

NETLMM Working Group
Internet-Draft
Expires: October 22, 2007

K. Weniger
G. Velez
Panasonic
April 20, 2007

Proxy Mobile IPv6 and Mobile IPv6 interworking issues
draft-weniger-netlmm-pmipv6-mipv6-issues-00

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 October 22, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Internet-Draft

PMIPv6-MIPv6 interworking issues

April 2007

Abstract

This document discusses issues that may arise if Proxy Mobile IPv6 and Mobile IPv6 are used together. Solutions for those issues are currently out of scope. The purpose of this document is to agree on a comprehensive list of interworking issues and to trigger the discussion of solutions.

Table of Contents

1.	Terminology	3
2.	Introduction	4
3.	List of PMIPv6-MIPv6 interworking issues	5
3.1.	Issue #1: Mobility mode selection	5
3.2.	Issue #2: MIPv6 de-registration Binding Update deletes PMIPv6 binding cache entry	5
3.3.	Issue #3: Race condition between Binding Update and Proxy Binding Update messages	5
3.4.	Issue #4: Mismatch of binding cache lookup key	6
3.5.	Issue #5: Use of wrong home agent or LMA after handover .	6
3.6.	Issue #6: Redirection attack against mobile nodes outside PMIP domain due to compromised MAG	6
4.	Security Considerations	8
5.	Acknowledgements	9
6.	References	10
6.1.	Normative References	10
6.2.	Informative References	10
	Authors' Addresses	11
	Intellectual Property and Copyright Statements	12

Internet-Draft

PMIPv6-MIPv6 interworking issues

April 2007

[1.](#) 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 [\[1\]](#).

Furthermore, the terminology defined in [\[2\]](#) and [\[3\]](#) is used.

2. Introduction

The NETLMM WG is standardizing Proxy Mobile IPv6 [3], a Mobile IPv6-based protocol for localized mobility management. This protocol allows the network to manage the mobility of mobile nodes, e.g., to enable IP mobility of nodes that do not implement Mobile IPv6. There are various scenarios, in which Mobile IPv6 (MIPv6) [2] and Proxy Mobile IPv6 (PMIPv6) can be used together. In [4], the following interworking scenarios are presented:

1. PMIPv6 and MIPv6 are used in a hierarchical manner. In this scenario, a mobile node's MIPv6-CoA equals the MN-HoA.
2. Transitioning between PMIPv6 and MIPv6. In this scenario, a mobile node's MIPv6-HoA equals the MN-HoA. Home agent and LMA are co-located.
3. Other co-existence of PMIPv6 and MIPv6 nodes in the same network, where neither MIPv6-CoA nor MIPv6-HoA equals MN-HoA. The home agent and LMA are typically co-located in this scenario and a mobility session of a specific mobile node is handled either exclusively by MIPv6 or exclusively by PMIPv6.

This draft intends to document all issues that may arise in any of these interworking scenarios. Issues specific to extensions of PMIPv6 or MIPv6 like IPv4 support, route optimization, MONAMI6 or NEMO etc. are currently out of scope of this document. Solutions for the issues are currently out of scope as well and may be specified in future versions of this document or in a companion document.

However, note that some of the interworking issues may be solvable by (pre-)configuration or may be handled at system-level by other SDOs.

[3.](#) List of PMIPv6-MIPv6 interworking issues

[3.1.](#) Issue #1: Mobility mode selection

This issue can arise in all interworking scenarios. [\[3\]](#) discusses that a MAG shall be able to announce the visited prefix to a MIPv6-enabled node instead of the home prefix, so that the mobile node can use MIPv6 to manage the mobility by itself. The issue is how the MAG can figure out which prefix to announce.

[3.2.](#) Issue #2: MIPv6 de-registration Binding Update deletes PMIPv6 binding cache entry

When the mobile node moves from a MIPv6 foreign network to the PMIPv6 home domain in scenario 2, the MAG registers the mobile node at the LMA by sending a Proxy Binding Update. Subsequently, the LMA updates the mobile node's binding cache entry with the MAG address and the MAG emulates the mobile node's home link. Upon detection of the home link, the mobile node will send a de-registration Binding Update to its home agent. According to [\[2\]](#), the home agent would delete the binding cache entry after accepting the de-registration Binding Update, i.e., it would delete the proxy binding cache entry that was

just established by the MAG. Hence, packets arriving at the LMA and destined for the mobile node would not be forwarded to the mobile node anymore.

3.3. Issue #3: Race condition between Binding Update and Proxy Binding Update messages

There are two variants of this issue, which apply to scenario 1 and 2, respectively. The fundamental reason for this issue is that MIPv6 and PMIPv6 use different mechanisms for handling re-ordering of registration messages and that they are sent by different entities. Whereas Binding Update messages are ordered by a sequence numbers and sent by the mobile node, Proxy Binding Update messages are ordered by a timestamp option and sent by MAGs.

The first variant of the issue can occur in scenario 2. Let's assume the mobile performs a handover from a MAG1 to a MAG2 in its PMIP home domain and shortly thereafter the mobile node moves out of the PMIP domain to an AR, where it configures a new MIPv6-CoA and sends a Binding Update message to its home agent. If now the Proxy Binding Update message from MAG2 is delayed so that it reaches the LMA after the Binding Update, the binding cache entry at the LMA would wrongly point to MAG2. Unless a new Binding Update is sent by the mobile node, packets are not forwarded to the mobile node, since the mobile node has already left MAG2. This may result in a significant packet loss. A similar situation can occur if the mobile node moves from

one AR to another and shortly thereafter enters the PMIP home domain.

A second variant of this issue can occur in scenario 1. When the mobile node enters a PMIP domain, it may configure a MIPv6-CoA and register this at its home agent before the Proxy Binding Update sent by the MAG reaches the LMA. This can happen, e.g., if the home prefix is announced to the mobile node before the MAG sends the corresponding Proxy Binding Update. In such case, packets arriving at the LMA are not forwarded to the mobile node until the Proxy Binding Update is received at the LMA, which may result in some packet loss.

3.4. Issue #4: Mismatch of binding cache lookup key

MIPv6 uses the home address as lookup key for the binding cache,

whereas PMIPv6 uses the NAI as lookup key. In some situations, the LMA may not even know the mobile node's home address. Hence, the LMA or home agent in scenario 2 may not be able to update the same binding cache entry when receiving both Binding Update and Proxy Binding Update messages. Consequently, two different binding cache entries for the same node may be created by the LMA or home agent, which may result in ambiguous forwarding entries and significant packet loss.

3.5. Issue #5: Use of wrong home agent or LMA after handover

This issues can arise in scenario 2 when multiple home agents and LMAs are deployed on the home link. If the mobile node moves from a MIPv6 foreign network to the PMIP home domain, the MAG must send the Proxy Binding Update to the particular LMA that is co-located with the home agent which maintains the active binding cache entry of the mobile node. If a different LMA is assigned to the MAG, packets addressed to the mobile node's home address do not reach the mobile node anymore. Similarly, if the mobile node moves from the PMIP home domain to a MIPv6 foreign network, the mobile node must send the Binding Update to the particular home agent that is co-located with the LMA which maintains the active proxy binding cache entry of the mobile node. If the mobile node selects a different home agent, packets addressed to the mobile node's home address do not reach the mobile node.

3.6. Issue #6: Redirection attack against mobile nodes outside PMIP domain due to compromised MAG

A MAG authorized to update the LMA's binding cache entry can update the entry of any mobile node registered at this LMA by sending a Proxy Binding Update with the mobile node's NAI. In deployment scenarios where an authorized MAG can be compromised by an attacker,

the attacker can redirect traffic for any mobile node in the PMIP domain to itself. Note that the mobile node does not need to be attached to the compromised MAG to allow this attack, i.e., this can be an off-path attack. In scenario 2, this threat is extended to MIPv6, because an authorized MAG must be able to modify a MIPv6 binding cache entry. Consequently, a compromised MAG can redirect traffic to itself which is destined for mobile nodes located outside the PMIP domain.

[4.](#) Security Considerations

This document only discusses issues that arise when combining two protocols. It does not propose any new mechanisms that require security considerations.

[5.](#) Acknowledgements

We would like to thank everybody that contributed to compiling the list of issue presented in this document. Many of the issues were presented by Gerardo Giaretta at the MIP6 WG during IETF#68 in Prague. The scenarios and some of the issues were mentioned by the authors of [\[3\]](#) and [\[4\]](#) in their documents or on the mailing list.

[6.](#) References

[6.1.](#) Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [2] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", [RFC 3775](#), June 2004.
- [3] Gundave, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", [draft-ietf-netlmm-proxymip6-00](#) (work in progress), April 2007.

[6.2.](#) Informative References

- [4] Devarapalli, V., Gundave, S., Chowdhury, K., and A. Muhanna, "Proxy Mobile IPv6 and Mobile IPv6 interworking", [draft-devarapalli-netlmm-pmipv6-mipv6-00](#) (work in progress), April 2007.

Internet-Draft

PMIPv6-MIPv6 interworking issues

April 2007

Authors' Addresses

Kilian A. Weniger
Panasonic R&D Center Germany
Monzastr. 4c
Langen 63225
Germany

Email: kilian.weniger@eu.panasonic.com

Genadi Velev
Panasonic R&D Center Germany
Monzastr. 4c
Langen 63225
Germany

Email: genadi.velev@eu.panasonic.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).