

Network Working Group
Internet-Draft
Expires: May 17, 2008

B. Sarikaya
Huawei Technologies USA
A. Qin
A. Huang
W. Wu
Huawei Technologies
November 14, 2007

PMIPv6 Route Optimization Protocol
draft-qin-mipshop-pmipro-01.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on May 17, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Internet-Draft

PMIPv6 Route Optimization

November 2007

Abstract

This document defines route optimization protocol for Proxy Mobile IPv6. Proxy home test, concurrent proxy care-of test and handover procedures based on Enhanced Route Optimization for Mobile IPv6 are explained. Mobile access gateway uses cryptographically generated home addresses so that no more home test is needed after the initial home test. Handover home keygen token is used during handover in order to eliminate home test for the next mobile access gateway. The protocol also supports IPv4 transport network operation.

Table of Contents

1.	Introduction	3
2.	Terminology	4
3.	PMIPv6 R0 Scenarios and Overview	5
3.1.	PMIPv6 R0 Scenario Analysis	5
3.2.	PMIPv6 R0 Overview	6
4.	PMIPv6 Route Optimization for Type 1 Correspondent Nodes . . .	8
4.1.	Proxy Home Test Procedure	8
4.2.	Concurrent Proxy Care-of Test	9
4.3.	Handover	10
4.4.	Complete Proxy Binding Update	11
5.	PMIPv6 Route Optimization for Type 2 Correspondent Nodes . . .	13
5.1.	IPv4 support	14
6.	Local Mobility Anchor Considerations	15
7.	Mobile Access Gateway Considerations	16
8.	Correspondent Node Considerations	16
9.	Requirements on PMIPv6 Handover/Context Protocol	17
10.	Message Formats	17
10.1.	Proxy Home Test	18
10.2.	Proxy Home Test Init Message	19
10.3.	Handover Home Keygen Token option	19
11.	IANA Considerations	20
12.	Security Considerations	20
13.	Acknowledgements	21
14.	References	21
14.1.	Normative References	21
14.2.	Informative references	21
	Authors' Addresses	22
	Intellectual Property and Copyright Statements	23

1. Introduction

In Mobile IPv6, the mobile nodes (MN) can establish a direct route with the correspondent nodes (CN), i.e. can optimize the route through MN establishing a binding of its Home Address (HoA) with its current care-of address (CoA) at CN [[RFC3775](#)]. The binding is established using return routability signaling and then refreshed periodically (every 7 minutes) and when MN's IP connectivity changes. Return routability procedure also called Correspondent Registrations involves CN's verification of MN's ownership of both HoA using a home address test (HoT) and CoA using care-of address test (CoT) all together designed to counter for the unprecedented security threats identified in [[RFC4225](#)] like impersonation and flooding threats.

Return routability procedure is lightweight, does not require a global Public-Key Infrastructure (PKI) or preshared keys between MN and CN. However, it increases signaling overhead and handoff delays. Return routability procedure can be optimized by using preshared keys [[RFC4449](#)] or cryptographically generated addresses [[RFC4866](#)].

In Proxy Mobile IPv6 (PMIPv6) scheme, the mobility is transparent to mobile nodes (MN) by the mobile access gateway (MAG) simulating a home link and acting as a proxy on Mobile IP operation, also is transparent to correspondent nodes (CN) by forcing all datagrams for a mobile node to be routed through its local mobility anchor (LMA). Thus, datagrams to the mobile node are often routed along paths that are significantly longer than optimal. However, packets could be routed directly between correspondent nodes and the mobile access gateway instead of through local mobility anchor, such path is optimal. Moreover, immunity to impersonation, denial of service, and redirection-based flooding is necessary for a route optimization protocol in PMIPv6. This document presents a mechanism, based on PMIPv6 [[I-D.ietf-netlmm-proxymip6](#)] and Enhanced Route Optimization for Mobile IPv6 [[RFC4866](#)], to securely establish optimal route between MAG and correspondent nodes or between two MAGs.

The following types of correspondent nodes are considered: correspondent nodes which have both Mobile IPv6 stack defined in [RFC3775](#) and recognize PMIPv6 messages, correspondent nodes without Mobile IPv6 function which are provided mobility support by Proxy Mobile IPv6. This document discusses both the first (Type 1 CNs) and the second (Type 2 CNs).

Type 1 CN's MUST support Enhanced Route Optimization for Mobile IPv6 [\[RFC4866\]](#) and extensions defined in this document. PMIPv6 RO is transparent for Type 2 CNs.

Some terminology is defined in Section 2. In [Section 3](#) scenarios are

defined and an overview of PMIPv6 RO is given. [Section 4](#) presents PMIPv6 Route Optimization Protocol for Type 1 CNs and [Section 5](#) presents for Type 2 CNs. [Section 6](#) defines local mobility anchor, [Section 7](#) defines mobile access gateway and [Section 8](#) defines correspondent node behaviour. [Section 9](#) is on requirements this protocol imposes on PMIPv6 Handover and Context Transfer protocol. In [Section 10](#), formats and options of messages are defined.

[2.](#) Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [\[RFC2119\]](#).

Most of the terminology used in this document refers to PMIPv6 [\[I-D.ietf-netlmm-proxymip6\]](#), Enhanced Route Optimization for Mobile IPv6 [\[RFC4866\]](#) and [\[I-D.ietf-netlmm-pmip6-ipv4-support\]](#). The changed definitions are listed below:

Mobile Access Gateway (MAG)

As is defined in [\[I-D.ietf-netlmm-proxymip6\]](#). In this document, the route optimization function is also provided by MAG.

Proxy Binding Cache

A cache of mobility bindings of mobile nodes, maintained by a mobile access gateway for use in sending or forwarding datagrams to MAGs serving for these mobile nodes.

Binding Update List

In this document, Binding Update List data structure is extended

to keep correspondent registrations at the mobile access gateway. Correspondent registration could be to another MAG for Type 2 CNs. Cryptographically generated home addresses

A cryptographically generated home address enables correspondent nodes to securely authenticate the owner of home address (HoA), by means of a strong, cryptographic binding between the interface identifier of the address and the address owner's public key. From the perspective of the correspondent node, the home address of the mobile node is owned by mobile access gateway during route optimization procedure. In this document, proxy mobile IPv6 home addresses are cryptographically generated home addresses using the mobile node's public key.

Permanent home keygen token

Permanent home keygen token A secret permanent home keygen token, which is generated by a correspondent node for a mobile node, is exchanged between mobile access gateway and a correspondent node. Permanent home keygen token kept by mobile access gateway is used to authenticate the mobile access gateway more efficiently in subsequent correspondent registrations. The permanent home keygen

token is renewed over complete PBU exchange and is not used to authenticate the early PBU message while the mobile node moves to the next mobile access gateway. Since the lifetime of proxy binding update is due, permanent home keygen token should be re-generated too.

Handover home keygen token

A secret handover home keygen token is a 64-bit random number generated by a correspondent node for a mobile node when the first proxy binding update containing Signature Option is received. Handover home keygen token is used to authenticate the early proxy binding update message and because of this, proxy home test after each handover can be skipped. During handover, handover home keygen token is transferred from the previous mobile access gateway to the next mobile access gateway.

Type 1 Correspondent Node

A node that is Mobile IPv6 enabled to be a correspondent node as per [\[RFC3775\]](#). Type 1 CNs can receive route optimized traffic from mobile access gateways serving their mobile nodes.

Type 2 Correspondent Node

A mobile node that is served by mobile access gateway. Route optimization is transparent to Type 2 CNs. Mobile access gateway provides both mobility and route optimization services to Type 2

CNs.

[3.](#) PMIPv6 R0 Scenarios and Overview

[3.1.](#) PMIPv6 R0 Scenario Analysis

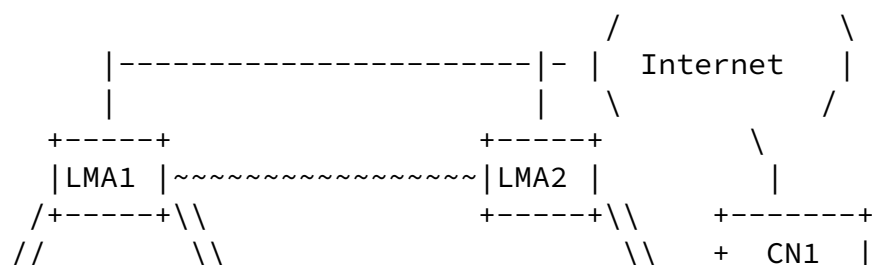
There are many possible scenarios due to the different location and capability of correspondent node (see Figure 1):

- o Case #1 : MN and CN attach to the same MAG and they belong to the same LMA.
- o Case #2 : MN and CN attach to the same MAG but they belong to different LMAs.
- o Case #3 : MN and CN attach to different MAGs, but they have the same LMA.
- o Case #4 : MN and CN attach to different MAGs, and they have different LMAs.
- o Case #5 : A MN is in the PMIPv6 domain and initiates route optimization procedures with a CN that is outside of the PMIPv6 domain, e.g. CN1 in Figure 1. In this case, the CN MUST support route optimization procedures defined in this document.

In Cases #1 through #4, the CN is a Type 2 CN. The MAG of the CN is involved with route optimization protocol. In Scenario #5, the CN is a Type 1 CN. The MAG of the MN has to negotiate with the CN directly. The route optimization mechanism should concern about the CN's security requirement.

Cases 1 and 2 do not require any signaling between PMAs and packets can be locally routed. As such, these cases are covered in the base specification [[I-D.ietf-netlmm-proxymip6](#)].

The protocol defined in [Section 5](#) covers Cases #3 and #4. PMIPv6 R0 Protocol for Scenario Case #5 is defined in [Section 4](#). For Cases #3 and #4, IPv4 transport network is supported.



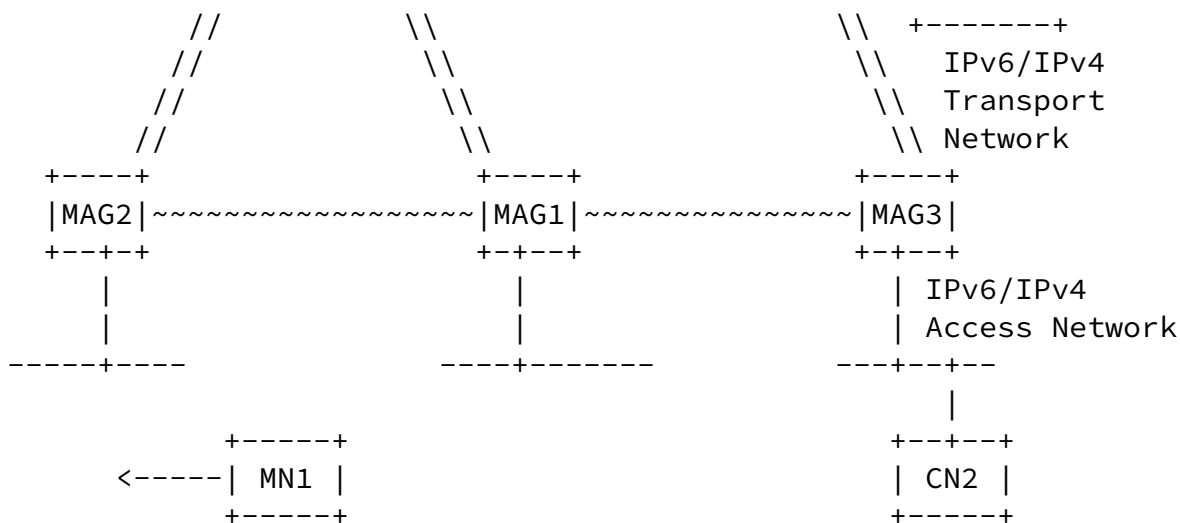


Figure 1: Route Optimization Scenarios in PMIPv6

3.2. PMIPv6 RO Overview

This document describes a route optimization protocol for PMIPv6. For Scenarios case #3 and case #4, specialized signaling can be defined between mobility access gateways or between local mobility anchors and mobility access gateways to setup and maintain route optimization states for MN and CN. However such an approach does not exploit the existing route optimization protocol defined for Mobile IPv6 in [RFC3775]. For Scenarios case #3, #4 and #5, return routability test procedures of Mobile IPv6 can be adopted to PMIPv6 route optimization. However such an approach does not leverage the enhancements to the return routability test procedures defined for Mobile IPv6 in [RFC4866]. Therefore, the protocol defined in this document for PMIPv6 route optimization is based on Enhanced Route Optimization for Mobile IPv6.

Once a mobile node enters its Proxy Mobile IPv6 domain, mobile access gateway which runs on the access router does the mobility related signaling on behalf of the mobile node. In MIPv6, a mobile node may determine when and which correspondent node needs route optimization. In contrast, in this document, such determination is done by the mobile access gateway according to some policies. The configuration of such policies is out of scope.

As soon as mobile access gateway makes decision on which correspondent node needs route optimization, mobile access gateway initiates proxy home test procedure depicted in [Section 4.1](#). Correspondent nodes verify the reachability of home address via this procedure.

Correspondent nodes also need to verify the reachability of care-of address. Proxy care-of test init message is piggybacked on a proxy binding update message which is sent by mobile access gateway on behalf of the mobile node to register with a correspondent node. After the first round trip of proxy binding update exchange is over between a correspondent node with mobile access gateway, the correspondent node sets up a binding cache entry and MAY start routing packets directly to care-of address of the mobile node even though the care-of address is not verified. However, the mobile access gateway obtains care-of keygen token via this round trip of proxy binding update exchange [[RFC4866](#)].

The mobile access gateway MAY initiate another proxy binding update exchange. Thus, the correspondent node MAY authenticate this proxy binding update with both temporary home keygen token and care-of keygen token, and then it makes sure of the validity of proxy binding cache entry created by early proxy binding update exchange. In order to protect against redirection-based flooding attacks, Credit-Based Authorization (CBA) can be exploited as described in [[RFC4866](#)].

During handover, the next mobile access gateway simulates home link for the mobile node. For the sake of security, proxy home test should be executed over again for correspondent node to verify the reachability and validity of home address of MN. In order to reduce handover latency brought up with the proxy home test, handover home keygen token is introduced in [Section 4.3](#). Handover home keygen token is used to eliminate the home test (PHoTI-PHoT exchange) at the next mobile access gateway because the correspondent node can authenticate early proxy binding update message sent by the new MAG using the shared handover home keygen token.

In PMIPv6 route optimization protocol, the proxy home test and proxy care-of test exchanges are initiated by MAG instead of MN. However, both the source address of proxy home test init message and the

destination address of proxy home test message are home address of

mobile node. So, the destination mobile access gateway MUST identify, intercept and process the proxy home test init message and the source mobile access gateway MUST identify, intercept and process the proxy home test message.

For the sake of security, cryptographically generated home addresses and permanent home keygen token, defined in [RFC4866], are used in PMIPv6 route optimization (PMIPv6R0) protocol. Cryptographically generated home addresses, CGA parameters and signature are calculated with the mobile node's public key and private key by each MAG the mobile node visits. The input parameters to the CGA calculations [RFC3972] like the subnet prefix, public key and private key are available to each MAG. One possible mechanism is context transfer from the previous MAG.

4. PMIPv6 Route Optimization for Type 1 Correspondent Nodes

4.1. Proxy Home Test Procedure

Proxy Home Test procedure validates the home address. It includes two messages as follows:

Proxy Home Test Init (Proxy HoTI)

Proxy Home Test (Proxy HoT).

Since the destination address of Proxy HoT message is the home address of MN, the destination MAG MUST intercept and process Proxy Home Test message instead of forwarding it to MN.

When handoff occurs, correspondent nodes must re-verify the reachability of home address by initiating the proxy home test. The next mobile access gateway MAY also initiate the proxy home test. Mobile access gateway MUST keep correspondent nodes list in its Binding Update List. When MN roams into the next MAG, the entries in the Binding Update List on MN identity like NAI, private and public keys, etc. SHOULD be transferred to the next MAG.

As shown in Figure 2, the mobile access gateway imitates the Mobile IP client of the mobile node. The Proxy Home Test Init (PHoTI) message is sent from MAG to the correspondent node, and it should be transmitted via the shared tunnel between the local mobility anchor and MAG.

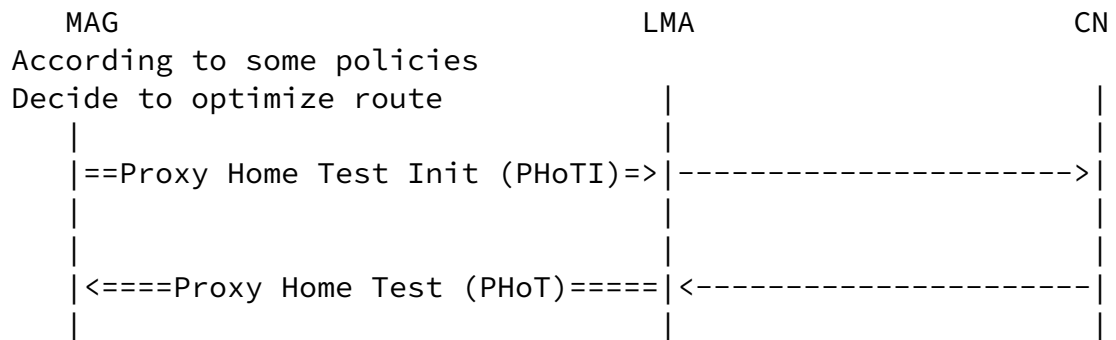


Figure 2: Proxy Home Test Procedure

4.2. Concurrent Proxy Care-of Test

Correspondent nodes also need to prove the reachability of care-of address. In this document, since the care-of test is initiated by mobile access gateway instead of by mobile node, we call it as proxy care-of test procedure.

The early PBU is a PBU which does not carry the care-of keygen token. A complete PBU follows up an early PBU after receiving a PBA message with a Care-of Test option as shown in Figure 3.

a) As a Type 1 CN receives an early PBU message which contains HoA option, Care-of Test Init option, the CGA Parameters and Signature options, it returns PBA message containing a care-of keygen token in Care-of Test option.

b) The MAG initiates complete proxy binding update exchange by sending a PBU message. CN authenticates this proxy binding update with both temporary home keygen token generated during proxy home address test procedure and care-of keygen token. CN also validates the proxy binding cache entry created by early proxy binding update exchange and then sends a complete PBA as a reply.

The MAG calculates CGA parameters and signature option according to MN's home address. MAG sends CGA parameters and signature in a complete proxy binding update message to acquire permanent home keygen token from the correspondent node in a PBA. MAG adds the permanent home keygen token to the binding update list entry for the correspondent node. The approach leverages the mechanism specified in [section 4 in \[RFC4866\]](#).

Internet-Draft

PMIPv6 Route Optimization

November 2007

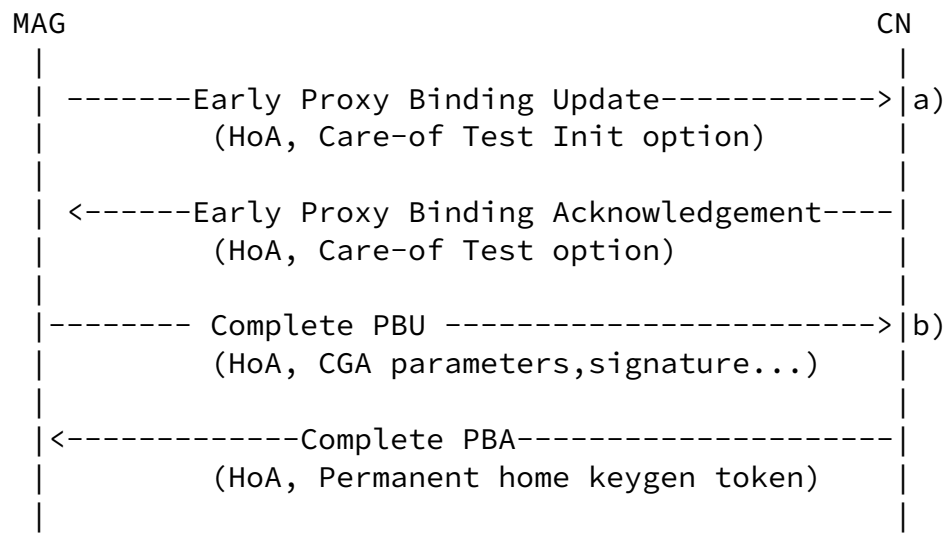


Figure 3: Concurrent Proxy Care-of Test

4.3. Handover

When handoff occurs, proxy care-of address changes. CN must re-verify the reachability of home address. The next MAG MAY also initiate the proxy home test. Handover home keygen token is used to authenticate early PBU originated from the next MAG, after handover home keygen token is transferred from the previous MAG to the next MAG. Eliminating proxy home test procedure makes the protocol more efficient by reducing the handover latency.

The handover procedure is depicted in Figure 4 and the steps are explained below.

a) If the previous MAG forecasts the forthcoming handover of the MN via layer 2 indication, the previous MAG MAY transfer context which includes HoA, CN addresses and corresponding handover home keygen tokens to the next MAG proactively. If the MN accessed to the next MAG before the context is transferred, the case is a reactive case. In reactive handover, as soon as the next MAG detects the attachment of the MN, the MAG requests the private key and other pertinent parameters from the previous MAG if the previous MAG is known. MAG MAY also obtain the private key during the authentication procedure.

- b) After the MN left the previous MAG, the previous MAG deregisters the Binding Cache Entry with correspondent nodes. From this point on, the CN does not renew the permanent home keygen token but reserves the handover home keygen token for further use.
- c) After the next MAG obtains handover home keygen token from the previous MAG, it sends out early proxy binding update piggybacked by care-of test init option to correspondent nodes. At this moment, the

MAG calculates the Binding Authorization Data option field of early proxy binding update message with handover home keygen token and care-of keygen token which is set to ZERO.

- d) The next MAG renews the permanent home keygen token and handover home keygen token via complete proxy binding update exchanges.

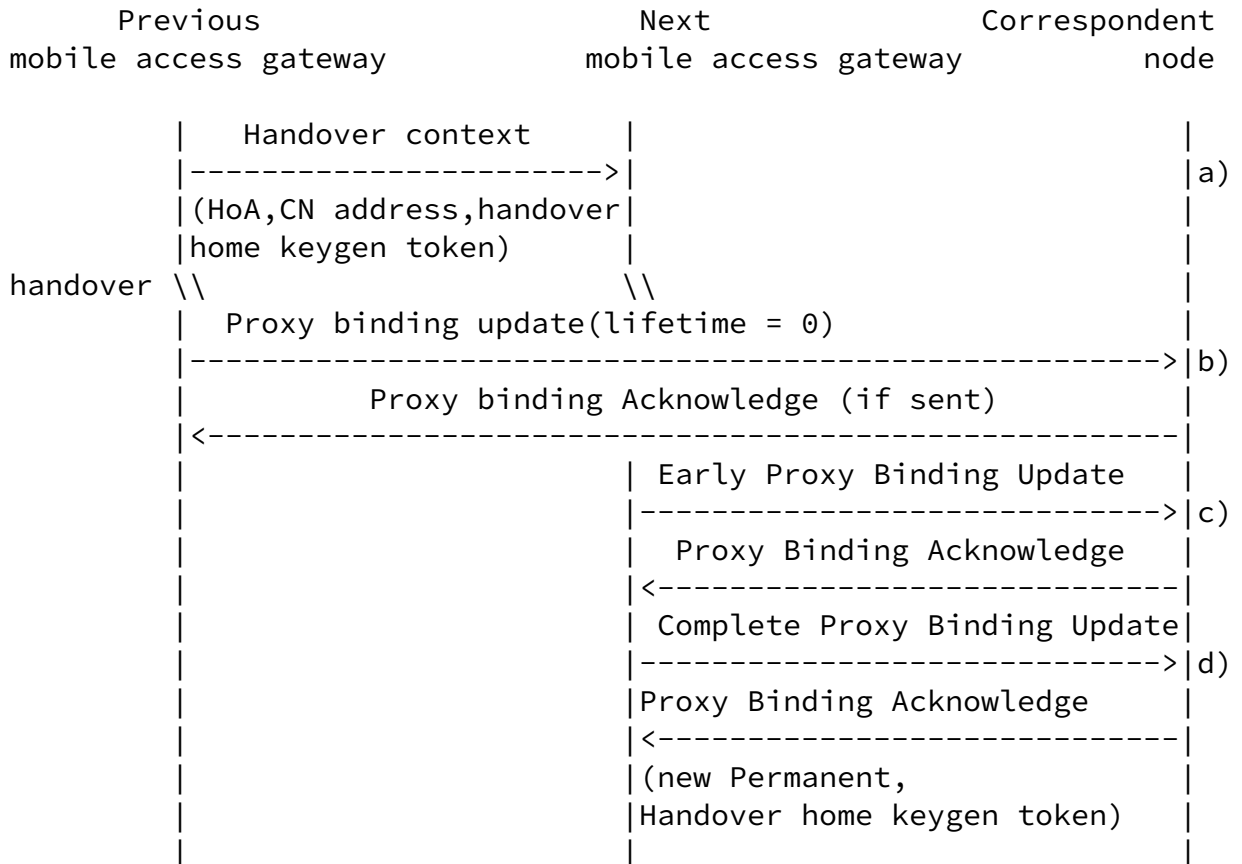


Figure 4: Route Optimization during Handover Procedure

4.4. Complete Proxy Binding Update

A complete proxy binding update is a proxy binding update defined in [[I-D.ietf-netlmm-proxymip6](#)]. After proxy binding update which piggybacks care-of test exchanges is finished, a complete proxy binding update must be done. The Binding Authorization Data option field of the complete proxy binding update is calculated by care-of keygen token for correspondent nodes to verify the reachability of care-of address and authenticate the legitimacy of the MAG which is sending this message on behalf of MN. The complete proxy binding update is exchanged as depicted in Figure 5.

Complete PBU message must be sent with CGA parameters and signature option for the mobile access gateway to request permanent home keygen token and handover home keygen token from the correspondent node. A

CGA provides a strong binding between its interface identifier and the CGA owner's public key. This enables other nodes to securely authenticate the CGA owner. Depending on the strong security brought up with cryptographically generated home addresses, lifetime of binding is extended to a longer period than 7 minutes [[RFC3775](#)]. Except for the initial test, the subsequent home tests every 7 minutes are no longer needed.

The correspondent node MUST authenticate the complete proxy binding update message based on the CGA property of the mobile node's home address. If the mobile access gateway has only temporary home keygen token, and then the mobile access gateway uses it to calculate the Binding Authorization Data option for the complete proxy Binding Update message.

If the mobile access gateway has permanent home keygen token, the mobile access gateway uses it to calculate the Binding Authorization Data option. The home nonce index is set to ZERO.

If the permanent home keygen token is required, both permanent home keygen token and handover home keygen token are generated and encrypted with the mobile access gateway's public key. Both of the two tokens are transferred from correspondent node to the next mobile access gateway via the proxy binding acknowledgement response to the complete proxy binding update message. This new handover home keygen

token will be exploited when the next handover occurs.

The PBA MAY be protected by CGA property of correspondent nodes.

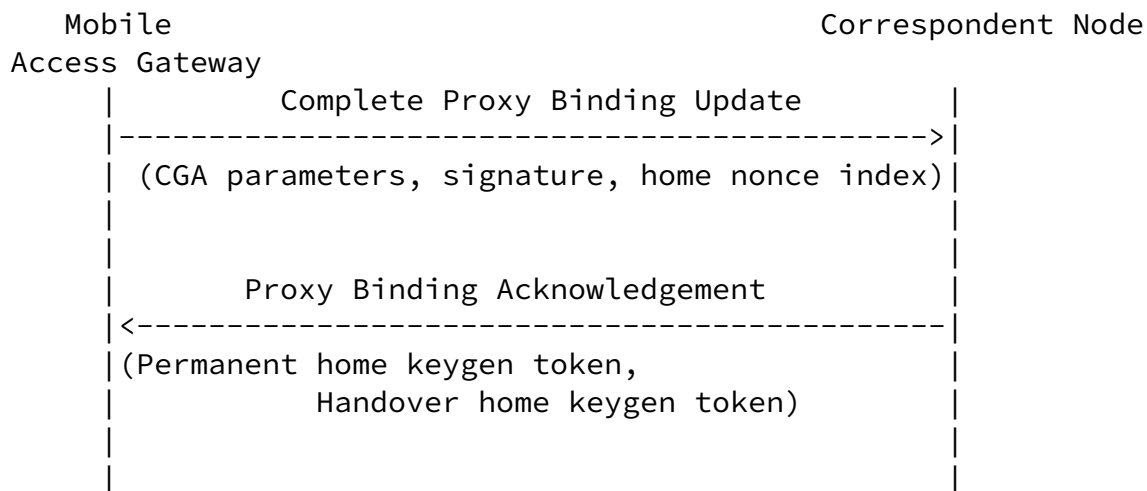


Figure 5: Complete Proxy Binding Update

5. PMIPv6 Route Optimization for Type 2 Correspondent Nodes

This section describes route optimization procedure for correspondent nodes that are served by mobile access gateways.

If a mobile access gateway provides mobility service for correspondent nodes, PMIPv6 Route Optimization protocol could be used for such correspondent nodes, as long as the mobile access gateway intercepts and processes route optimization extensions by looking over the MH types and distinguishing Proxy Mobile IP signaling from data.

The process for Scenario case #4 is shown in Figure 6. The proxy home test init message is transmitted over the shared tunnel between mobile access gateway and local mobility anchor of mobile node. This proxy home test init message is forwarded to home address of the correspondent node by LMA. At the local mobility anchor of the correspondent node, this message is tunnelled into the shared tunnel

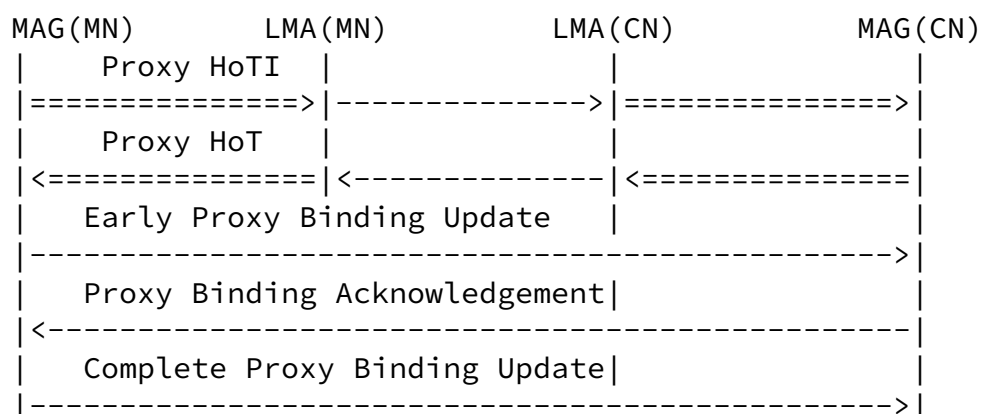
between the home agent of correspondent node and the mobile access gateway of the correspondent node.

The mobile access gateway of CN intercepts proxy home test init message and extracts MN's home address and care-of address from PHoTI. MAG of CN sends a proxy home test message back to MAG of MN and adds care-of address of CN into PHoT message. MAG of CN creates a Binding Cache entry for this MN. PHoT is transmitted over the shared tunnel between MAG of CN and LMA of CN. LMA of CN forwards this message to the home address of MN which tunnels it to MAG of MN.

MAG of MN receives PHoT message, it extracts the care-of address of CN and adds this information to the Binding Cache entry for CN. MAG of MN next starts care-of test signaling by sending an early binding update message directly to the care-of address of CN, i.e. to MAG of CN.

Due to the address exchange using PHoTI and PHoT messages, care-of test signaling in Figure 6 MUST NOT be started in parallel to home test signaling.

Since the mobile access gateway is sending PBA on behalf of the correspondent node, that mobile access gateway SHOULD use the correspondent node's CGA property to protect PBA.



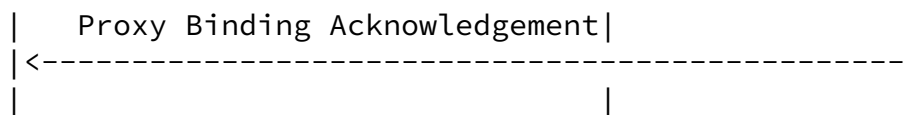


Figure 6: Route Optimization for Type 2 Correspondent Nodes

Scenario case #3 route optimization is a simpler case of Figure 6. LMA of MN has to re-encapsulate each packet and send it in MAG-LMA tunnel of CN's MAG and back in MAG-LMA tunnel of MN's MAG.

5.1. IPv4 support

The typical IPv4 transport network scenario is as follows: both the MN and the CN, located in PMIP domains, are IPv6-enabled nodes, allocated IPv6 addresses and being served by dual-stack MAGs. The transport network between the LMA and the MAG is an IPv4 network.

Initially, both MN and CN configure IPv4 home addresses by exchanging PBU/PBA as explained in [[I-D.ietf-netlmm-pmip6-ipv4-support](#)]. In Scenario case #3, MAG of MN starts RO signaling by sending PHoTI message to CN in IPv4 tunnel established between MAG and LMA of MN. MAG of MN MUST add IPv4 care-of address of MN into the care-of address field of PHoTI. LMA removes IPv4 header and looks at the destination address of inner header. LMA finds MAG address of this CN and sends PHoTI in IPv4 tunnel between MAG and LMA of CN. PHoTI message sent from MAG to LMA is shown at Figure 7:

PHoTI message:

```

IPv4 header (src=MAG of MN's IPv4 P.CoA, dst=IPv4 LMAA)
  IPv6 header (src=MN's IPv6 HoA, dst=IPv6 HoA of CN)
    Mobility header
      - Proxy HoTI
      IPv4 care-of address of MN
    Mobility Options
  
```

Figure 7: PHoTI message

MAG of CN sends a PHoT message as a reply. PHoT message is sent in IPv4 tunnel to LMA encapsulated in an IPv4 header. MAG of CN must add IPv4 care-of address of CN into the care-of address field of PHoT. PHoT message gets routed to MN. MAG of MN MUST obtain IPv4

address of CN from PHoT message's care-of address field. This establishes direct route between MN and CN.

PHoT message:

- IPv4 header (src= MAG of CN's IPv4 P.CoA, dst= IPv4 LMAA)
- IPv6 header (src=MAG of CN's IPv6 P.CoA, dst=IPv6 HoA of MN)
- Mobility header
 - PHoT
- IPv4 care-of address of CN
- Mobility Options

Figure 8: PHoT message

In Scenario case #4, after receiving PHoTI message, LMA of MN needs to map IPv6 home address of CN to either IPv4 address of CN's LMA or IPv4 home address of CN. One possible solution is that MAG of MN includes IPv4 home address of CN in PHoTI message. LMA of MN then sends pHoTI message in an IPv4 tunnel to CN which is received by LMA of CN. LMA of CN processes PHoTI exactly like LMA of CN did in Scenario case #3 and sends the message to MAG of CN.

MAG of CN sends a PHoT message as a reply. PHoT message is sent in IPv4 tunnel to LMA of CN encapsulated in an IPv4 header. MAG of CN must add IPv4 care-of address of CN into the care-of address field of PHoT. MAG of CN must also add IPv4 address of MN into the care-of address field of PHoT. PHoT message gets routed to MN. MAG of MN MUST obtain IPv4 address of CN from PHoT message's care-of address field. This establishes direct route between MN and CN.

For supporting IPv4 private address space, NAT detection Option is required from the DSMIP6 specification [[I-D.ietf-mip6-nemo-v4traversal](#)]. For the NAT handling, UDP header MUST be always used for the proxy binding update. These operations are defined in [[I-D.ietf-netlmm-pmip6-ipv4-support](#)].

6. Local Mobility Anchor Considerations

The local mobility anchor MUST drop all HoTI messages received from a home address that has corresponding Binding Cache entry with the proxy registration flag set. The local mobility anchor MUST forward all Proxy HoTI messages received from a home address that has corresponding Binding Cache entry with the proxy registration flag

set.

7. Mobile Access Gateway Considerations

MAG, after successful Home and Care-of Test exchanges, creates a Binding Cache entry for the correspondent node or MAG of the correspondent node. For each mobile node, the Binding Cache contains one entry for each correspondent node. After handover, context transfer procedure and PBU with lifetime set to zero exchanges are finished, the previous MAG deletes the Binding Cache entry and deregisters MN with all its correspondent nodes.

MAG MUST maintain a Binding Update List for each MN. The fields are as defined in [\[RFC3775\]](#) and with extensions defined in [\[I-D.ietf-netlmm-proxymip6\]](#). For each MN for which route optimization service is offered, the list in addition MUST contain the private and public keys of MN as well as the permanent home keygen token and handover home keygen token. Apart from home registrations as in [\[I-D.ietf-netlmm-proxymip6\]](#), Binding Update List contains correspondent registrations for route optimization.

After handover, correspondent registration entries in the Binding Update List SHOULD be transferred to the next MAG except for the permanent home keygen token. Such a transfer provides continuity of correspondent registrations for route optimization. The next MAG refreshes such registrations only after lifetime expiry.

MAG MUST maintain a Binding Cache if it has Type 2 CNs. Binding cache entries are created when MAG receives a home test init message. This Binding Cache is called Proxy Binding Cache.

From the correspondent nodes MAG receives data packets with Type 2 routing header. Type 2 routing header MUST conform to the structure given in [Section 6.1.5 of \[RFC3775\]](#). MAG MUST process the packet as follows: MAG replaces the source address with the home address given in Type 2 routing header. MAG removes Type 2 routing header. MAG sends the packet to MN.

8. Correspondent Node Considerations

This section states the differences in the behaviour of a correspondent node that conforms to [Section 9 of \[RFC3775\]](#) and [\[RFC4866\]](#).

Upon receiving a Proxy Home Test Init message, Early Proxy Binding

node verifies the following: The packet MUST NOT include a Home Address destination option. The correspondent node MUST silently ignore such packets.

Correspondent nodes MUST have a handover home keygen token in the binding cache entry for each mobile node they are involved in route optimized communication.

After a successful Home and Care-of Test exchanges, the correspondent node creates a Binding Cache entry for the mobile access gateway proxying the mobile node. The entry MUST be deleted after the expiration of its lifetime or after receiving a proxy binding update message which deregisters the mobile node.

Correspondent node MUST receive route optimized data packets from MAG encapsulated in IP-in-IP encapsulation. Source address of the outer header MUST be equal MAG's egress interface address and MUST match the Binding Cache entry. CN MUST remove the outer header before passing the packet to the upper layers.

CN MUST use Type 2 routing header in outgoing packets to MAG. The destination address is MAG's egress interface address which serves as Care-of address for the mobile node and the type 2 routing header contains MN's home address.

[9.](#) Requirements on PMIPv6 Handover/Context Protocol

PMIPv6 RO Protocol has the following requirements on PMIPv6 Handover/Context Transfer protocol: Context transfer from the previous MAG to the next MAG SHOULD include:

HoA of MN, Home Network Prefix (HNP) of MN,

Address of each CN and handover home keygen token from the Binding Update list entry for this MN,

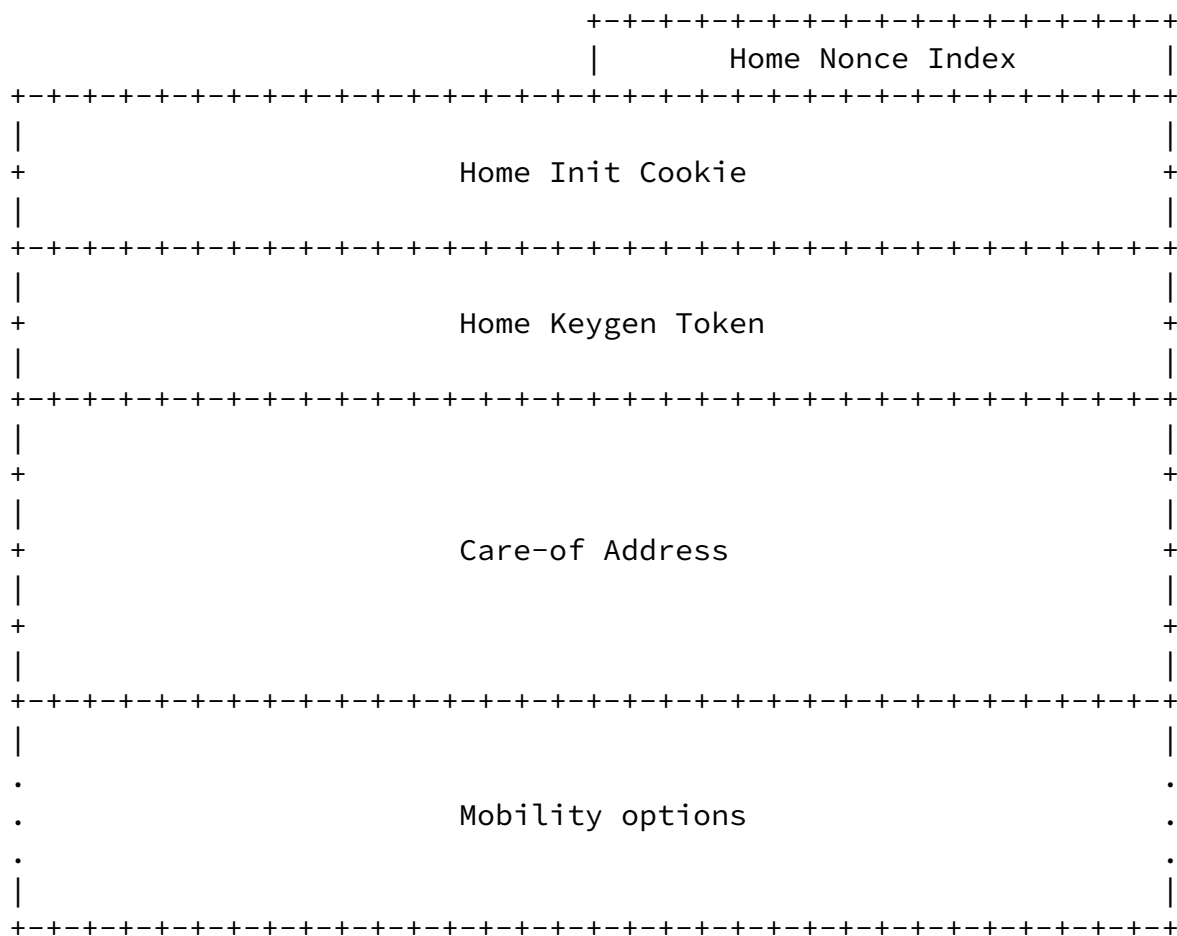
Permanent home keygen token,

Private and public key of MN.

10. Message Formats

This section defines extensions to the Proxy Mobile IPv6 [[I-D.ietf-netlmm-proxymip6](#)] protocol messages and the enhanced route optimization in MIPv6 protocol messages [[RFC4866](#)].

10.1. Proxy Home Test



A new MH type should be assigned by IANA.

Home Keygen Token

This field contains the 64 bit temporary home keygen token used to authenticate the proxy binding update.

This field contains the care-of address assigned to the CN by MAG. For descriptions of other fields present in this message, refer to [section 6.1.5 in \[RFC3775\]](#).

```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     | Reserved                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     | Home Init Cookie                         |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     |                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     |                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     | Care-of Address                         |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     |                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     |                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     | Mobility Options                         |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

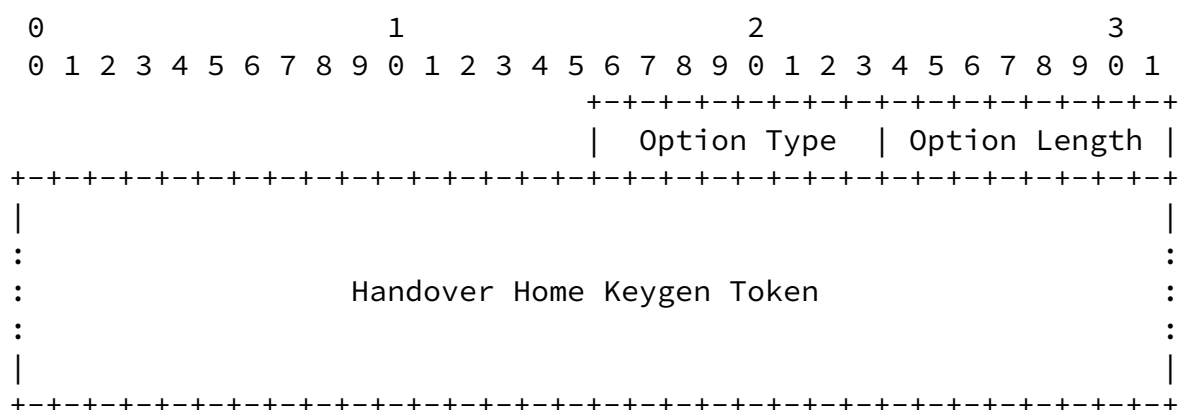
```

Care-of Address

This field contains the care-of address assigned to the mobile node by MAG.
 For descriptions of other fields present in this message, refer to [section 6.1.5 in \[RFC3775\]](#).

10.3. Handover Home Keygen Token option

Handover home keygen token is a mobility option. It is sent by CN in proxy binding acknowledgement message.



Option Type

8-bit identifier of the type of this mobility option. Its value is TBD by IANA.

Option Length

8-bit unsigned integer representing the length of the Handover Home Keygen Token field in octets.

Handover Home Keygen Token

This field contains the Handover home keygen token generated by the correspondent node. The content of this field MUST be encrypted with the mobile access gateway's public key. The length of the handover home keygen token is 8 octets before encryption. After it is encrypted, this field may be longer than 8 octets.

11. IANA Considerations

TBD.

12. Security Considerations

Security mechanism is very important in the route optimization process, especially for the proposal of establishing the tunnel between two mobile access gateways. In the case of route optimization without return routability, if mobile access gateway does not authenticate Proxy Binding Update and Proxy Binding Acknowledge messages, a malicious node may send such signaling messages to mobile access gateways to get the data packets destined for other nodes directed to itself.

In addition, when mobile access gateway sends data packets through the bi-directional tunnel between two mobile access gateways, corresponding MAG SHOULD examine the data packets to make sure there is a Binding Cache entry for the data source terminal.

Route optimization signaling between MAG of MN and CN specified in this document is based on [[RFC4866](#)] and use return routability with better security properties than the return routability of the base protocol [[RFC3775](#)].

Return routability signaling between two MAGs specified in this document is also based on [[RFC4866](#)] and has better security properties.

13. Acknowledgements

We would like to thank Dr. Vogt for his comments that have lead to many improvements in this document.

14. References

14.1. Normative References

[I-D.ietf-netlmm-pmip6-ipv4-support]

Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy

Mobile IPv6", [draft-ietf-netlmm-pmip6-ipv4-support-01](#)
(work in progress), July 2007.

- [I-D.ietf-netlmm-proxymip6]
Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K.,
and B. Patil, "Proxy Mobile IPv6",
[draft-ietf-netlmm-proxymip6-07](#) (work in progress),
November 2007.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support
in IPv6", [RFC 3775](#), June 2004.
- [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)",
[RFC 3972](#), March 2005.
- [RFC4866] Arkko, J., Vogt, C., and W. Haddad, "Enhanced Route
Optimization for Mobile IPv6", [RFC 4866](#), May 2007.

[14.2](#). Informative references

- [I-D.ietf-mip6-nemo-v4traversal]
Soliman, H., "Mobile IPv6 support for dual stack Hosts and
Routers (DSMIPv6)", [draft-ietf-mip6-nemo-v4traversal-05](#)
(work in progress), July 2007.
- [RFC4225] Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E.
Nordmark, "Mobile IP Version 6 Route Optimization Security
Design Background", [RFC 4225](#), December 2005.
- [RFC4449] Perkins, C., "Securing Mobile IPv6 Route Optimization
Using a Static Shared Key", [RFC 4449](#), June 2006.

Authors' Addresses

Behcet Sarikaya
Huawei Technologies USA
1700 Alma Dr. Suite 500

Plano, TX 75075

Email: sarikaya@ieee.org

Alice Qin
Huawei Technologies
No.91 BaiXia Rd.
Nanjing, Jiangsu 210001
China

Email: Alice.Q@huawei.com

Andy Huang
Huawei Technologies
No.91 BaiXia Rd.
Nanjing, Jiangsu 210001
China

Phone: +86-25-84565457
Email: hpanda@huawei.com

Wenson Wu
Huawei Technologies
No.91 BaiXia Rd.
Nanjing, Jiangsu 210001
China

Phone: +86-25-84565459
Email: sunseawq@huawei.com

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).

