

Mobility Extensions for IPv6  
(Mext)  
Internet-Draft  
Intended status: Standards Track  
Expires: September 14, 2011

W. Haddad  
Ericsson  
March 13, 2011

Enhancing Mobile IPv6 Route Optimization Mode with Secure Social  
Dimension  
draft-haddad-mext-mobisoc-04

## Abstract

This memo introduces the concept of peer-to-peer route optimization mode which enables Mobile IPv6 route optimization, without requiring mobility signaling messages exchange between two mobile endpoints. For this purpose, we use a social dimension within the home network as one tool to implement our concept.

## Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on September 14, 2011.

## Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in [Section 4.e](#) of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Conventions used in this document . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Motivation and Goal . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Protocol Description . . . . .	<a href="#">6</a>
<a href="#">5.</a>	New Options, Bits and Messages Formats . . . . .	<a href="#">8</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">9</a>
<a href="#">7.</a>	References . . . . .	<a href="#">10</a>
<a href="#">7.1.</a>	Normative References . . . . .	<a href="#">10</a>
<a href="#">7.2.</a>	Informative References . . . . .	<a href="#">10</a>
<a href="#">Appendix A.</a>	. . . . .	<a href="#">11</a>
Author's Address	. . . . .	<a href="#">12</a>

## 1. Introduction

This memo introduces the concept of "peer-to-peer (P2P)" route optimization (R0) mode which enables Mobile IPv6 ([\[I-D.ietf-mext-rfc3775bis\]](#)) route optimization, without requiring mobility signaling messages exchange between two mobile endpoints. For this purpose, we use a social dimension within the home network as one tool (among others), to implement our concept.

By limiting the scope to the home network, our suggested proposal can be applied only to mobile nodes using the same HA (or cluster of HAs). In this context, our tool enables two mobile endpoints which know each other "fairly" well (e.g., a la Facebook) to trigger the R0 mode without exchanging any mobility signaling messages on the direct path.

## 2. Conventions used in this document

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](#)].

### [3.](#) Motivation and Goal

It is important to start this section by highlighting an important observation related to the selected tool. In fact, neither the selected tool nor any other tool may be needed in order to implement P2P R0 mode (i.e., case where the decision to switch or not to the R0 mode is made only by the common HA). In fact, using the social variable provides a clear description of how P2P R0 mode could work in general.

Our tool selection is motivated by the stunning growth of social networking especially now that is becoming a desirable component and enabler for successful and attractive technologies.

It is also well known that the R0 mode enables a more efficient data packets exchange than the bidirectional tunneling and thus, should be applied whenever possible unless the mobile node (MN) is not interested in disclosing its topological location, i.e., care-of address (CoA), for the correspondent node (CN), e.g., for privacy reasons.

However, MIPv6 R0 mode requires exchanging a significant amount of

mobility signaling messages in order to establish, and periodically refresh a bidirectional security association (BSA) between the MN and the CN. While the mobility signaling exchange severely impacts the handoff latency, the BSA is needed to authenticate two particular messages only, namely the binding update (BU) and binding acknowledgement (BA) messages (although it can be argued that sending a BA is not mandatory). Note also that the amount of mobility signaling messages further increases when the CN is also mobile.

Our goal is to enable R0 mode between two mobile endpoints at minimum or no cost. This means that two mobile nodes should be able under some specific circumstances, e.g., if they both explicitly ask for it, to switch from BT mode to R0 mode without exchanging additional mobility signaling messages on the direct path nor through their HA. The immediate results are a much lower handoff latency to apply R0 mode and the absence of BSA.

#### [4.](#) Protocol Description

Our proposal enables two mobile users who are mutual friends, e.g., two "buddies", to translate their friendship at a network and device levels into a "bidirectional cryptographic relationship (BCR)". At some particular point, e.g., before or during an ongoing session, the two "buddies" confidentially disclose their BCR to their HA, in order to request implementing a fast "zero signaling message" R0 mode.

An important observation is to mention that expressing mutual friendship is by no means limited to establishing BCR between two or more "buddies". In this proposal, we use crypto-relationship only as an example to demonstrate how social networking can be used in order to optimize dual mobility.

To better clarify our ideas, we consider in the following, two mobile "buddies" using each its mobile device, i.e., MN1 and MN2. Our proposal requires the mobile nodes to use "cryptographically generated address (CGA)" technique (described in [[RFC3972](#)]), in order to compute and auto-configure their IPv6 home addresses. Note that using CGA in our context can also serve for authentication purposes between the MN and its HA, as described in [[I-D.laganier-mext-cga](#)]. We also assume that the two mobile devices have already established a bidirectional cryptographic relationship. For this purpose, the "Secure Neighbor Discovery" protocol ([[RFC3971](#)]) can be used. Appendix 1 describes how the BCR can be computed between the two mobile devices and the parameters sent by each MN to the HA, in order to disclose the BCR. It should be noted that the established BCR MUST be disclosed to the HA either before or during an ongoing session between the two mobile devices. In the following, we consider that the BCR is disclosed when MIPv6 handoff signaling is exchanged between each MN and its HA.

Let's consider that MN1 is the first to move to a foreign network. After configuring its CoA, MN1 sends a BU message to its HA. An explicit request to enabling P2P RO mode between the two mobile endpoints requires MN1 to disclose its BCR with MN2 to the HA. For this purpose, MN1 inserts BCR parameters related to MN2 in new options carried by the BU message. These parameters are then stored by the HA and a BA message is sent to MN1. No further action is required at this stage until MN2 moves to a foreign network.

When MN2 attaches to a foreign network, it explicitly requests from its HA a P2P RO mode service with MN1. This is done exactly in the same way as with MN1's request, i.e., by sending BCR parameters related to MN1 in the BU message sent to the HA. At this stage, the HA has all necessary BCR parameters to validate and act upon. Assuming that the claimed BCR between the two mobile nodes is valid,

the HA proceeds in two directions simultaneously. In the first one, it sends back a BA message to MN2 in which it inserts MN1's CoA (and potentially a selected list of flows that should be moved to the direct path). In another direction, the HA sends a new signaling message ("Neighbor Binding Update (NBU)") to MN1. NBU message carries MN2's new CoA (and the same list of flows which has been sent to MN2 in the BA message). After validating the NBU message, MN1 MUST send back a new message ("Neighbor Binding Acknowledgement

(NBA)") to the HA.

It becomes clear at this stage that both NBU and NBA messages will be authenticated using the same security mechanisms already in place between MN1 and its HA. This means that both messages are injected in the same IPsec tunnel established between the two nodes. Consequently, no additional security mechanism between the MN and its HA is required at any stage.

The inclusion of MN1's CoA in the BA message together with sending an NBU message to MN1 allow both mobile nodes to quickly learn each other's current topological location from a "trusted" source, and to create the necessary binding in order to immediately redirect their data packets on the direct path. As previously highlighted, such redirection does not require exchanging direct mobility signaling messages between the two MNs prior to exchanging data packets on the direct path. Hence, the return routability (RR) procedure is not needed anymore.

Note that in order to increase the overall performance, the HA can send multiple consecutive copies of the NBU messages until it receives a valid NBA message.

Subsequent BU messages sent to the HA and carrying new CoAs are processed in the same way as the first one as long as the selected flows (i.e., the one(s) that were moved to the direct path) are still active. This means that the HA should always simultaneously update the buddy node while acknowledging the BU message.

The suggested proposal can be extended to include multiple mobile nodes in which case the neighbor update(s) would consist of sending one or multiple NBU messages to the designated "buddies" nodes located outside the home network.



TBD

## 6. Security Considerations

This proposal aims to enhance the RO mode efficiency by removing the need for the return routability procedure. It should be noted that the RR procedure was carefully designed in order to mitigate a significant number of threats. Its main drawback was the amount of signaling messages which was needed between the MN and the CN. By removing the need for the RR procedure, these threats are also eliminated which in turn would significantly increase the overall security.

In MIPv6 protocol, there is one mandatory secure path between the MN and its HA and one trusted node, i.e., the HA. Our suggested mechanism introduces two new signaling messages which are exchanged between the MN and its HA over the secure path. Consequently, these two messages do not introduce any new threats as they are exchanged within the IPsec ESP tunnel established between the MN and its HA.

In addition to the encryption and integrity protection set up between the MN and the HA, there is also a mutual trust between the two nodes which provides insurance about the validity of the new messages content. However, the mutual trust between the MN and the HA does not propagate among mobile nodes sharing the same HA.

## [7.](#) References

### [7.1.](#) Normative References

[I-D.ietf-mext-rfc3775bis]

Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", [draft-ietf-mext-rfc3775bis-13](#) (work in progress), March 2011.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", [RFC 3971](#), March 2005.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", [RFC 3972](#), March 2005.

### [7.2.](#) Informative References

[I-D.laganier-mext-cga]

Laganier, J., "Authorizing Mobile IPv6 Binding Update with Cryptographically Generated Addresses", [draft-laganier-mext-cga-01](#) (work in progress), October 2010.

## Appendix A.

The required BCR between the two mobile nodes is used as a proof of mutual friendship. For this purpose, each unidirectional crypto-relationship can be generated as it follows:

When MN2 establishes a unidirectional crypto-relationship with MN1, it generates a 128-bit modifier from hashing MN1's public key together with a 128-bit random number (RAN):

$$\text{Modifier} = \text{First} [128, \text{SHA-2}(\text{PK}(\text{MN1}) \mid \text{RAN})]$$

MN2 confidentially notifies MN1 about the RAN used to generate its CGA address and MN1 stores the RAN together with MN2's CGA address. The same procedure is repeated by MN1 in order to compute its unidirectional relationship with MN2.

Each MN can confidentially share its own part of the BCR with its HA whenever needed (e.g., in order to request a P2P RO mode service). For this purpose, the "proof of friendship" is inserted in the first BU message sent by MN1 to its HA. Such proof consists of MN2's IPv6 address, public key and RAN. After CGA validation, the HA stores the crypto-relationship in the binding cache entry (BCE) created for MN1.

As already mentioned, when MN2 moves to a foreign network, it discloses its own crypto-relationship with MN1. At this stage, the HA can validate the BCR and take appropriate actions.

Haddad

Expires September 14, 2011

[Page 11]

---

Internet-Draft

MIPv6 R0 Mode Optimization

March 2011

Author's Address

Wassim Michel Haddad  
Ericsson  
300 Holger Dr  
San Jose, CA 95134  
US

Phone: +1 646 256 2030

Email: [Wassim.Haddad@ericsson.com](mailto:Wassim.Haddad@ericsson.com)

Haddad

Expires September 14, 2011

[Page 12]