NETLMM Working Group G. Giaretta, Ed.
Internet-Draft Qualcomm
Intended status: Informational October 28, 2010
Expires: May 1, 2011

Interactions between PMIPv6 and MIPv6: scenarios and related issues
draft-ietf-netlmm-mip-interactions-07

Abstract

The use of Proxy Mobile IPv6 (PMIPv6) and Mobile IPv6 (MIPv6) in the same network requires some care. This document discusses scenarios where such mixed usage is appropriate and points out the need for interaction between the two mechanisms. Solutions and recommendations to enable these scenarios are also described.

Requirements Language

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 RFC 2119 [RFC2119].

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 May 1, 2011.

Copyright Notice

Copyright (c) 2010 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.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction

Proxy Mobile IPv6 (PMIPv6) [RFC5213] is a network based IP mobility protocol standardized by IETF. In some deployment scenarios this protocol will be deployed together with Mobile IPv6 (MIPv6) [RFC3775], for example with PMIPv6 as local mobility protocol and MIPv6 as global mobility protocol. While the usage of a local mobility protocol should not have implications of how global mobility is managed, since PMIPv6 is partially based on MIPv6 signaling and data structure, some considerations are needed to understand how the protocols interact and how the different scenarios can be enabled.

Some standardization fora are also investigating more complex scenarios where the mobility of some nodes is handled using Proxy Mobile IPv6, while other nodes use Mobile IPv6; or the mobility of a node is managed in turn by a host-based and a network-based mechanism. This needs also to be analyzed as a possible deployment scenario.

This document provides a taxonomy of the most common scenarios that require direct interaction between MIPv6 and PMIPv6. The list is not meant to be exhaustive. Moreover, this document presents and identifies most of the issues pertained to these scenarios and discusses possible means and mechanisms that are recommended to enable them.

2. Terminology

General mobility terminology can be found in [RFC3753]. The following acronyms are used in this document:

- o AR (Access Router): first hop router.

- o BCE (Binding Cache Entry): an entry of the MIPv6 or PMIPv6 Binding Cache.

- o LMA (Local Mobility Anchor): the PMIPv6 mobility anchor as specified in [RFC5213]

- o MAG (Mobility Access Gateway): the PMIPv6 client as specified in [RFC5213]

- o MN-HoA: the home address of a mobile node in a PMIPv6 domain.

- o MN-HNP: the IPv6 prefix that is always present in the Router Advertisements that the mobile node receives when it is attached to any of the access links in that PMIPv6 domain. MN-HoA always

belongs to this prefix.

- o MIPv6-HoA: the Home Address the MN includes in MIPv6 binding update messages.

- o MIPv6-CoA: the Care-of Address the MN includes in MIPv6 binding update messages.

3. Overview of the scenarios and related issues

Several scenarios can be identified where MIPv6 and PMIPv6 are deployed in the same network. This document not only focuses on scenarios where the two protocols are used by the same mobile node to manage local and global mobility, but also investigates more complex scenarios where the protocols are more tightly integrated or where there is a co-existence of nodes which do or do not implement MIPv6.

In particular the scenario space can be split into hierarchical deployments and alternative deployments of Mobile IP (MIP) and Proxy Mobile IP (PMIP). Hierarchical deployments are scenarios where the two mobility protocols are used in the same network in a hierarchical

manner for global and local mobility management. Alternative deployments are scenarios where only one of the two protocols is used for mobility management of a given mobile node.

The following hierarchical scenarios are identified:

Scenario A.1 - in this scenario PMIPv6 is used as a network based local mobility management protocol whereas MIPv6 is used as a global mobility management protocol. This interaction is very similar to the HMIPv6-MIPv6 interaction [RFC4140]; MIPv6 is used to manage mobility among different access networks, while the mobility within the access network is handled by PMIPv6. The address managed by PMIPv6 (i.e. the MN-HoA) is registered as Care-of Address by the MN at the HA. This means that the HA has a binding cache entry for MIPv6-HoA that points to the MN-HoA.

The following figure illustrates this scenario.

```
                           +-----+
                           | HA  |  MIPv6-HoA -> MN-HoA
                           +-----+
                             /\
                            /  \
             +-------------/----\--------------+
            (             /      \              ) Global Mobile IPv6
            (            /        \             ) Domain
             +----------/----------\-----------+
                       /            \
                    +-----+        +-----+
    MN-HoA -> MAG1  |LMA1|         |LMA2|
                    +-----+        +-----+
                     //\\              \\
```

```
               +----//--\\---+   +-----\\------+
              (    //    \\   ) (       \\      ) Local Mobility Network
              (   //      \\  ) (        \\     ) PMIPv6 domain
               +-//--------\\+   +--------\\---+
                //          \\             \\
               //            \\             \\
              //              \\             \\
           +-----+          +-----+         +-----+
           |MAG1|           |MAG2|          |MAG3|
           +-----+          +-----+         +-----+
             |                |               |
            [MN]
```

Figure 1 - Scenario A.1

Scenario A.2 - in this scenario the mobile node is moving across different access networks, some of them supporting PMIPv6 and some others not supporting it. Therefore the mobile node is roaming from an access network where the mobility is managed through a network-based solution to an access network where a host-based management (i.e. Mobile IPv6) is needed. This scenario may have different sub-scenarios depending on the relations between the MIPv6 home network and the PMIPv6 domain. The following figure illustrates an example of this scenario, where the MN is moving from an access network where PMIPv6 is supported (i.e. MAG functionality is supported) to a network where PMIPv6 is not supported (i.e. MAG functionality is not supported by the AR). This implies that the home link of the MN is actually a PMIPv6 domain. In this case the MIPv6-HoA is equal to the MN-HoA (i.e. the address managed by PMIPv6).


```
                         MIPv6-HoA == MN-HoA -> MAG1
                               +------+
                               |HA/LMA|-----------------------+
                               +------+                       |
                                 //\\                         |
                        +-------//--\\--------+               |
                       (       //    \\ PMIPv6 )              |
                       (      //      \\ domain)       +--------------+
```

```
                    +----//--------\\-----+       (   Non-PMIPv6   )
                        //          \\            (   domain       )
                       //            \\            +---------------+
                      //              \\                  |
                     +-----+          +-----+          +-----+
                     |MAG1|           |MAG2|           | AR |
                     +-----+          +-----+          +-----+
                       |                |                 |
                      [MN]
```

Figure 2 - Scenario A.2

In the scenario illustrated in Figure 2 the non-PMIPv6 domain can actually be also a different PMIPv6 domain that handles a different MN_HoA. The following figure illustrates this sub-case: the MIPv6-HoA is equal to the MN_HoA; however when the MN hands over to MAG3 it gets a different IP address (managed by LMA2 using PMIPv6) and registers it as a MIPv6 CoA.


```
          MIPv6-HoA == MN-HoA -> MAG_1
```

```
                              +--------+
                              |HA/LMA1|-----------------------+
                              +--------+                      |
                                //\\                       +-----+
                       +--------//--\\--------+            |LMA2|
                      (       //    \\  home  )            +-----+
                      (      //      \\ PMIPv6)       +------||-------+
                      (     //        \\domain)      (       ||visited)
                       +---//----------\\-----+      (       ||PMIPv6 )
                          //            \\           (       ||domain )
                         //              \\           +------||-------+
                      +-----+          +-----+             +-----+
                      |MAG1|           |MAG2|              |MAG3|
                      +-----+          +-----+             +-----+
                        |                |                   |
                       [MN]

                                        (a)

                       MIPv6-HoA -> MN_CoA
                              +--------+
                              |HA/LMA1|-----------------------+
                              +--------+                      |
                                //\\                       +-----+
                       +--------//--\\--------+            |LMA2|  MN_CoA -> MA
                      (       //    \\  home  )            +-----+
                      (      //      \\ PMIPv6)       +------||-------+
                      (     //        \\domain)      (       ||visited)
                       +---//----------\\-----+      (       ||PMIPv6 )
                          //            \\           (       ||domain )
                         //              \\           +------||-------+
                      +-----+          +-----+             +-----+
                      |MAG1|           |MAG2|              |MAG3|
                      +-----+          +-----+             +-----+
                        |                |                   |
                                                            [MN]

                                         (b)


                  Figure 3 - Scenario A.2 with visited PMIPv6 domain
```

The following alternative deployment has been identified:

Scenario B - in this scenario some mobile nodes use MIPv6 to manage their movements while others rely on a network-based mobility solution provided by the network as they don't support Mobile IPv6.

There may be a common mobility anchor that acts as MIPv6 Home Agent and PMIPv6 LMA, depending on the type of the node as depicted in the figure. However, the LMA and HA can also be separated and this has no impacts to the mobility of the nodes.

```
                                +---------+
                                 | HA/LMA |
                                 +---------+


                +-------+                                      +-------+
                | MAG1 |                                       | MAG2 |
                +-------+                                      +-------+


                           +------------+
                           | IPv6 host |    ------------------>
                           +------------+        movement
                        +-----------+
                        | MIPv6 MN |    ------------------>
                        +-----------+        movement
```

Figure 4 - Scenario B

Note that some of the scenarios can be combined. For instance, scenario B can be combined with scenario A.1 or scenario A.2.

The following sections describe some possible issues for each scenario. Respective recommendations are described in Section 4.3. The specifications considered as a baseline for the analysis are the following: [RFC3775], [RFC4877] and [RFC5213].

3.1. Issues related to scenario A.1

This scenario is very similar to other hierarchical mobility schemes, including a HMIPv6-MIPv6 scheme. No issues have been identified in this scenario. Note that a race condition where the MN registers the CoA at the HA before the CoA is actually bound to the MAG at the LMA is not possible. The reason is that per PMIPv6 specification the MAG does not forward any packets sent by the MN until the PMIPv6 tunnel is up, regardless the mechanism used for address allocation.

Section 4.1 describes one message flow in case PMIPv6 is used as a local mobility protocol and MIPv6 is used as a global mobility protocol.

3.2. Issues related to scenario A.2

This section highlights some considerations that are applicable to

scenario A.2.

1. HoA management and lookup key in the binding cache

   * In MIPv6 [RFC3775] the lookup key in the Binding Cache is the Home Address of the MN. In particular, the base specification [RFC3775] doesn't require the MN to include any identifier, such as the MN-ID [RFC4283], in the Binding Update message other than its Home Address. As described in [RFC4877], the identifier of the MN is known by the Home Agent after the IKEv2 exchange, but this is not used in the MIPv6 signaling, nor as a lookup key for the binding cache. On the other hand, as specified in [RFC5213], a Proxy Binding Update contains the Home Prefix of the MN, the MN-ID and does not include the Home Address of the MN (since it may not be known by the MAG and consequently by the HA/LMA). The lookup key in the binding cache of the LMA is either the home prefix or the MN-ID. This implies that lookup keys for MIPv6 and PMIPv6 registrations are different. Because of that, when the MN moves from its home network (i.e. from the PMIPv6 domain) to the foreign link, the Binding Update sent by the MN is not identified by the HA as an update of the Proxy Binding Cache Entry containing the home prefix of the MN, but a new binding cache entry is created. Therefore PMIPv6 and MIPv6 will always create two different binding cache entries in the HA/LMA which implies that the HA and LMA are logically separated. How to handle the presence of the two binding cache entries for the same MN is described in Section 4.2.

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, 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. It is necessary to make sure that the de-registration of the MIPv6 BU does not change the PMIPv6 binding cache entry just created

by the MAG.

3. Race condition between Binding Update and Proxy Binding Update messages (Sequence Numbers and Timestamps)

   * MIPv6 and PMIPv6 use different mechanisms for handling re-ordering of registration messages and they are sent by different entities. In MIPv6, Binding Update messages that are sent by the mobile node to the home agent are ordered by

the sequence numbers. The other side, in PMIP, Proxy Binding Update messages that are sent by the MAG to the LMA are ordered by a timestamp option. When the mobile node moves from one access where Mobile IP is used to another access when Proxy Mobile IP is used, delay in the mobility signaling sent may imply adverse situations. For example if the mobile node sends a Mobile IP binding update from access A before moving to access B and this binding update gets delayed (e.g. a refresh binding update), the binding update may reach the combined LMA/HA after the proxy binding update sent by the MAG, re-directing packets to access A even after the mobile has moved to access B.

4. Threat of compromised MAG

   * In MIPv6 base specification [RFC3775] there is a strong binding between the Home Address registered by the mobile node and the Security Association used to modify the corresponding binding cache entry.

   * In PMIPv6 specification, the MAG sends proxy binding updates on behalf of a mobile node to update the binding cache entry that corresponds to the mobile node's home address. Since the MAG sends the binding updates, PMIPv6 requires security associations between each MAG and the LMA.

   * As described in [RFC4832], in PMIPv6 the MAG compromise or impersonation is an issue. RFC4832, section 2.2, describes how a compromised MAG can harm the functionality of LMA, e.g. manipulating LMA's routing table (or binding cache).

   * In this mixed scenario, both host-based and network-based

security associations are used to update the same binding cache entry at the HA/LMA (but see the first bullet of this list, as the entry may not be the same). Based on this consideration, the threat described in [RFC4832] is worse as it affects also hosts that are using the LMA/HA as MIPv6 HA and are not using PMIPv6

3.3. Issues related to scenario B

In this scenario there are two types of nodes in the access network: some nodes support MIPv6 while some others do not. The rationale behind such a scenario is that the nodes implementing MIPv6 manage their own mobility to achieve better performance, e.g. for inter-technology handovers. Obviously, nodes that do not implement MIPv6 must rely on the network to manage their mobility: therefore Proxy MIPv6 is used for those nodes.

Based on the current PMIPv6 solution described in [RFC5213], in any link of the PMIPv6 domain the MAG emulates the mobile node's home link, advertising the home link prefix to the MN in a unicast Router Advertisement message. This ensures that the IP address of the MN is still considered valid by the MN itself. The home network prefix (and any other information needed to emulate the home link) is included in the mobile node's profile that is obtained by the MAG via context transfer or via a policy store.

However, in case there are nodes that implement MIPv6 and want to use this protocol, the network must offer MIPv6 service to them. In such case the MAG should not emulate the home link. Instead of advertising the MN-HNP, the MAG should advertise the topologically correct local IP prefix, i.e. the prefix belonging to the MAG, so that the MN detects an IP movement, configures a new CoA and sends a MIPv6 Binding Update based on [RFC3775].

4. Analysis of possible solutions

4.1. Solutions related to scenario A.1

As mentioned in Section 3.1, there are no significant issues in this scenario.

Figures 5 and 6 show a scenario where a mobile node is moving from one PMIPv6 domain to another, based on the scenario of Figure 1. In Figure 5, the mobile node moves from an old MAG to MAG2 in the same PMIPv6 domain: this movement triggers a PBU to LMA1 and the updating of the binding cache at the LMA1; there is no MIPv6 signaling as the CoA_1 registered at the HA is the Home Address for the PMIPv6 session. In Figure 6, the mobile node moves from MAG2 in the LMA1 PMIPv6 domain to MAG3 in a different PMIPv6 domain: this triggers the PMIPv6 signaling and the creation of a binding at the LMA2. On the other hand, the local address of the mobile node is changed, as the LMA has changed, and therefore the mobile node sends a MIPv6 Binding Update to the HA with the new CoA_2.


```
    +-----+                 +-------+            +-------+      +-----+
    | MN |                  | MAG2 |             | LMA1 |       | HA |
    +-----+                 +-------+            +-------+      +-----+
      |                        |                     |             |
      |                        |                     |   +------------------+
      |                        |                     |   |  HoA -> CoA_1    |
      |                        |                     |   | binding present  |
      |                        |                     |   +------------------+
      |                        |                     |             |
      | CoA conf/confirm |  PBU(CoA_1,MAG_2)   |             |
      | <---------------->|  ----------------->|             |
      |                        |           +------------------+|
      |                        |           | CoA_1 -> MAG_2   ||
      |                        |           | binding updated  ||
      |                        |           +------------------+|
      |                        |          PBA        |             |
      |                        |   <-----------------|             |
      |                        |                     |             |
```

Figure 5 - Local Mobility Message Flow

```
 +-----+                  +-------+               +-------+          +-----+
 | MN  |                  | MAG3  |               | LMA2  |          | HA  |
 +-----+                  +-------+               +-------+          +-----+

    |    CoA config       |  PBU(CoA_2,MAG_3)  |             |
    |<------------------->|------------------->|             |
    |                     |               +------------------+ |
    |                     |               | CoA_2 -> MAG_3   | |
    |                     |               | binding created  | |
    |                     |               +------------------+ |
    |                     |          PBA       |             |
    |                     |<-------------------|             |
    |                     |                    |             |
    |                     |  BU (HoA, CoA_2)   |             |
    |----------------------------------------------------->|
    |                     |                    |             |
    |                     |                    |     +------------------+
    |                     |                    |     |  HoA -> CoA_2    |
    |                     |                    |     | binding updated  |
    |                     |                    |     +------------------+
    |                     | BA                 |             |
    |<-----------------------------------------------------|
```

Figure 6 - Global Mobility Message Flow

4.2. Solutions related to scenario A.2

As described in Section 3.2, in this scenario the mobile node relies on PMIPv6 as long as it is in the PMIPv6 domain. The mobile node then uses MIPv6 whenever it moves out of the PMIPv6 domain which basically implies that the MIPv6 home link is a PMIPv6 domain.

Analyzing the issues described in Section 3.2, it is clear that most of them are applicable only to the case where there is a common binding cache entry for the PMIPv6 registration and the MIPv6 registration. The issue 1 on how the two protocols identify the

binding cache entry is valid only in case we assume that a PMIPv6 message has any value for a MIPv6 BCE. Also the issues 2 and 3 are not applicable in case different logical BCEs are used by the LMA and the HA. For this reason, it is recommended that when the MIPv6 home link is implemented as a PMIPv6 domain, the HA/LMA implementation treats the two protocol as independent.

More in details the following principles should be followed by the HA/LMA implementation:

o PMIPv6 signaling does not overwrite any MIPv6 BCE. In particular, when a PMIPv6 binding cache entry is created for a mobile node which has previously created a MIPv6 BCE, the MIPv6 binding cache entry of the MN is not overwritten and a new PMIPv6 binding cache entry is created.

o The downlink packets in the case where both the MIPv6 binding cache entry and PMIPv6 binding cache entry exist are processed as follows:

   1. The MIPv6 binding cache entry is processed first. If the destination address of the received downlink packet matches the the binding cache entry of the HA, the packet is forwarded by encapsulating it with the care-of-address contained in the BCE.

   2. If the destination address does not match the MIPv6 BCE, the binding cache entry created by PMIPv6 is applied and the packet are encapsualted to the registered MAG.

The following subsections provide a description of the procedures which will be followed by the mobile node and HA/LMA based on the above principles. The analysis is performed in two different subsections, depending if the mobile node moves from a PMIPv6 domain to a non-PMIPv6 domain or vice versa.

4.2.1. Mobility from a PMIPv6 domain to a non-PMIPv6 domain

Let's assume the mobile node is attached to a PMIPv6 domain and there is a valid Proxy Binding Cache entry at the LMA. Then the mobile

node moves to a different access network and starts using MIPv6 (e.g. because PMIPv6 is not supported). The mobile node needs to bootstrap MIPv6 parameters and send a MIPv6 Binding Update in order to have service continuity. Therefore the following steps must be performed by the UE:

- HA/LMA address discovery: the mobile node needs to discover the IP address of the LMA which has a valid binding cache entry for its home network prefix. This is described in Section 3.2 as issue 4.

- Security Association establishment: the mobile node needs to establish an IPsec Security Association with the HA/LMA as described in [RFC4877]

- HoA or home network prefix assignment: as part of the MIPv6 bootstrapping procedure the HA assigns a MIPv6 HoA to the MN. This address must be the same the mobile node was using in the PMIPv6 domain.

Since all these steps must be performed by the mobile node before sending the Binding Update, they have an impact on the handover latency experienced by the MN. For this reason it is recommended that the mobile node establishes the IPsec security association (and consequently is provided by the HA/LMA with a MIPv6-HoA) when it is initialized. This implies that the mobile node has MIPv6 stack active while in the PMIPv6 domain, but as long as it is attached to the same PMIPv6 domain, it will appear to the mobile node as if it is attached to the home link.

In order to establish the security association with the HA/LMA, the mobile node needs to discover the IP address of the LMA/HA while in the PMIPv6 domain. This can be done either based on DNS or based on DHCPv6, as described in [RFC5026] and [boot-integrated]. The network should be configured so that the mobile node discovers or gets assigned the same HA/LMA that was serving as the LMA in the PMIPv6 domain. Details of the exact procedure are out of scope of this document.

When the mobile node establishes the security association, it acquires a home address based on [RFC5026]. However, based on PMIPv6 operations, the LMA knows only the Home Network Prefix used by the mobile node and does not know the MN-HoA.For this reason, the mobile node must be configured to propose MN-HoA as the home address in the IKEv2 INTERNAL_IP6_ADDRESS attribute during the IKEv2 exchange with

the HA/LMA. Alternatively the HA/LMA can be configured to provide the entire Home Network Prefix via the MIP6_HOME_LINK attribute to the mobile node as specified in [RFC5026]; based on this Home Network Prefix the mobile node can configure a home address. Note that the security association must be bound to the MN-HoA used in the PMIPv6 domain as per [RFC4877]. Note that the home network prefix is shared between the LMA and HA and this implies that there is an interaction between the LMA and the HA in order to assign a common home network prefix when triggered by PMIPv6 and MIPv6 signaling

When the mobile node hands over to an access network which does not support Proxy Mobile IPv6, it sends a Binding Update to the HA. The mobile node may set the R bit defined in NEMO specification (implicit mode) [RFC3963]in order to indicate that the entire HNP is moved to the new CoA. A MIPv6 binding cache entry is created irrespective of the existing PMIPv6 BCE. Packets matching the MIPv6 binding cache entry are sent to the CoA present in the MIPv6 BCE. The PMIPv6 binding cache entry will expire in case the MAG does not send a refresh PBU.

4.2.2. Mobility from a non-PMIPv6 domain to a PMIPv6 domain

In this section it is assumed that the mobile node is in a non-PMIPv6 access network and it has bootstrapped MIPv6 operations based on [RFC5026]; therefore there is valid binding cache for its MIPv6-HoA (or HNP in case of NEMO) at the HA. Then the mobile node moves to a PMIPv6 domain which is configured to be the home link for the MIPv6-HoA the mobile node has been assigned.

In order to provide session continuity, the MAG needs to send a PBU to the HA/LMA that was serving the MN. The MAG needs to discover the HA/LMA; however the current version of [RFC5213] assumes that the LMA is assigned to the MAG or discovered by the MAG when the mobile node attaches to the MAG. the exact mechanism is not specified in [RFC5213]. A detailed description of the necessary procedure is out of the scope of this document. Note that the MAG may also rely on static configuration or lower layer information provided by the mobile node in order to select the correct HA/LMA.

The PBU sent by the MAG creates a PMIPv6 binding cache entry for the mobile node which is independent of the MIPv6 BCE. Traffic destined to the MIPv6-HoA (or to the HNP in case the mobile node had set the flag R in the last BU) is still forwarded to the CoA present in the MIPv6 BCE. When the mobile node wants to use the HoA directly from the home link, it sends a de-registration message and at that point only the PMIPv6 binding cache entry is present.

4.3. Solutions related to scenario B

The solution for this scenario depends on the access network being able to determine that a particular mobile node wants to use Mobile IPv6. This requires a solution at the system level for the access network and may require knowledge of the detailed configuration and software capabilities of every mobile node in the system. These issues are out of scope of this document

5. Security Considerations

Scenario A.1 does not introduce any new security issues in addition to those described in [RFC5213] or [RFC3775].

For scenario A.2, this document requires that the a home agent that also implements the PMIPv6 LMA functionality should allow both the mobile node and the authorized MAGs to modify the binding cache entries for the mobile node. Note that the compromised MAG threat described in [RFC4832] applies also here in a more severe form as explained in Section 3.2. Scenario B relies on the secure identification of mobile nodes and their capabilities so that the right service can be provided for the right mobile nodes. For instance, a malicious mobile node should not get the home address of some other node assigned to it, and a mobile node that desires to employ its own mobility management should be able to do so. The ability to identify nodes is already a requirement in [RFC5213], but scenario B adds a requirement on identification of node capabilities.

6. IANA considerations

This document has no IANA actions.

7. Additional Authors

Chowdhury, Kuntal - kchowdhury@starentnetworks.com

Hesham Soliman - Hesham@elevatemobile.com

Vijay Devarapalli - vijay.devarapalli@azairenet.com

Sri Gundavelli - sgundave@cisco.com

Kilian Weniger - Kilian.Weniger@googlemail.com

Genadi Velev - Genadi.Velev@eu.panasonic.com

Ahmad Muhanna - amuhanna@nortel.com

George Tsirtsis - tsirtsis@googlemail.com

Suresh Krishnan - suresh.krishnan@ericsson.com

8. Acknowledgements

This document is a merge of four different Internet Drafts: draft-weniger-netlmm-pmipv6-mipv6-issues-00, draft-devarapalli-netlmm-pmipv6-mipv6-01, draft-tsirtsis-logically-separate-lmaha-01and draft-giaretta-netlmm-mip-interactions-00. Thanks to the authors and editors of those drafts.

The authors would also like to thank Jonne Soininen and Vidya Narayanan, NETLMM WG chairs, for their support.

9. References

9.1. Normative References

[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.

[RFC3963] Devarapalli, V., "Network Mobility (NEMO) Basic Support Protocol", January 2005, <http://www.rfc-editor.org/rfc/rfc3963.txt>.

[RFC4140] Soliman, H., "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", August 2005, <http://www.rfc-editor.org/rfc/rfc4140.txt>.

[RFC4832] Vogt, C. and J. Kempf, "Security Threats to Network-Based Localized Mobility Management (NETLMM)", April 2007.

[RFC4877] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", 2005.

[RFC5026] Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

[RFC5213] Gundavelli, S., "Proxy Mobile IPv6", August 2008.

[boot-integrated] Chowdhury, K., Ed., "MIP6-bootstrapping for the Integrated Scenario", 2007.

9.2. Informative References

[RFC3753] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[RFC4283] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.

Author's Address

Gerardo Giaretta (editor)
Qualcomm

Email: gerardog@qualcomm.com