NETLMM Working Group
Internet-Draft
Intended status: Informational
Expires: May 18, 2008

G. Giaretta, Ed.
Qualcomm

November 15, 2007

Interactions between PMIPv6 and MIPv6: scenarios and related issues
draft-giaretta-netlmm-mip-interactions-02

Status of this Memo

Copyright Notice

Abstract

The scenarios where Proxy Mobile IPv6 (PMIPv6) and Mobile IPv6 (MIPv6) protocols interact with each other need special considerations. An analysis of all the scenarios that involve this interaction is necessary in order to provide guidelines to PMIPv6 protocol design and applicability. This document describes all identified possible scenarios, which require an interaction between PMIPv6 and MIPv6 and discusses all issues related to these scenarios. Solutions 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].

Table of Contents

1. Introduction

The NETLMM WG is chartered to standardize a network-based protocol for localized mobility management. The goals that must be fulfilled by the protocol design are listed in [RFC4831]. Proxy Mobile IPv6 [pmipv6-draft] has been designated as the network-based localized mobility management protocol.

There are two main reasons why the interactions between Proxy Mobile IPv6 and Mobile IPv6 need to be studied. The first reason is that Mobile IPv6 is the main global mobility management protocol developed in IETF; it is therefore worth investigating for example the details of a hierarchical mobility scheme where Proxy Mobile IPv6 is used for local mobility and Mobile IPv6 is used for global mobility.

The second reason is that Proxy Mobile IPv6 has been chosen by the NETLMM WG mainly for reusability grounds and a MIPv6 home agent can be extended to handle PMIPv6.

Moreover, based on these considerations, some SDOs are investigating complex scenarios where the mobility of some nodes are 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 document provides a taxonomy of all scenarios that require direct interaction between MIPv6 and PMIPv6. Moreover, this document presents and identifies all known issues pertained to these scenarios and discusses possible means and mechanisms that may be required to enable them.

2. Terminology

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

MN-HoA: the home address of a mobile node in a Proxy Mobile IPv6 domain.

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 Proxy Mobile IPv6 domain. MN-HoA always belongs to this prefix.

MIPv6-HoA: the Home Address the MN includes in MIPv6 binding update messages. Based on the scenario, MIPv6-HoA and MN-HoA may be the same or different.

MIPv6-CoA: the Care-of Address the MN includes in MIPv6 binding update messages. Based on the scenario, MIPv6-HoA and MN-HoA may be the same or different.

3. Overview of the scenarios and related issues

Several scenarios can be identified where Mobile IPv6 and Proxy Mobile IPv6 are used in the same network. This document does not only focus on scenarios where the two protocols are used by the same mobile node to manage local and global mobility, but it investigates also 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 Mobile IPv6.

The following scenarios were identified:

- Scenario A - in this scenario Proxy Mobile IPv6 is used as a network based local mobility management protocol whereas Mobile IPv6 is used as a global mobility management protocol. This interaction is very similar to the HMIPv6-MIPv6 interaction; Mobile IPv6 is used to manage mobility among different access networks, while the mobility within the access network is handled by Proxy Mobile IPv6. The address managed by PMIPv6 (i.e. the MN-HoA based on PMIPv6 terminology) 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.

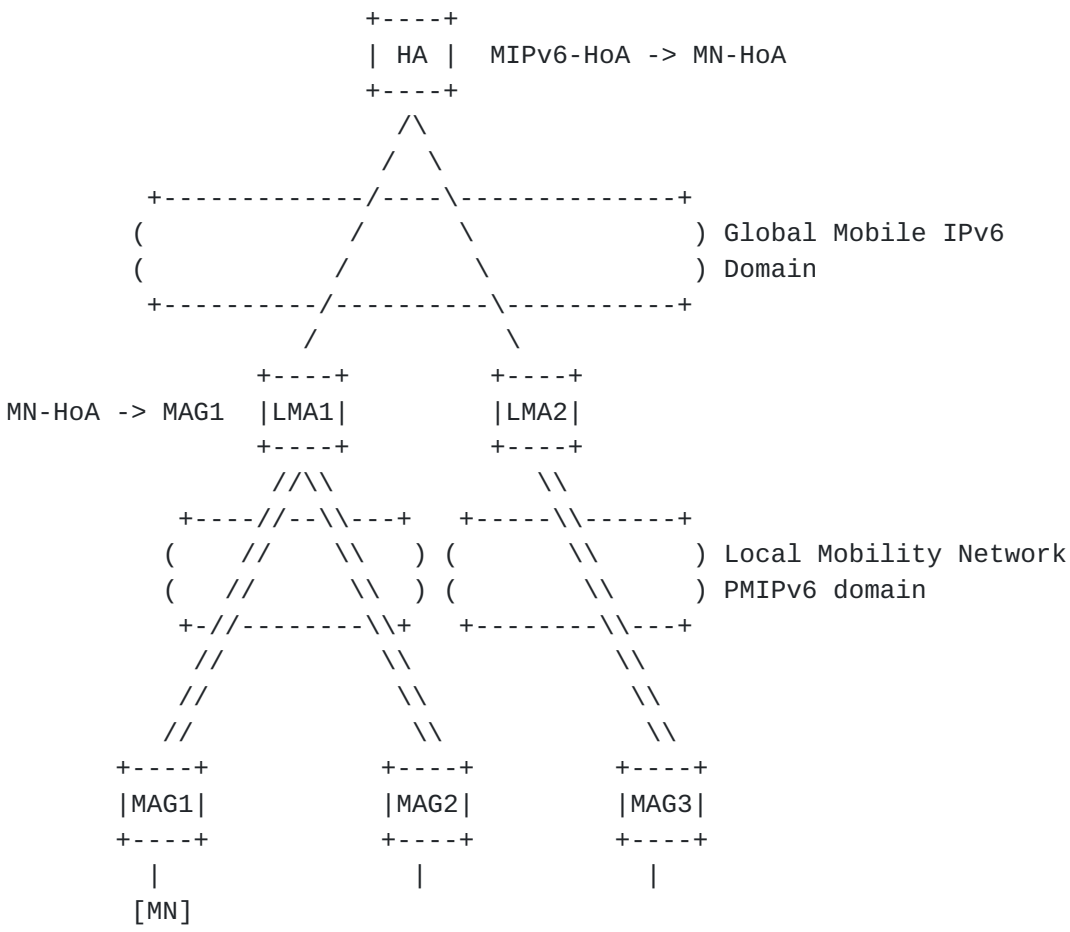


Figure 1 - Scenario A

o Scenario B - in this scenario some mobile nodes use Mobile IPv6 to manage their movements while others rely on a network-based mobility solution provided by the network. There is a common mobility anchor that acts as Mobile IPv6 Home Agent and Proxy Mobile IPv6 LMA, depending on the type of the node.

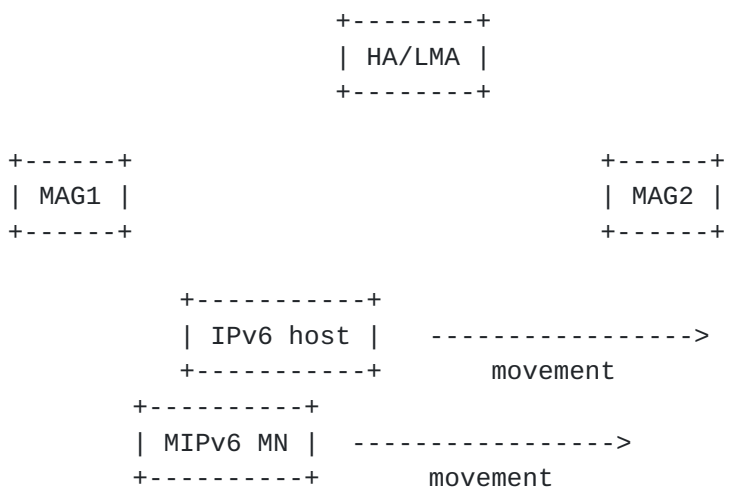


Figure 2 - Scenario B

- Scenario C - in this scenario the mobile node is moving across different access networks, some of them supporting Proxy Mobile IPv6 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 Mobile IPv6 home network and the Proxy Mobile IPv6 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). In this case the MIPv6-HoA is equal to the MN-HoA (i.e. the address managed by PMIPv6).

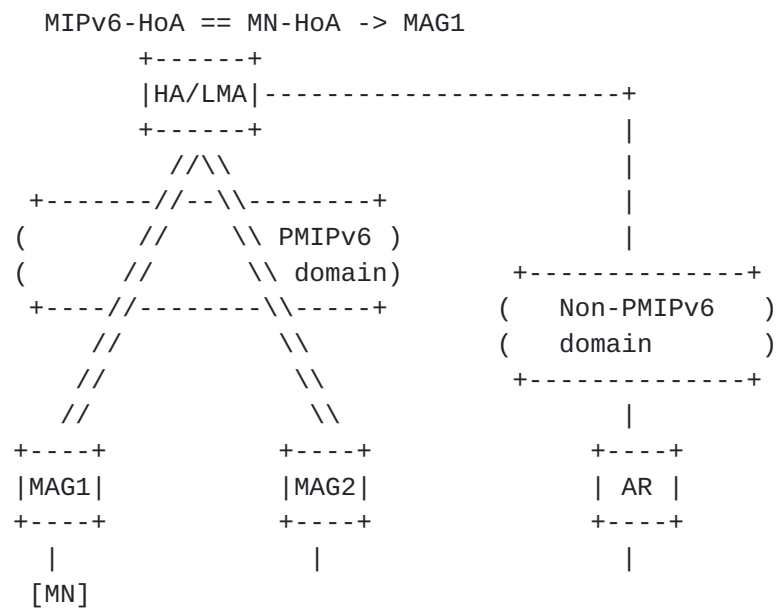
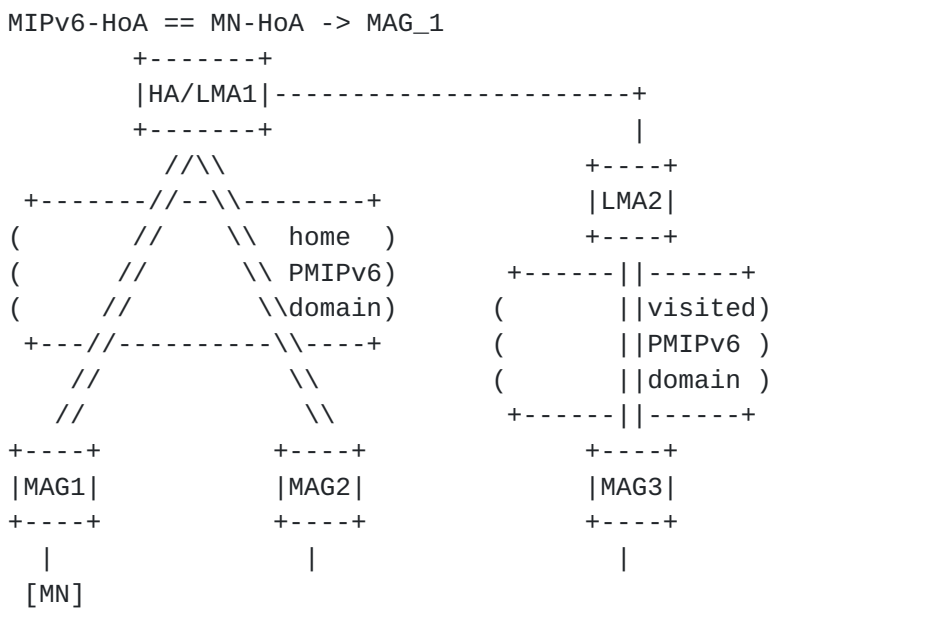
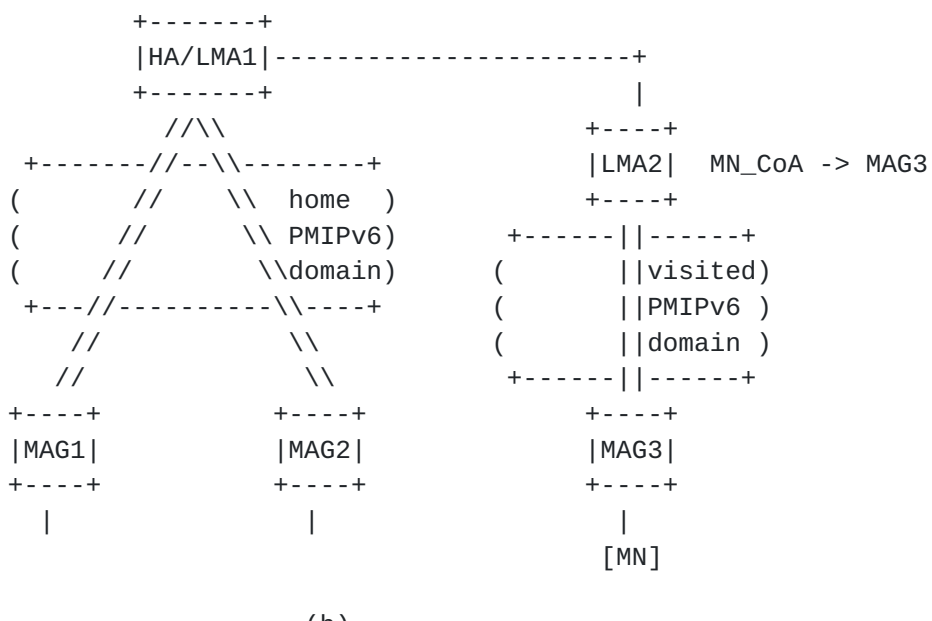


Figure 3 - Scenario C

In the above figure 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.



(a)



(b)

Figure 4 - Scenario C with visited PMIPv6 domain

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

The following sections describe some possible issues for each

scenario. Note that the issues are described based on current specification and does not assume any optimized solution for any scenario. The specifications considered as a baseline for the analysis are the following: [RFC3775], [RFC4877] and [pmipv6-draft]. For example, the collocation of HA and LMA are considered as the combination of HA according [RFC3775] and LMA according to [pmipv6-draft], e.g. no combined binding caches are considered. The analysis of the collocated HA and LMA would show what is the preferred behaviour for this entity. The behaviour and respective recommendations are described in Section 4.3.

3.1. Issues related to scenario A

This scenarios is very similar to other hierarchical mobility schemes, including a HMIPv6-MIPv6 scheme. This is the scenario referenced in [RFC4830]. 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 B

In this scenario there are two types of nodes in the access network: some nodes support Mobile IPv6 while some others do not. The rationale behind such a scenario is that the nodes implementing Mobile IPv6 may prefer or be configured to manage their own mobility. 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 [pmipv6-draft], 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 Mobile IPv6 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 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].

3.3. Issues related to scenario C

Some issues are present in this scenario:

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, based on the base specification [RFC3775], the MN does not 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 [pmipv6-draft], 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. Based on these considerations, there is an "unused" (proxy) binding cache entry in the Binding Cache of the LMA/HA. Note that the assumption in this section is that the binding caches of the LMA and the HA are different and there is not any combined binding cache. The need of such a combined binding cache will be discussed in Section 4.3.

   * When the MN returns to the MIPv6 home link that is also a PMIPv6 domain, it de-registers to remove the binding cache entry it had created. However in [RFC3775], de-registration is recommended (but not mandatory). This implies that the MN receives a Router Advertisement with the home prefix, may start using its HoA directly, without tunneling uplink packets but may not send a Binding Update to remove the binding cache entry related to the HoA. In case the de-registration BU is not sent, the PBU sent by the MAG will not update the Binding Cache entry related to the HoA, but will create a new proxy binding cache entry including the home prefix of the MN, the

MN-ID and the MAG address. This implies that, in case the MN does not send a de-registration binding update when returning home, the downlink packets may still be tunneled to the CoA and not to the MAG.

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. According to RFC3775, 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. 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. 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.

   * Assuming the mobile node's MAG sends a Proxy Binding Update message (for refreshing the mobile node's BCE or because the mobile node has just done a handover to this MAG) and shortly thereafter the mobile node moves out of the PMIP home domain, 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 the MAG is delayed so that it reaches the LMA after the Binding Update, the binding cache entry at the LMA would wrongly point to the MAG. Without further measures, packets are not forwarded to the mobile node unless a new Binding Update is sent by the mobile node. This may result in a significant packet loss. A similar situation can occur if the mobile node sends a Binding Update messsage from outside the PMIP home domain and shortly thereafter enters the PMIP home domai

4. Use of wrong home agent or LMA after handover

* This issues can arise if multiple LMAs are deployed in the PMIP home domain. 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.

5. Threat of compromised MAG

* In MIPv6 base specification [RFC3775] there is a strong binding between the Home Address registered by the MN 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 binging 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

4. Analysis of possible solutions

4.1. Solutions related to scenario A

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

Figures 5 and 6 show a scenario where a MN is moving from one PMIPv6 domain to another, based on the scenario of Figure 1. In Figure 5, the MN 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 MN 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 MN is changed, as the LMA hss changed, and therefore the MN sends a MIPv6 Binding Update to the HA with the new CoA_2.

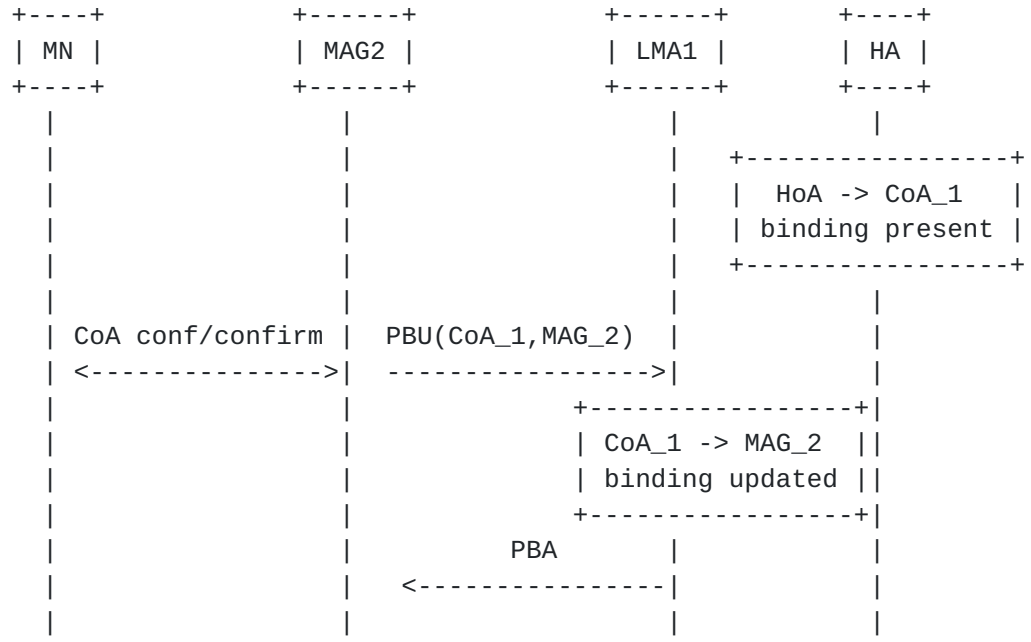


Figure 5 - Local Mobility Message Flow

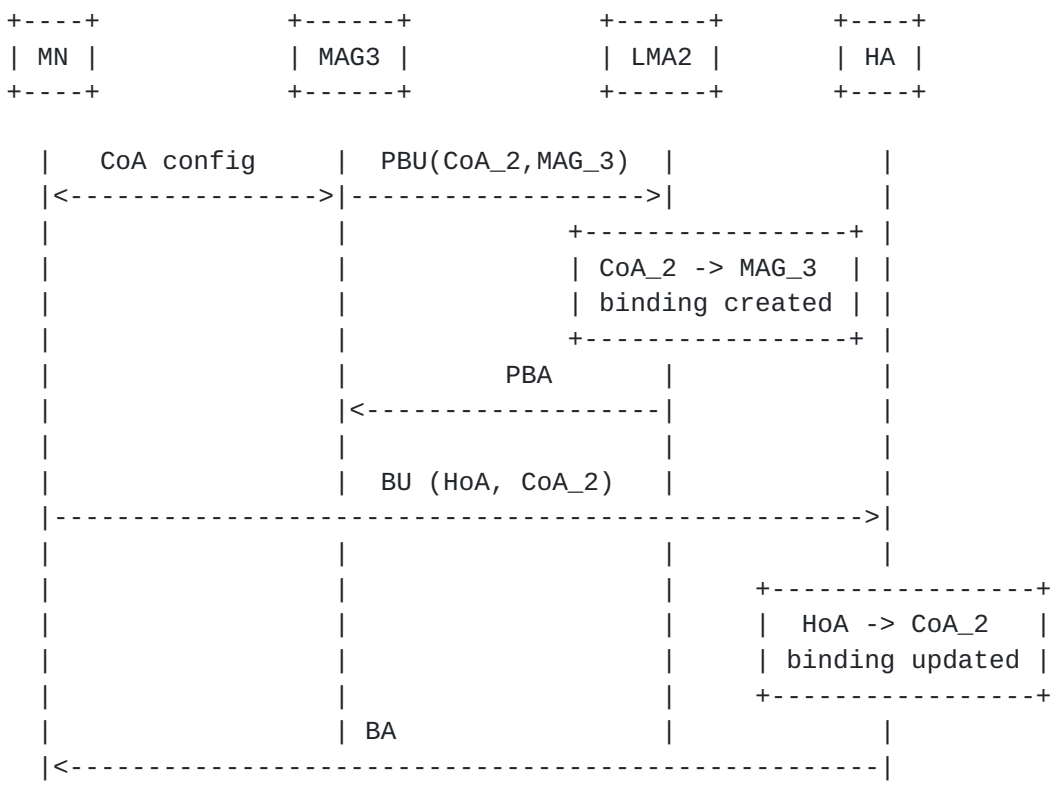


Figure 6 - Global Mobility Message Flow

4.2. Solutoins related to scenario B

The solution for this scenario may depend on the access network being able to determine that a particular mobile node wants to use Mobile IPv6. This would require a solution at the system level for the access network and is out of scope of this document. Solutions that do not depend on the access network are out of the scope of this document.

4.3. Solutions related to scenario C

As described in Section 3.3, in this scenario the mobile node relies on Proxy Mobile IPv6 as long as it is in the Proxy Mobile IPv6 domain. The mobile node then uses Mobile IPv6 whenever it moves out of the PMIPv6 domain.

This section provides an analysis of the solutions for the issues described in Section 3.3. The analysis is performed in two different subsections, depending if the MN moves from a PMIPv6 domain to a non-PMIPv6 domain or vice versa.

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

Let's assume the MN is attached to a PMIPv6 domain and there is a valid Proxy Binding Cache entry at the LMA. Then the MN moves to a adifferent access network and starts using MIPv6 (e.g. because PMIPv6 is not supported). The MN 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 MN 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 3.3 as issue 4.

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

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

Since all these steps must be performed by the MN 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 MN establishes the IPsec security association (and consequently is provided by the HA/LMA with a MIPv6-HoA) when it is still attached to the PMIPv6 domain. This implies that the mobile node has Mobile IPv6 stack active while in the PMIPv6 domain, but as long as it is attached to the same Proxy Mobile IPv6 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 MN 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 MN 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 MN establishes the security association, it pacquires a home address based on [RFC5026]. However, based on PMIPv6 operations, the LMA knows only the Home Network Prefix used by the MN and does not know the MN-HoA.For this reason, the MN 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. Note that the security association must be bound to the MN-HoA used in the PMIPv6 domain as per [RFC4877].

When the MN hands over to an access network which does not support Proxy Mobile IPv6, it sends a Binding Update to the HA/LMA. The LMA/HA must match the HoA with the MN-ID and update the respective BCE accordingly. This is because the proxy BCE is associated to the MN-ID and MN-HNP and not to the MN-HoA. Note that this implies a change in the BU processing if compared to RFC 3775: the LMA/HA must match the HoA included in the BU with the MN-ID known based on IKEv2 signalling and update the respective BCE accordingly (clearing the P flag).

More generally, when the LMA and the HA are co-located, binding cache lookup for a mobile node must use a combination of the mobile node's identifier and the home address. The Binding Update from the mobile node contains the home address of the mobile node, whereas the Proxy Binding Update from the MAG contains only the mobile node's identifier. Therefore when transitioning between using Proxy Mobile IPv6 and Mobile IPv6, the Home Agent must ensure that the mobile node's binding cache entry must be looked up with both the home address and identifier of the mobile node. This requires the Home Agent to acquire the mobile node identifier other than from the Binding Update message (for e.g., from the preceding IKEv2 exchange that set up security associations for sending the Binding Update) and to store it as part of the binding cache entry for the mobile node. Note that this requires that the MN-ID used by the mobile node during the IKEv2 set-up is the same of the MN-ID used by the MAG in PMIPv6 signalling. This solves the issue 1 described in Section 3.3.

Note that in this scenario the same binding cache entry for the mobile node is at times modified by the mobile node and other times modified by a MAG. The home agent must ensure that only authorized MAGs in addition to the mobile node are allowed to modify the binding cache entry for the mobile node. This is valid, even though not explicitly mentioned, also for the next subsection.

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

In this section it is assumed that the MN 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 at the HA. Then the MN moves to a PMIPv6 domain which is configured to be the home link for the MIPv6-HoA the MN 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 [pmipv6-draft] assumes that the LMA is assigned or discovered when the MN attaches to the MAG. the exact mechanism is not specified in [pmipv6-draft]. 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 MN in order to select the correct HA/LMA.

The PBU sent by the MAG must update the MIPv6 BCE of the MN. However this PBU contains the MN-HNP and not the MN-HoA. For this reason, in order to ensure that the PMIPv6 addressing model is maintained when the MN moves back to the PMIPv6 domain, a HA which acts also as LMA must allocate a home network prefix to the MN, even though during the MIPv6 bootstrapping only a /128 Home Address is assigned. It is implementation specific if this prefix is stored on the MIPv6 BCE when the MN is just using MIPv6.

As the MN moves to its home link, it will send a de-registration binding update with zero lifetime to its home agent. This is done approximately at the same time the MAG the sends a Proxy Binding Update to the LMA functionality co-located with the home agent. Actually the de-registration of the MN will be received by the HA/LMA after the PBU from the MAG as, based on [pmipv6-draft], the MAG forwards pakets only when the PMIPv6 tunnel is established. The HA/LMA MUST NOT delete the binding cache entry for the mobile node after receiving a de-registration BU if in the binding cache there is a BCE with the P-flag set for the same MN. This solves issue 2 described in Section 3.3.

NOTE: A solution for race conditions between BU and PBU messages (issue #3) is TBD.

5. Security Considerations

Scenarios A and B described in Section 3 do not introduce any security considerations in addition to those described in [pmipv6-draft] or [RFC3775].

In Scenario C described in Section 3.3, the home agent has to allow the authorized MAGs in a particular PMIPv6 domain to be able to modify the binding cache entry for a mobile node. [RFC3775] requires that only the right mobile node is allowed to modify the binding cache entry for its home address. 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 entry for the mobile node. Note that the compromised MAG threat described in [RFC4832] applies also here; in this scenario the threat is worse as it affects also hosts that are using the LMA/HA as MIPv6 HA and are not using PMIPv6.

6. 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@eu.panasonic.com

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

Ahmad Muhanna - amuhanna@nortel.com

7. Acknowledgements

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

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

8. References

8.1. 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.

[RFC4830] Kempf, J., "Problem Statement for Network-Based Localized Mobility Management (NETLMM)", April 2007.

[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.

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

[pmipv6-draft] Gundavelli, S., Ed., "Proxy Mobile IPv6", 2007, <http://www.ietf.org/internet-drafts/draft-ietf-netlmm-proxymip6-01.txt>.

8.2. 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.

[RFC4831] Kempf, J., "Goals for Network-Based Localized Mobility Management (NETLMM)", RFC 4831, April 2007.

Author's Address

Gerardo Giaretta (editor)
Qualcomm

Email: gerardog@qualcomm.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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