could replace this bit with a status code, as in the Registration Reply message. The mobile node could log the error, but currently has no real way to recover from it, so perhaps the exact reason for the error isn’t that useful.

Reserved

Sent as 0; ignored on reception.

Mobile Node Home Address

Copied from the Binding Update message being acknowledged.
Identification

Copied from the Binding Update message being acknowledged, if present there.
4.5. Registration Request Message

One bit is added to the flag bits in the Registration Request message to indicate that the mobile node would like its home agent to keep its mobility binding "private". Normally, the home agent sends Binding Update messages to correspondent nodes as needed to allow them to cache the mobile node’s binding. If the mobile node sets the Private (P) bit in the Registration Request message, the home agent MUST not send the mobile node’s binding in Binding Update messages. Instead, each Binding Update message should give the mobile node’s care-of address equal to its home address, and should give a Lifetime value of 0.

Thus, the Registration Request message under Route Optimization begins as follows:

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type |S|B|D|M|G|P|rvd|          Lifetime             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| (unchanged...)                           
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Private (P)

The Private (P) bit is set by the node sending the Binding Update message to indicate that the home agent should keep its mobility binding private. In any Binding Update message sent by the mobile node’s home agent, the care-of address should be set equal to the mobile node’s home address, and the Lifetime should be set equal to 0.
5. Route Optimization Extension Formats

Route Optimization defines the following Mobile IP message extensions:

- 96 = Previous Foreign Agent Notification Extension
- 97 = Route Optimization Authentication Extension
- 98 = Registration Key Request Extension
- 99 = Home-Mobile Registration Key Reply Extension
- 100 = Home-Foreign Registration Key Reply Extension
- 101 = Diffie-Hellman Registration Key Request Extension
- 102 = Diffie-Hellman Registration Key Reply Extension
- 103 = Foreign Agent Public Key Digest Advertisement Extension
- 104 = Registration Key Request Public Key Digest Extension
- 105 = Foreign Agent Public Key Extension
- 106 = Mobile Node Public Key Extension
- 107 = Foreign-Mobile Registration Key Reply Extension

Route Optimization also requires one minor change to existing Mobile IP message extensions: a new flag bit must be added to the Mobile Service extension, replacing a previously unused, reserved bit in the extension.

This section describes each of the new Route Optimization message extensions and the change to Mobile Service extension.
5.1. Previous Foreign Agent Notification Extension

The Previous Foreign Agent Notification extension may be included in a Registration Request message sent to a foreign agent. It requests the new foreign agent to send a Binding Update message to the mobile node’s previous foreign agent on behalf of the mobile node, to notify it that the mobile node has moved. The previous foreign agent deletes the mobile node’s visitor list entry and, if a new care-of address is included in the Binding Update message, also creates a binding cache entry for the mobile node pointing to its new care-of address. The Previous Foreign Agent Notification extension contains only those values not otherwise already contained in the Registration Request message that are needed for the new foreign agent to construct the Binding Update message.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Cache Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Previous Foreign Agent Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Care-of Address Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authenticator ...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Type

96

Length

10 plus the length of the Authenticator

Cache Lifetime

The number of seconds remaining before the binding cache entry created by the previous foreign agent must be considered expired. A value of all ones indicates infinity. A value of zero indicates that the previous foreign agent should not create a binding cache entry for the mobile node once it has deleted the mobile node’s visitor list entry. The Cache Lifetime value is copied into the Lifetime field of the Binding Update message.
Previous Foreign Agent Address

The IP address of the mobile node’s previous foreign agent to which the new foreign agent should send a Binding Update message on behalf of the mobile node.

New Care-of Address

The new care-of address for the new foreign agent to send in the Binding Update message to the previous foreign agent. This SHOULD be either the care-of address being registered in this new registration (i.e., to cause IP datagrams from the previous foreign agent to be tunneled to the new foreign agent) or the mobile node’s home address (i.e., to cause the previous foreign agent to only delete its visitor list entry for the mobile node).

Authenticator

The authenticator value to be used in the Route Optimization Authentication extension in the Binding Update message sent by the new foreign agent to the mobile node’s previous foreign agent. This authenticator is calculated only over the Binding Update message body.
5.2. Route Optimization Authentication Extension

The Route Optimization Authentication extension is used to authenticate certain Route Optimization management messages.

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Length    |        Authenticator ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   Type
      97
Length
The length of the Authenticator
Authenticator
(variable length) A value computed from a stream of bytes including the shared secret, the UDP payload (that is, the Route Optimization management message), all prior extensions in their entirety, and the type and length of this extension, but not including the Authenticator field itself nor the UDP header.
5.3. Registration Key Request Extension

The Registration Key Request extension may be used in Registration Request messages to request a registration key from the mobile node’s home agent. The extension is included in the Registration Request message by the mobile node. It is authenticated along with the rest of the Registration Request message, and thus no additional authenticator is included in the extension. In response to a Registration Key Request extension, the home agent MAY include a Home-Mobile Registration Key Reply extension and a Home-Foreign Registration Key Reply extension in its Registration Reply message, containing encrypted copies of the (same) new registration key for the mobile node and the foreign agent, respectively.

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

Type

98

Length

0

The mobility security association assumed to exist between the home agent and the mobile node will be used to encrypt the key sent in the Home-Mobile Registration Key Reply extension, unless a Key Identification extension is also included with the Registration Request message.

The home agent must also share a mobility security association with the foreign agent in order to return the requested registration key, and the home agent will use this security association to encrypt the key sent in the Home-Foreign Registration Key Reply extension.
5.4. Home-Mobile Registration Key Reply Extension

The Home-Mobile Registration Key Reply extension may be used in Registration Reply messages to send a registration key from the mobile node’s home agent to the mobile node. When used, the home agent MUST also include a Home-Foreign Registration Key Reply extension in the Registration Reply message, giving a copy of the same key to the mobile node’s new foreign agent. The Home-Mobile Registration Key Reply extension is authenticated along with the rest of the Registration Reply message, and thus no additional authenticator is included in the extension.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Mobile Node Encrypted Key</th>
</tr>
</thead>
</table>
| 99   |        | (variable length) The registration key, chosen by the home agent, encrypted under the mobility security association between the home agent and the mobile node. The same key must be sent, encrypted for the foreign agent in a Foreign Agent Registration Key extension in this Registration Reply message.
5.5. Home-Foreign Registration Key Reply Extension

The Home-Foreign Registration Key Reply extension may be used in Registration Reply messages to send a registration key from the mobile node’s home agent to the mobile node’s new foreign agent. When used, the home agent MUST also include a Home-Mobile Registration Key Reply extension in the Registration Reply message, giving a copy of the same key to the mobile node. The Home-Foreign Registration Key Reply extension is authenticated by including an authenticator in the extension, computed based on the mobility security association shared between the home agent and the foreign agent. In order for this extension to be used, the home agent MUST share a mobility security association with the foreign agent.

```
+----------------+----------------+----------------+----------------+
|     Type      |     Length    |  Foreign Agent Encrypted Key ... |
+----------------+----------------+----------------+----------------+----------------+
|    Authenticator ... |
+----------------+----------------+----------------+
```

Type

100

Length

The length of the Foreign Agent Encrypted Key plus the length of the Authenticator

Foreign Agent Encrypted Key

(variable length) The registration key, chosen by the home agent, encrypted under the mobility security association between the home agent and the foreign agent. The same key must be sent, encrypted for the mobile node in a Mobile Node Registration Key extension in this Registration Reply message.

Authenticator

(variable length) A value computed from a stream of bytes including the shared secret and the fields in this extension other than the Authenticator field itself.
5.6. Diffie-Hellman Registration Key Request Extension

The Diffie-Hellman Registration Key Request extension may be included in a Registration Request message sent to a foreign agent. It begins the Diffie-Hellman key exchange algorithm [2] between the mobile node and its new foreign agent, as described in Section 7.2. The foreign agent SHOULD then include a Diffie-Hellman Registration Key Reply extension in its Registration Reply message sent to the mobile node in order to complete the key exchange.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3 times the length of each of Prime, Generator, and Computed Value. The values Prime, Generator, and Computed Value must all be the same length, which must be a multiple of 8 bits.</td>
</tr>
</tbody>
</table>

**Prime**

One of the two public numbers involved in the Diffie-Hellman key exchange algorithm. The value Prime should be a large prime number.

**Generator**

One of the two public numbers involved in the Diffie-Hellman key exchange algorithm. If p is the value of the Prime used for this Diffie-Hellman exchange, the value Generator should be less than p, and should be a primitive root of p.
Computed Value

The public computed value from the mobile node for this Diffie-Hellman exchange. The mobile node chooses a large random number, x. If \( g \) is the value of the Generator and \( p \) is the value of the Prime, the Computed Value in the extension is \((g^x) \mod p\).
5.7. Diffie-Hellman Registration Key Reply Extension

The Diffie-Hellman Registration Key Reply extension SHOULD be included in a Registration Reply message sent by a foreign agent to a mobile node that included a Diffie-Hellman Registration Key Request extension in its Registration Request message to the foreign agent.

+---------------+---------------+---------------+---------------+
| Type          | Length        |
+---------------+---------------+---------------+---------------+
|               |               |               |
+---------------+---------------+---------------+---------------+
| Computed Value|
+---------------+---------------+---------------+---------------+

Type

101

Length

The length of the Computed Value. The length of the Computed Value must be a multiple of 8 bits.

Computed Value

The foreign agent chooses a large random number, y. If g is the value of the Generator and p is the value of the Prime, the Computed Value in the extension is (g**y) mod p. The values of the Generator and Prime are taken from the Diffie-Hellman Registration Key Request extension from the mobile node’s Registration Request message.
5.8. Mobile Service Extension

One bit is added to the flag bits in the Mobile Service extension (forming an Agent Advertisement message), when sent by a foreign agent, to indicate that the foreign agent supports registration key establishment using the Diffie-Hellman key exchange algorithm. When this bit is set in the Agent Advertisement, the mobile node MAY request a registration key be established by including a Diffie-Hellman Registration Key Request extension in its Registration Request message. The foreign agent replies with the Diffie-Hellman Registration Key Reply extension in its Registration Reply to the mobile node.

Thus, the Mobile Service extension under Route Optimization begins 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |        Sequence Number        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Lifetime            |R|B|H|F|M|G|D|    reserved     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| (unchanged...)|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
Diffie-Hellman (D)

The Diffie-Hellman (D) bit is set by the foreign agent sending the Agent Advertisement message to indicate that it supports the registration key establishment protocol using the Diffie-Hellman Registration Key Request and Diffie-Hellman Registration Key Reply extensions.
6. Mobility Security Association Management

One of the most difficult aspects of Route Optimization for Mobile IP in the Internet today is that of providing authentication for all messages that affect the routing of datagrams to a mobile node. In the base Mobile IP protocol, all routing of datagrams to the mobile node while away from its home network is controlled by the home agent, since only the home agent is aware of the mobile node’s mobility binding and only the home agent tunnels datagrams to the mobile node. Authentication is currently achieved based on a manually established mobility security association between the home agent and the mobile node. Since the home agent and the mobile node are both owned by the same organization (both are assigned IP addresses within the same IP subnet), this manual configuration is manageable, and (for example) can be performed while the mobile node is at home.

However, with Route Optimization, authentication is more difficult to manage, since a Binding Update may in general need to be sent to any node in the Internet. Since no general authentication or key distribution protocol is available in the Internet today, the Route Optimization procedures defined in this document make use of the same type of manually configured mobility security associations used in the base Mobile IP protocol. For use with Route Optimization, a mobility security association held by a correspondent node or a foreign agent must in general include the same parameters as required by the base Mobile IP protocol specification [6].

For a correspondent node to be able to create a binding cache entry for a mobile node, the correspondent node and the mobile node’s home agent MUST have established a mobility security association. This mobility security association, though, may be used in creating and updating binding cache entries at this correspondent node for all mobile nodes served by this home agent. This places the correspondent node in a fairly natural relationship with respect to the mobile nodes served by this home agent. For example, these mobile nodes may represent different people affiliated with the organization owning the home agent and these mobile nodes, with which the user of this correspondent node often collaborates. In this case, the effort of establishing the necessary mobility security association with this home agent may be justified. It is similarly possible for a home agent to have a manually established mobility security association with the foreign agents often used by its mobile nodes, or for a particular mobile node to have a manually established mobility security association with the foreign agents serving the foreign networks that it often visits.
In general, if the movement and communication patterns of a mobile node or the group of mobile nodes served by the same home agent are sufficient to justify establishing a mobility security association with the mobile node's home agent, users or network administrators are likely to do so. Without establishing a mobility security association, nodes will not currently be able to use the Route Optimization extensions but can use the base Mobile IP protocol.
7. Methods of Establishing a Registration Key

This document suggests four different methods that a mobile node could use for dynamically establishing a registration key with a foreign agent when it registers with that foreign agent.

7.1. Using the Home Agent as a Key Distribution Center

One method of establishing a registration key is for the mobile node to request its home agent to generate one during registration, and for the home agent to send a copy of this key to both the mobile node and its new foreign agent. The home agent in this case acts as a "key distribution center" (KDC) for the mobile node and the foreign agent. The mobile node requests this by including a Registration Key Request extension in its Registration Request message. The home agent sends the generated key to the mobile node and to its foreign agent by including a Home-Mobile Registration Key Reply extension and a Home-Foreign Registration Key Reply extension its Registration Reply message. The Home-Mobile Registration Key Reply extension contains a copy of the chosen key encrypted under a key and algorithm shared between the home agent and the mobile node, and a Home-Foreign Registration Key Reply extension contains a copy of the same key encrypted under a key and algorithm shared between the home agent and the foreign agent.

In order for the registration key to be established using this method, the foreign agent must have a mobility security association with the home agent. For example, if mobile nodes from some home network often visit this foreign agent, it may in general be worth the effort of creating such a mobility security association between this foreign agent and the home agent serving that home network. If no mobility security association exists, a mobile node may instead be able to establish a registration key with its home agent using the alternative method described in the next section.

7.2. Using Diffie-Hellman with the Foreign Agent

An alternate method defined in this document for establishing a registration key is for the mobile node and its foreign agent to execute the Diffie-Hellman key exchange algorithm [2] as part of the mobile node's registration. The Diffie-Hellman algorithm is a public key cryptosystem that allows two parties to establish a shared secret key, such that the shared secret key cannot be determined by other parties overhearing the messages exchanged during the algorithm. It is used, for example, in other protocols that require a key exchange, such as in the Cellular Digital Packet Data (CDPD) system [1].
Briefly, the Diffie-Hellman algorithm involves the use of two large public numbers, a Prime number \((p)\) and a Generator \((g)\). The Prime number and the Generator must be known by both parties involved in the algorithm, but need not be kept secret; these values may be different for each execution of the algorithm and are not used once the algorithm completes. Each party chooses a private random number, produces a Computed Value based on this random number and the Prime and the Generator, and sends the Computed Value in a message to the other party. Each party then computes the (same) shared secret key using its own private random number, the Computed Value received from the other party, and the Prime and Generator values.

To use this algorithm during registration with a foreign agent, the mobile node includes a Diffie-Hellman Registration Key Request extension in its Registration Request message, containing its values for the Prime and Generator, along with the Computed Value from its own private random number. The foreign agent then chooses its own private random number and includes a Diffie-Hellman Registration Key Reply extension in its Registration Reply message to the mobile node; the extension includes the foreign agent’s own Computed Value based on its chosen random number and the supplied Prime and Generator values from the mobile node. The mobile node and foreign agent each independently form the (same) shared secret key from their own chosen random number, the Computed Value supplied by the other party, and the Prime and Generator values.

The Diffie-Hellman algorithm allows the mobile node and its foreign agent to establish a registration key without any pre-existing mobility security associations, but the Diffie-Hellman algorithm itself is covered by a patent in the United States. The method of establishing a registration key using Diffie-Hellman thus may not be usable by those who have not licensed the patent. An implementation of the Diffie-Hellman key exchange algorithm is available, though, in the free RSAREF toolkit from RSA Laboratories [7].

Also, establishing a registration key using Diffie-Hellman is computationally more expensive than the method described in Section 7.1. The use of Diffie-Hellman described here, though, is designed to allow the Diffie-Hellman computations to be overlapped with other activities. The mobile node may choose (or be manually configured with) the Prime and Generator values at any time, or may use the same two values for a number of registrations. The mobile node may also choose its private random number and compute its Computed Value at any time. For example, after completing one registration, the mobile node may choose the private random number for its next registration and begin the computation of its new Computed Value based on this random number, such that it has completed this computation before it is needed in its next registration.
registration; in its simplest form, the mobile node may use the same private random number and Computed Value for any number of registrations. The foreign agent may choose its private random number and begin computation of its Computed Value based on this number as soon as it receives the mobile node's Registration Request message, and need only complete this computation before it sends the matching Registration Reply message for the mobile node’s registration.

The Agent Advertisement message (Mobile Service extension) is revised under Route Optimization to include a bit to indicate that the foreign agent sending the advertisement supports this method of registration key establishment using the Diffie-Hellman algorithm. If this bit is not set in the Agent Advertisement from the foreign agent, the mobile node MUST NOT send a Diffie-Hellman Registration Key Request extension to the foreign agent in its Registration Request message.

**DISCUSSION:** This could be extended to support other similar key exchange algorithms, either by adding a new Request and Reply extension for each, or by adding a field in the extensions to indicate which algorithm is to be used. Diffie-Hellman seems the only obvious choice, though, currently.

### 7.3. Using a Mobile Node Public Key

The mobile node includes its public key (such as RSA) in its Registration Request to the foreign agent, using a Mobile Node Public Key extension. The foreign agent chooses the new registration key and returns a copy of it encrypted with the mobile node’s public key, using a Foreign-Mobile Registration Key Reply extension.

### 7.4. Using a Foreign Agent Public Key

The foreign agent includes an MD5 digest of its public key (such as RSA) in its Agent Advertisement messages, using a Foreign Agent Public Key Digest Advertisement extension. The mobile node includes a copy of this digest in its Registration Request, using a Registration Key Request Public Key Digest extension, and the foreign agent adds its full public key to the Registration Request when relaying it to the home agent, using a Foreign Agent Public Key extension. The home agent then chooses the new registration key and returns a separate encrypted copy of the key to the foreign agent (using this public key) and to the mobile node (using its mobility security association with the mobile node) in its Registration Request.
Reply message. The copy sent to the foreign agent is included in a Home-Foreign Registration Key Reply extension, and the copy sent to the mobile node is included in a Home-Mobile Registration Key Reply extension.
8. Binding Cache Considerations

Any node may maintain a binding cache in order to optimize its own communication with mobile nodes. When sending an IP datagram, if the sending node has a binding cache entry for the destination node, it MAY tunnel the datagram to the mobile node’s care-of address using the encapsulation techniques described for home agents in the base Mobile IP protocol specification [6]. Any optional encapsulation methods supported are indicated by flag bits in the Binding Update message.

When a mobile node’s home agent intercepts a datagram on the home network and tunnels it to the mobile node, the originating node generally has no binding cache entry for the destination mobile node. In such cases, the home agent MAY send a Binding Update message to the originator.

Similarly, when a node other than the foreign agent currently serving a mobile node receives a datagram for a mobile node, and this datagram has been tunneled to that node, the node tunneling the datagram generally has an out-of-date binding for the mobile node in its binding cache. In such cases, the node receiving the tunneled datagram MAY send a Binding Warning message to the mobile node’s home agent, advising it to send a Binding Update message to the tunneling node.

8.1. Cache Management

A node maintaining a binding cache may use any reasonable strategy for managing the space within the cache. When a new entry needs to be added to the binding cache, the node MAY choose to drop any entry already in the cache, if needed, to make space for the new entry. For example, a "least-recently used" (LRU) strategy for cache entry replacement is likely to work well.

Each binding in the binding cache also has an associated lifetime, specified by in the Binding Update message in which the node obtained the binding. After the expiration of this time period, the binding MUST be deleted from the cache.

8.2. Receiving Binding Update Messages

When a node receives a Binding Update message, it MUST verify the authentication in the message, using the mobility security association it shares with the mobile node’s home agent. The authentication data is found in the Route Optimization Authentication
extension (Section 5.2). If the authentication succeeds, then a binding cache entry SHOULD be updated for use in future transmissions of data to the mobile node. Otherwise, an authentication exception SHOULD be raised.

8.3. Using Special Tunnels

Whenever any node receives a tunneled datagram for which it has no visitor list entry for the datagram’s destination, the node may deduce that the tunneling node has an out-of-date binding cache entry for the destination mobile node. If the node receiving the tunneled datagram has a binding cache entry for the destination, it SHOULD re-tunnel the datagram to the care-of address indicated in this binding cache entry.

However, if the node receiving the tunneled datagram has no binding cache entry for the destination, it cannot re-tunnel the node to its destination. Instead, the node SHOULD forward the datagram to the destination mobile node’s home agent, using a special form of tunneling called a "special tunnel". To tunnel the datagram using a special tunnel, the tunneled datagram’s destination address is set equal to the destination address in the tunneled datagram. Thus, both the "inner" and "outer" destination addresses are set to the home address of the mobile node. The tunneled datagram will thus be routed to the mobile node’s home network, where it will be intercepted by the mobile node’s home agent in the same way as other datagrams addressed to the mobile node.

The home agent SHOULD then tunnel the datagram to the current care-of address for the mobile node. However, the home agent MUST NOT tunnel the datagram to the current care-of address if the special tunnel of the datagram originated at that care-of address, as indicated by the "outer" source address of the special tunnel datagram. The use of the special tunnel format allows the home agent to identify the node that tunneled the datagram to it (as well as the original sender of the datagram). If the home agent believes that the current care-of address for the mobile node is the same as the source of the special tunnel, then the home agent SHOULD discard the datagram; in this case, the foreign agent serving the mobile node appears to have lost its entry for the mobile node in its visitor list, for example, if the foreign agent has crashed and rebooted.

After tunneling the datagram to the current care-of address for the mobile node, the home agent MAY notify the source of the special tunnel of the mobile node’s current binding, by sending it a Binding Update message.
9. Home Agent Considerations

The home agent will be the frequent source of Binding Update messages sent to correspondent nodes that are communicating with its mobile nodes. Any correspondent node that has no binding cache entry for a mobile node, will send normal, untunneled datagrams through the home agent by the normal routing in the Internet. When the home agent first receives a datagram for a mobile node, it SHOULD also send a Binding Update message to the originator of the datagram in hopes that the originator will be able to create a binding cache entry for that mobile node. Then, future datagrams sent by this node to the mobile node should not need the involvement of the home agent.

9.1. Rate Limiting

A home agent MUST provide some mechanism to limit the rate at which it sends Binding Update messages to the same node about any given mobility binding. This rate limiting is especially important because it is expected that, within the short term, many Internet nodes will not support maintenance of a binding cache. In this case, continual transmissions of Binding Update messages to such a correspondent node will only add unnecessary overhead to the home agent and correspondent node, and along the Internet path between these nodes.

9.2. Receiving Binding Warning Messages

A home agent will receive a Binding Warning message if a node maintaining a binding cache entry for one of the home agent’s mobile nodes uses the entry after it becomes out-of-date. When a home agent receives a Binding Warning message, it SHOULD send a Binding Update message to the Target Node Address identified in the Binding Warning, giving it the current binding for the mobile node identified in the Mobile Node Home Address field of the Binding Warning.

If using nonces for replay protection, the use of the Identification field in the Binding Update message is different in this case, in order to still allow replay protection even though the Binding Update is not being sent in reply to a request directly from the target node. In this case, the high-order 32 bits of the Identification field MUST be set by the home agent to the value of the nonce that will be used by the home agent in the next Binding Update message sent to this node. The low-order 32 bits of the Identification field MUST be set to the value of the nonce being used for this message. Thus, on each Binding Update message, the home agent communicates to the target node, the value of the nonce that will be used next time, and if no Binding Updates are lost in the network, the home agent and...
the target node can remain synchronized with respect to the nonces being used. If, however, the target node receives a Binding Update with what it believes to be an incorrect nonce, it may resynchronize with the home agent by requesting the mobile node’s binding using a Binding Request message.

9.3. Receiving Binding Request Messages

When the home agent receives a Binding Request message, it consults its home list and determines the correct binding information to be sent to the requesting node. Before satisfying the request, the home agent MUST check whether or not the mobile node has allowed the information to be disseminated. If the mobile node specified the Private (P) bit in its Registration Request message, then the home agent MUST not satisfy any Binding Requests. In this case, the home agent SHOULD return a Binding Update in which both the Care-of Address is set equal to the mobile node’s home address and the Lifetime is set to zero. Such a Binding Update message indicates that the binding cache entry for the specified mobile node should be deleted.

9.4. Receiving Registration Key Requests

When the home agent receives a Registration Request message, a Registration Key Request extension (Section 5.3) may be present in the message, requesting the home agent to provide a registration key to the mobile node and its foreign agent, as described in Section 3.2. In that event, the home agent employs a good algorithm for producing random keys [4] and encrypts the result separately for use by the foreign agent and by the mobile node. The chosen key is encrypted under the mobility security association shared between the home agent and the mobile node, and the encrypted key is placed in a Home-Mobile Registration Key Reply extension (Section 5.4) in the Registration Reply message. The same key also is encrypted under the mobility security association shared between the home agent and the foreign agent, and the encrypted key is placed in a Home-Foreign Registration Key Reply extension (Section 5.5) in the Registration Reply message.

If the home agent receives a Registration Key Request extension in a Registration Request message, but it does not have an established mobility security association with the foreign agent with which the mobile node is registering, the home agent MUST reject the registration attempt. In this case, the home agent returns a Registration Reply message indicating that the foreign agent failed authentication.
9.5. Receiving Special Tunnels

The home agent may also receive datagrams tunneled to the mobile node using a special tunnel (Section 8.3), which it has intercepted for the mobile node in the same way as any datagram destined to the mobile node while the mobile node is away from home. The home agent MUST examine the tunnel source address (the "outer" address of the tunneled datagram). If the tunnel source address differs from the care-of address shown in the home list entry for the mobile node, the home agent SHOULD decapsulate the inner datagram from the tunnel and re-tunnel it to the mobile node’s care-of address. However, if the tunnel source address is the same as the mobile node’s care-of address, the home agent MUST NOT tunnel the datagram back to that same node; the home agent SHOULD instead discard the datagram.

In either case, the home agent SHOULD also send a Binding Update message to the sender of the original datagram (the "inner" source address of the tunneled datagram), if it shares a mobility security association with this node. The sending of this Binding Update message, though, is subject to the rate limiting restriction described in Section 9.1.
10. Foreign Agent Considerations

In addition to managing the resources needed to handle registrations in the base Mobile IP protocol, a foreign agent participating in Route Optimization assumes two additional responsibilities. It SHOULD maintain a binding cache for forwarding datagrams to mobile nodes once they have moved to new care-of addresses, and it SHOULD support the use of a Binding Update message for notifying a mobile node’s previous foreign agent that it has moved.

10.1. Establishing a Registration Key

As part of the registration procedure, a mobile node and its new foreign agent can establish a registration key (Sections 7.1 and 7.2). Within this document, the registration key is used only for authentication of a single Binding Update message. Other uses for the registration key are possible, such as the use of this key to provide privacy along the wireless link connecting between the mobile node and its foreign agent; such additional uses of the registration key are outside the scope of this discussion.

This document specifies two alternative methods for establishing a registration key as part of a mobile node’s registration with a foreign agent.

The foreign agent may receive a Registration Key Request extension in the mobile node’s Registration Request message (Section 7.1). The foreign agent need not process the Registration Key Request extension. When the Registration Reply is received by the foreign agent from the home agent, it MAY contain a Home-Foreign Registration Key Reply extension and a Home-Mobile Registration Key Reply extension. In this case, the foreign agent removes the Home-Foreign Registration Key Reply extension, and forwards the rest of the Registration Reply message to the mobile node. The Home-Foreign Registration Key Reply extension is covered by its own authentication, not by the authentication covering the Registration Reply message itself, and thus removing the Home-Foreign Registration Key Reply extension does not interfere with the mobile node’s ability to verify the authentication on the Registration Reply message. The foreign agent decrypts the supplied registration key using the mobility security association it shares with the home agent, and stores the key as part of the visitor list entry created for the mobile node for this registration.

Alternatively, the foreign agent may receive a Diffie-Hellman Registration Key Request extension in the mobile node’s Registration Request message (Section 7.2). The extension contains the Prime
and Generator values, chosen by the mobile node, to be used for this execution of the Diffie-Hellman algorithm. The foreign agent chooses its own private random number and returns the Diffie-Hellman Computed Value when it sends the Registration Reply message sent to the mobile node. The foreign agent uses Prime and Generator values and the Computed Value from the mobile node that it received in the Diffie-Hellman Registration Key Request extension, together with its own chosen private random number, to form the registration key. The foreign agent stores this registration key as part of the visitor list entry created for the mobile node for this registration.

Establishing the registration key in effect establishes a mobility security association between the mobile node and the foreign agent. After the mobile node moves to a new care-of address, this mobility security association is used for authenticating the Binding Update message from the mobile node notifying this foreign agent of its movement.

10.2. Previous Foreign Agent Notification

When a mobile node registers with a new foreign agent, the mobile node MAY request its new foreign agent to notify its previous foreign agent that it has moved. The mobile node includes a Previous Foreign Agent Notification extension in its Registration Request message to the foreign agent, requesting that the foreign agent send a Binding Update message to its previous foreign agent. As with all Binding Update messages, this Binding Update must be authenticated using the Route Optimization Authentication extension (Section 5.2).

The foreign agent assembles the Binding Update message using the fields in the Registration Request message (including the Authenticator supplied in the Previous Foreign Agent Notification extension) and sends it to the previous foreign agent identified in the extension. The Acknowledge (A) bit MUST be set in this Binding Update message.

When the previous foreign agent receives the Binding Update, it will authenticate the message using the mobility security association set up with the registration key established with the mobile node during its registration with this mobile node. If the message authentication is correct, the visitor list entry for the mobile node at the previous foreign agent will be deleted and a Binding Acknowledge message returned to the sender. In addition, if a new care-of address was included in the Binding Update message, the previous foreign agent will create a binding cache entry for the mobile node; the previous foreign agent can then tunnel datagrams to
the mobile node’s new care-of address using that binding cache, just as any node maintaining a binding cache.

In particular, the previous foreign agent can tunnel the Binding Acknowledge message back to the new care-of address specified in the received binding. This creates an interesting problem for the new foreign agent when it receives the acknowledgment before the registration reply from the home agent. It is suggested that the new foreign agent deliver the acknowledgment to the mobile node anyway, even though the mobile node is technically unregistered. If there is concern that this provides a loophole for unauthorized traffic to the mobile node, the new foreign agent could limit the number of datagrams delivered to the unregistered mobile node to this single instance. Alternatively, a new extension to the Registration Reply message can be defined to carry along the acknowledgement from the previous foreign agent. This latter approach would have the benefit that fewer datagrams would be transmitted over bandwidth-constrained wireless media during registrations.

The registration key established with this previous foreign agent is destroyed as a part of the processing of this Binding Update message. Since the previous foreign agent deletes the visitor list entry for the mobile node, it also deletes its record of the registration key. A registration key is thus useful only for the notification to the previous foreign agent after moving to a new care-of address. No subsequent use of this registration key is possible, and thus no reply protection is necessary for the Binding Update message used for this notification.

10.3. Receiving Tunneled Datagrams

When a foreign agent receives a datagram tunneled to itself, it examines its visitor list for an entry for the destination mobile node, as in the base Mobile IP protocol. If a visitor list entry is found, the foreign agent delivers the datagram to the mobile node.

However, if no visitor list entry is found, the foreign agent examines its binding cache for a cache entry for the destination mobile node. If one is found, the foreign agent re-tunnels the new care-of address indicated in the binding cache entry. In this case, the foreign agent also may deduce that the sender of the datagram has an out-of-date binding cache entry for this mobile node, since it otherwise would have tunneled the datagram directly to the correct new care-of address itself. The foreign agent SHOULD then send a Binding Warning message to the mobile node’s home agent, which it learned in the Binding Update message from which this binding cache entry was created.
10.4. Rate Limiting

A foreign agent MUST provide some mechanism to limit the rate at which it sends Binding Warning messages to the same node about any given mobility binding. This rate limiting is especially important because it is expected that, within the short term, many Internet nodes will not support maintenance of a binding cache. In this case, continual transmissions of Binding Warning messages to such a correspondent node will only add unnecessary overhead to the foreign agent and correspondent node, and along the Internet path between these nodes.

10.5. Sending Special Tunnels

If a foreign agent receives a tunneled datagram for a mobile node for which it has no visitor list entry or binding cache entry, the foreign agent MAY forward the datagram to the mobile node’s home agent by sending it as a special tunnel (Section 3.2). The home agent will intercept the special tunnel datagram addressed to the mobile node in the same way as any datagram for the mobile node while it is away from home.
11. Mobile Node Considerations

11.1. Establishing a Registration Key

When a mobile node sends a Registration Request message, it can also request a registration key to be established between itself and the new foreign agent. The key may be used later to authenticate the Binding Update sent to this foreign agent to notify it that the mobile node has moved to a new care-of address.

The mobile node may include a Registration Key Request extension in its Registration Request message to request its home agent to act as a "key distribution center" (KDC) for establishing a registration key with its new foreign agent (Section 7.1). The home agent chooses a new key and returns encrypted copies of it for the foreign agent and the mobile node. The mobile node receives its copy of the new key in the Home-Mobile Registration Key Reply extension in the Registration Reply extension. The mobile node decrypts the key using the mobility security association it shares with its home agent, and stores the key for later use in notifying this foreign agent that it has moved to a new care-of address.

Alternatively, the mobile node may include a Diffie-Hellman Registration Key Request extension in its Registration Request message to request its new foreign agent to participate in the Diffie-Hellman key exchange algorithm with it. The mobile node chooses a private random number and includes the Prime and Generator values to be used in this execution of the Diffie-Hellman algorithm, together with the Computed Value based on its chosen private random number, in the Diffie-Hellman Registration Request extension. The foreign agent chooses its own private random number, and returns the Computed Value based on this number in a Diffie-Hellman Registration Key Reply extension in the Registration Reply that it returns to the mobile node. The mobile node forms the registration key according to the Diffie-Hellman algorithm and stores it for later use in notifying this foreign agent that it has moved to a new care-of address.

11.2. Notifying Previous Foreign Agents

During registration with a new foreign agent, a mobile node may request its new foreign agent to notify its previous foreign agent that it has moved. The new foreign agent sends a Binding Update message to the previous foreign agent on behalf of the mobile node.

To notify its previous foreign agent as part of the new registration, the mobile node includes a Previous Foreign Agent Notification extension (Section 5.1) in its Registration Request message. The
extension contains only those values needed by the new foreign agent to construct the Binding Update message that are not already included in the Registration Request message. In particular, the new foreign agent only sends the Binding Update message on behalf of the mobile node. The mobile node computes the correct Authenticator value for the Binding Update message, based on the registration key it established with its previous foreign agent, and includes this Authenticator value in the extension for inclusion in the Binding Update message by the new foreign agent. The new foreign agent does not learn the previous foreign agent registration key during the new registration or notification.

When the Binding Acknowledgment message from the previous foreign agent is received by the new foreign agent, it detunnels it and sends it to the mobile node. In this way, the mobile node can discover that its previous foreign agent has received the Binding Update message. This is important, because otherwise the previous foreign agent would often become a "black hole" for datagrams destined for the mobile node based on out-of-date binding cache entries at other nodes. The new foreign agent has no further responsibility for helping to update the binding cache at the previous foreign agent.

The mobile node expects to eventually receive a Binding Acknowledgement message from its previous foreign agent, signifying that the Binding Update message was received. If the acknowledgement has not been received after sufficient time, the mobile node is responsible for retransmitting another Binding Update message to its previous foreign agent. Although the previous foreign agent may have already received and processed the Binding Update message (the Binding Acknowledge message may have been lost in transit to the new foreign agent), the mobile node should continue to retransmit its Binding Update message until the previous foreign agent responds with a Binding Acknowledgement.
References


Appendix A. Using a Master Key at the Home Agent

Rather than storing each mobility security association that it has established with many different correspondent nodes and foreign agents, a home agent may manage its mobility security associations so that each of them can be generated from a single "master" key. With the master key, the home agent could build a key for any given other node by computing the node-specific key as

\[
\text{MD5}(\text{node-address} \ || \ \text{master-key} \ || \ \text{node-address})
\]

where node-address is the IP address of the particular node for which the home agent is building a key, and master-key is the single master key held by the home agent for all mobility security associations it has established with correspondent nodes. The node-specific key is built by computing an MD5 hash over a string consisting of the master key with the node-address concatenated as a prefix and as a suffix.

Using this scheme, when establishing each mobility security association, the network administrator managing the home agent computes the node-specific key and communicates this key to the network administrator of the other node through some "secure" channel, such as over the telephone. The mobility security association is configured at this other node in the same way as any mobility security association. At the home agent, though, no record need be kept that this key has been given out. The home agent need only be configured to know that this scheme is in use for all of its mobility security associations (perhaps only for specific set of its mobile nodes).

When the home agent then needs a mobility security association as part of Route Optimization, it builds the node-specific key based on the master key and the IP address of the other node with which it is attempting to authenticate. If the other node knows the correct node-specific key, the authentication will succeed; otherwise, it will fail as it should.
Chairs’ Addresses

The working group can be contacted via the current chairs:

Tony Li
Cisco Systems
170 W. Tasman Drive
San Jose, CA  95134

Phone:  +1-408-526-8186
E-mail: tli@cisco.com

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

Phone:  +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

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

Charles Perkins
Room J1-A25
T. J. Watson Research Center
IBM Corporation
30 Saw Mill River Rd.
Hawthorne, NY  10532

Phone:    +1-914-784-7350
Fax:       +1-914-784-7007
E-mail: perk@watson.ibm.com