Internet Engineering Task Force (IETF)
Request for Comments: 6612
Category: Informational
ISSN: 2070-1721

G. Giaretta, Ed.
Qualcomm

May 2012

Interactions between Proxy Mobile IPv6 (PMIPv6) and Mobile IPv6 (MIPv6): Scenarios and Related Issues

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.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6612.

Table of Contents

1. Introduction

Proxy Mobile IPv6 (PMIPv6) [RFC5213] is a network-based IP mobility protocol standardized by the IETF. In some deployment scenarios, this protocol will be deployed together with Mobile IPv6 (MIPv6) [RFC6275], 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 on 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 also needs 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 pertaining 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:

- AR (Access Router): first hop router
- BCE (Binding Cache Entry): an entry of the MIPv6 or PMIPv6 binding cache
- LMA (Local Mobility Anchor): the PMIPv6 mobility anchor as specified in [RFC5213]
- MAG (Mobility Access Gateway): the PMIPv6 client as specified in [RFC5213]
- MN-HoA: the Home Address (HoA) of a Mobile Node (MN) in a PMIPv6 domain
- MN-HNP: the IPv6 prefix that is always present in the Router Advertisements that the MN receives when it is attached to any of the access links in that PMIPv6 domain (MN-HoA always belongs to this prefix.)
- MIPv6-HoA: the HoA the MN includes in MIPv6 Binding Update messages
- 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 MN to manage local and global mobility but also investigates more complex scenarios where the protocols are more tightly integrated or where there is a coexistence of nodes that 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 MN.

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 interaction between Hierarchical Mobile IPv6 (HMIPv6) and MIPv6 [RFC5380]; 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 the Care-of Address by the MN at the Home Agent (HA). This means that the HA has a BCE for MIPv6-HoA that points to the MN-HoA.

The following figure illustrates this scenario.

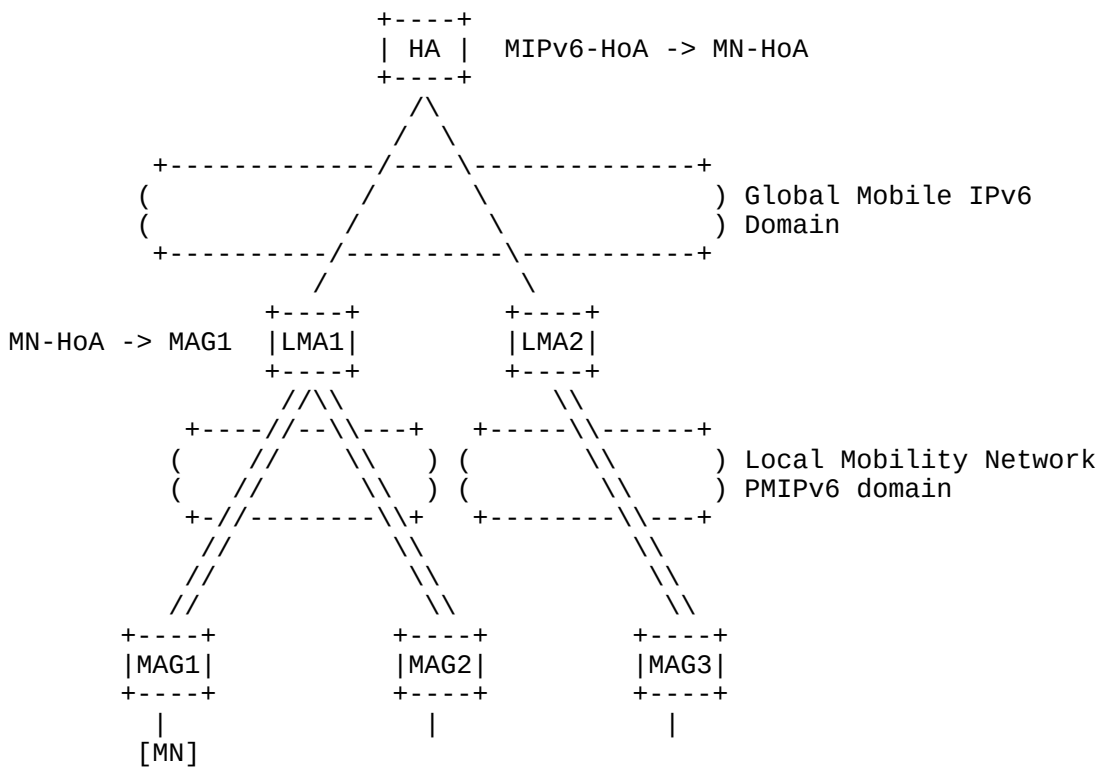


Figure 1: Scenario A.1

Scenario A.2: In this scenario, the MN is moving across different access networks, some of them supporting PMIPv6 and some others not supporting it. Therefore, the MN 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).

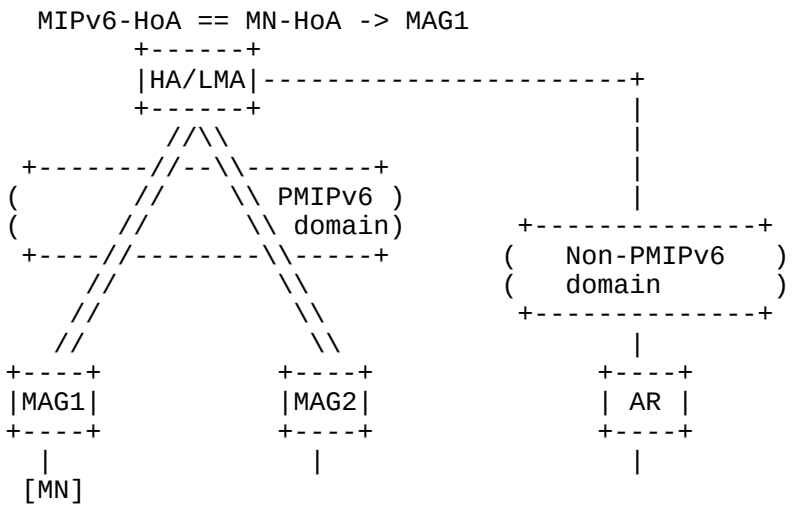
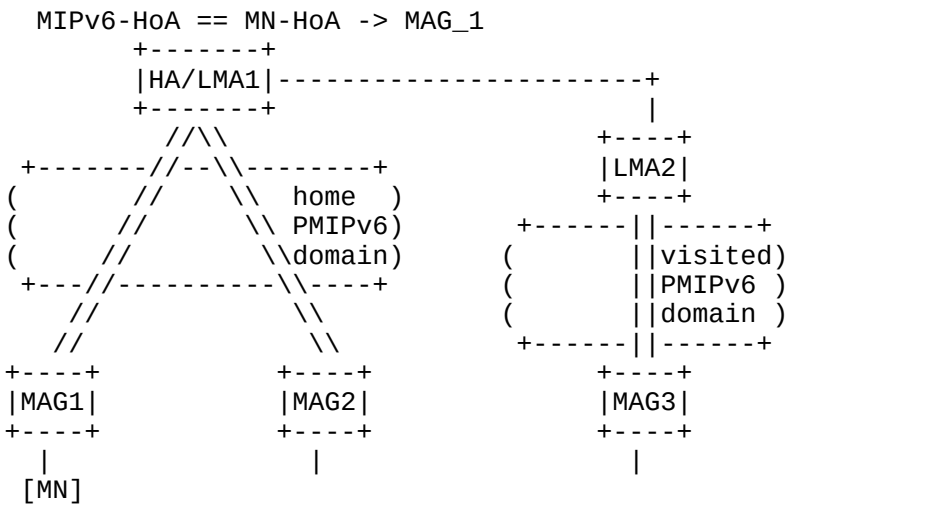
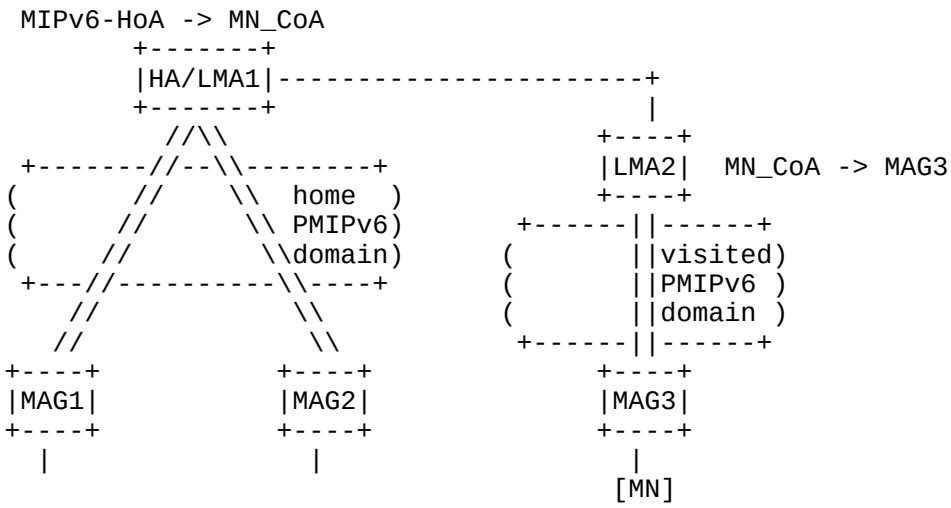


Figure 2: Scenario A.2

In the scenario illustrated in Figure 2, the non-PMIPv6 domain can actually also be 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 3: Scenario A.2 with Visited PMIPv6 Domain

The following alternative deployment has been identified:

Scenario B: In this scenario, some MNs 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 impact on the mobility of the nodes.

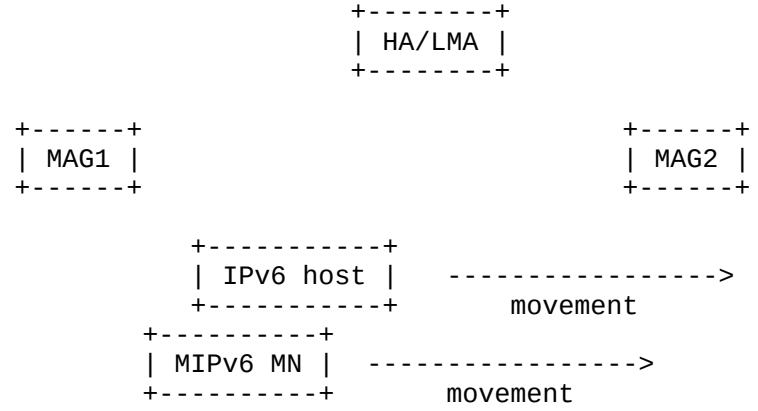


Figure 4: Scenario B

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: [RFC6275], [RFC4877], and [RFC5213].

3.1. Issues Related to Scenario A.1

This scenario is very similar to other hierarchical mobility schemes, including an 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 the PMIPv6 specification [RFC5213], 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 [RFC6275], the lookup key in the binding cache is the HoA of the MN. In particular, the base specification [RFC6275] doesn't require the MN to include any identifier, such as the MN-ID [RFC4283], in the Binding Update message other than its HoA. As described in [RFC4877], the identifier of the MN is known by the Home Agent after the Internet Key Exchange Protocol (IKEv2) exchange, but this is not used in the MIPv6 signaling or 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 HoA 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 BCE containing the home prefix of the MN, but a new binding cache entry is created. Therefore, PMIPv6 and MIPv6 will always create two different BCEs in the HA/LMA, which implies that the HA and LMA are logically separated. How to handle the presence of the two BCEs for the same MN is described in Section 4.2.

2. MIPv6 de-registration Binding Update deletes PMIPv6 binding cache entry

   * When the MN moves from a MIPv6 foreign network to the PMIPv6 home domain, the MAG registers the MN at the LMA by sending a Proxy Binding Update. Subsequently, the LMA updates the MN's BCE with the MAG address and the MAG emulates the MN's home link. Upon detection of the home link, the MN will send a de-registration Binding Update to its home agent. It is necessary to make sure that the de-registration of the MIPv6 Binding Update does not change the PMIPv6 BCE 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 MN to the home agent are ordered by the sequence numbers. The other side, in PMIPv6, Proxy Binding Update messages that are sent by the MAG to the LMA are

ordered by a timestamp option. When the MN 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 MN 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 MN has moved to access B.

4. Threat of compromised MAG

* In the MIPv6 base specification [RFC6275], there is a strong binding between the HoA registered by the MN and the Security Association (SA) used to modify the corresponding BCE.

* In the PMIPv6 specification [RFC5213], the MAG sends Proxy Binding Updates on behalf of a MN to update the BCE that corresponds to the MN's HoA. Since the MAG sends the Binding Updates, PMIPv6 requires SAs between each MAG and the LMA.

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

* In this mixed scenario, both host-based and network-based SAs 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 also affects hosts that are using the LMA/HA as MIPv6 HA and 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 MN'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 MN'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 a 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 [RFC6275].

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 an 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 HoA 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 mobile node is changed, as the LMA has changed; therefore, the MN sends a MIPv6 Binding Update to the HA with the new CoA_2.

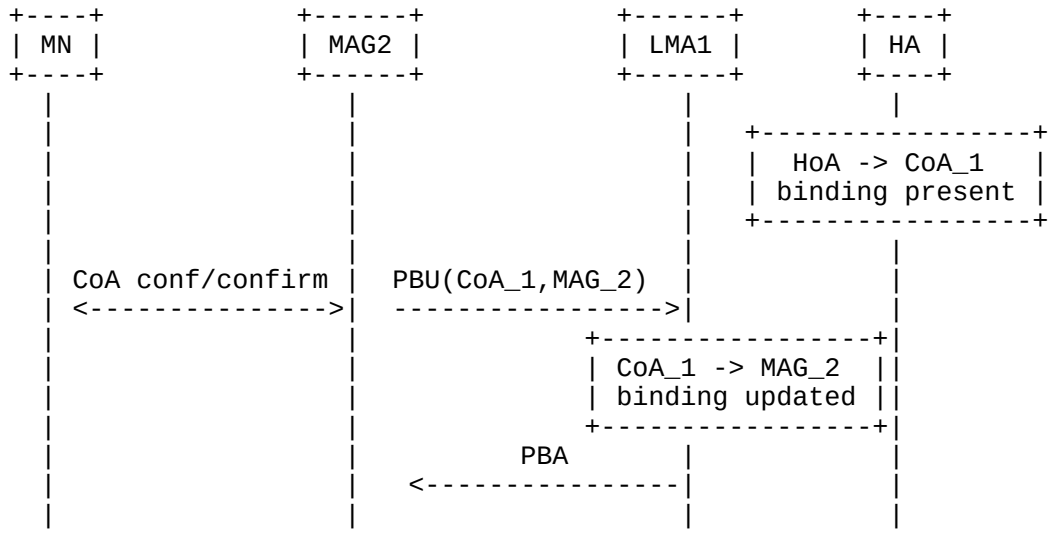


Figure 5: Local Mobility Message Flow

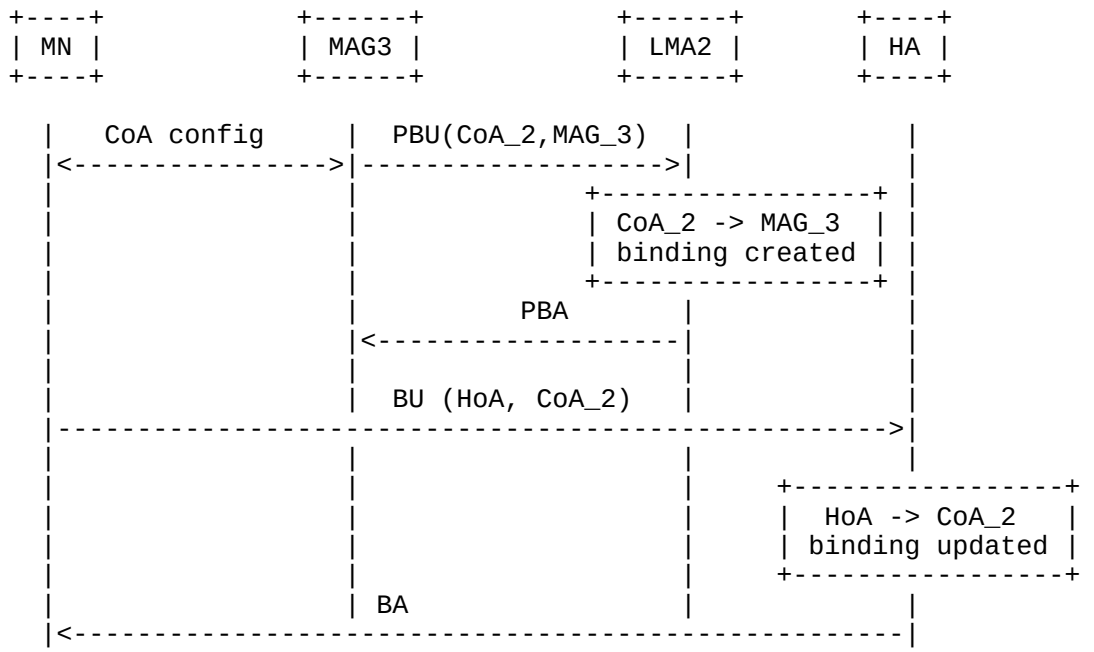


Figure 6: Global Mobility Message Flow

4.2. Solutions Related to Scenario A.2

As described in Section 3.2, in this scenario, the MN relies on PMIPv6 as long as it is in the PMIPv6 domain. The MN 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 BCE for the PMIPv6 registration and the MIPv6 registration. Issue 1, on how the two protocols identify the BCE, is valid only in the case in which we assume that a PMIPv6 message has any value for a MIPv6 BCE. Also, Issues 2 and 3 are not applicable in the case in which 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 treat the two protocols as independent.

In more detail, the following principles should be followed by the HA/LMA implementation:

- PMIPv6 signaling does not overwrite any MIPv6 BCE. In particular, when a PMIPv6 BCE is created for an MN that has previously created a MIPv6 BCE, the MIPv6 BCE of the MN is not overwritten, and a new PMIPv6 BCE is created.

- The downlink packets in the case where both the MIPv6 BCE and PMIPv6 BCE exist are processed as follows:

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

  2. If the destination address does not match the MIPv6 BCE, the BCE created by PMIPv6 is applied, and the packets are encapsulated to the registered MAG.

The following subsections provide a description of the procedures that will be followed by the MN and HA/LMA based on the above principles. The analysis is performed in two different subsections, depending on whether the MN 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 MN is attached to a PMIPv6 domain and there is a valid Proxy BCE at the LMA. Then, the MN moves to a different 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 User Equipment (UE):

- HA/LMA address discovery: the MN needs to discover the IP address of the LMA that has a valid BCE for its home network prefix. This is described in Section 3.2 as Issue 4.

- SA establishment: the MN 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 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 establish the IPsec SA (and, consequently, be provided by the HA/LMA with a MIPv6-HoA) when it is initialized. This implies that the MN 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 MN as if it is attached to the home link.

In order to establish the SA 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 [RFC6611]. 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 SA, it acquires an HoA 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 the MN-HoA as the HoA 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 MN as specified in [RFC5026]; based on this home network prefix, the MN can configure an HoA. Note that the SA 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 MN hands over to an access network that does not support Proxy Mobile IPv6, it sends a Binding Update to the HA. The MN may set the R bit defined in the Network Mobility (NEMO) specification (implicit mode) [RFC3963] in order to indicate that the entire HNP is moved to the new CoA. A MIPv6 BCE is created irrespective of the existing PMIPv6 BCE. Packets matching the MIPv6 BCE are sent to the CoA present in the MIPv6 BCE. The PMIPv6 BCE will expire in the case in which 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 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 (or HNP in case of NEMO) at the HA. Then, the MN moves to a PMIPv6 domain that 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, [RFC5213] assumes that the LMA is assigned to the MAG or discovered by the MAG when the MN 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 MN in order to select the correct HA/LMA.

The PBU sent by the MAG creates a PMIPv6 BCE for the MN that is independent of the MIPv6 BCE. Traffic destined to the MIPv6-HoA (or to the HNP in case the MN had set the flag R in the last BU) is still forwarded to the CoA present in the MIPv6 BCE. When the MN wants to use the HoA directly from the home link, it sends a de-registration message and, at that point only, the PMIPv6 BCE 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 MN 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 MN in the system. These issues are out of the 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 [RFC6275].

For Scenario A.2, this document requires that the a home agent that also implements the PMIPv6 LMA functionality should allow both the MN and the authorized MAGs to modify the BCEs for the MN. Note that the compromised MAG threat described in [RFC4832] also applies here in a more severe form as explained in Section 3.2. Scenario B relies on the secure identification of MNs and their capabilities so that the right service can be provided for the right MNs. For instance, a malicious MN should not get the HoA of some other node assigned to it, and a MN 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. Contributors

Kuntal Chowdhury - kuntal@hotmail.com

Vijay Devarapalli - vijay.devarapalli@azairenet.com

Sri Gundavelli - sgundave@cisco.com

Suresh Krishnan - suresh.krishnan@ericsson.com

Ahmad Muhanna - amuhanna@nortel.com

Hesham Soliman - Hesham@elevatemobile.com

George Tsirtsis - tsirtsis@googlemail.com

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

Kilian Weniger - Kilian.Weniger@googlemail.com

7. Acknowledgements

This document is a merge of four different documents: "Proxy Mobile IPv6 and Mobile IPv6 interworking issues" (April 2007), "Proxy Mobile IPv6 and Mobile IPv6 interworking" (April 2007), "Behavior of Collocated HA/LMA" (October 2008), and "Interactions between PMIPv6 and MIPv6: scenarios and related issues" (November 2007). Thanks to the authors and editors of those documents.

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

8. References

8.1. Normative References

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[RFC4832] Vogt, C. and J. Kempf, "Security Threats to Network-Based Localized Mobility Management (NETLMM)", RFC 4832, April 2007.

[RFC4877] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.

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

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.

[RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[RFC6611] Chowdhury, K., Ed. and A. Yegin, "Mobile IPv6 (MIPv6) Bootstrapping for the Integrated Scenario", RFC 6611, May 2012.

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.

Author’s Address

Gerardo Giaretta (editor)
Qualcomm

EMail: gerardog@qualcomm.com