Diameter Maintenance and                                      M. Liebsch
Extensions (DIME)                                            P. Loureiro
Internet-Draft                                                       NEC
Intended status: Standards Track                             J. Korhonen
Expires: April 29, 2010                           Nokia Siemens Network
                                                        October 26, 2009

# Local Mobility Anchor Resolution for PMIPv6
## draft-liebsch-dime-pmip6-lmaresolve-01.txt

Status of this Memo



Copyright Notice

Abstract

The IETF is specifying Diameter extensions to support mobility service authorization and home network prefix allocation for Proxy Mobile IPv6. The protocol operates between a Local Mobility Anchor and a AAA server. Furthermore, the associated specification extends the existing protocol for network access service to support dynamic assignment and discovery of a Local Mobility Anchor during the authentication procedure. The AAA server maintains mobile nodes' profile in a policy store, which includes information about the assigned Local Mobility Anchor as well as the home network prefix. This document proposes a further extension to allow Local Mobility Anchors benefit from the AAA server's policy store and resolve an unknown mobile node's IP address into a routable address of its assigned Local Mobility Anchor.

Table of Contents

## 1. Introduction

The IETF specified Proxy Mobile IPv6 (PMIPv6) [RFC5213] as solution for network-based localized mobility management. While in host mobility solutions, such as Mobile IPv6 [RFC3775], the mobile node (MN) takes care about updating its routing state on a mobility anchor, in PMIPv6 a Mobility Access Gateway (MAG) recognizes an attachment of an MN and takes over the role of registering the MN at a selected Local Mobility Anchor (LMA).

The base PMIPv6 protocol as per [RFC5213] specifies protocol operation between a MAG and an LMA for registration, de-registration and handover. The LMA is under control of assigning a unique IP address prefix (Home Network Prefix, HNP) to a registering MN and performs prefix-based forwarding of downlink data packets according to the MN's binding cache entry (BCE). The MAG, which performed the registration of the MN by means of sending a Proxy Binding Update (PBU) to the responsible LMA, is referred to as proxy care-of-address for the MN and the LMA forwards downlink data packets to the MN's MAG through an IP tunnel. The MAG forwards the packets to the MN by means of link mechanisms.

[RFC5213] considers selection of a responsible LMA as well as sources for the assignment of an HNP to a registering MN at the LMA out of scope. [I-D.ietf-dime-pmip6] specifies extensions to the Network Access Server (NAS), which is collocated with a MAG in the access network, to retrieve an MN's policy profile and LMA information from a AAA server during access authentication. Furthermore, generic extensions to the Diameter protocol are specified for mobility service authorization and prefix delegation, which apply to the interface between an LMA and the AAA server.

As MNs get assigned a unique prefix during the PMIPv6 registration and associated IP addresses may be from a virtual address space and remain anchored at the LMA, there is no efficient means to resolve an MN's virtual IP address into the routable address of the MN's LMA. This may be needed to support different use cases in a PMIPv6 domain, which utilizes multiple LMAs for load sharing or other purposes. Two exemplary use cases are referred to in Section 3.

This document proposes a mechanism which further extends the generic Diameter protocol extension as per [I-D.ietf-dime-pmip6] to support the resolution of an MN's virtual IP address into the associated LMA's routable IP address.

## 2. Conventions and 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 [RFC2119].

## 3. Problem Statement and Reference Architecture

Addressing of MNs in PMIPv6 [RFC5213] is based on the assignment of individual Home Network Prefixes to an MN during its registration with an LMA. An LMA may use a local prefix pool, DHCP or other means to retrieve a valid and unique HNP for an MN. In large PMIPv6 domains, multiple LMAs will serve MNs to ensure load distribution. In case of local communication within the PMIPv6 domain or even beyond a single PMIPv6 domain, a particular LMA has only forwarding information for destination MNs, which are registered with this particular LMA. For unknown destination prefixes, the LMA may forward data to a default gateway.

In some scenarios it may be useful or even necessary for one LMA to discover the LMA of the destination MN. Hence, an LMA needs to resolve the destination MN's virtual IP address into the routable IP address of the destination MN's LMA. Figure 1 depicts this problem for the communication between MN1 and MN2, which are registered with LMA1 and LMA2 respectively. The reference architecture of this document assumes a NAS being collocated with the MAG on an access router, which performs Diameter protocol operation with a AAA server for access authentication and LMA discovery according to [I-D.ietf-dime-pmip6] (B1,B2 interface of Figure 1). Furthermore, the architecture assumes a Diameter client on each LMA for mobility service authorization and HNP delegation according to [I-D.ietf-dime-pmip6] (A1,A2 interface of Figure 1).

```
                                +---------+
                +--------------->| AAA &   |<--------------+
                |         +---->| Policy  |<----+         |
                |         |     | Profile |     |         |
                |     Diameter  +---------+   Diameter    |
                |        A1                     A2        |
                |         |                     |         |
             Diameter     v                     v      Diameter
                B1       +----+  LMA2?      +----+        B2
                |        |LMA1| ------>     |LMA2|        |
                |        +----+             +----+        |
                |          |                  |           |
                |         //                  \\          |
                |        //                    \\         |
                |       //                      \\        |
                |       |                        |        |
                |     +----+                   +----+     |
                +---->|MAG1|                   |MAG2|<----+
                      +----+                   +----+
                         :                        :
                      +---+                     +---+
                      |MN1|                     |MN2|
                      +---+                     +---+
```

Figure 1: Reference architecture

Exemplary use cases for the resolution of an MN's (virtual) IP address into the anchor's node are as follows:

o Local Routing: Two MNs, MN1 and MN2, which are attached to the same PMIPv6 domain but are registered with different LMAs, LMA1 and LMA2, communicate with each other. MN1 sends data to MN2 through its LMA1. Dependent on the nature of MN2's IP address prefix, LMA1 needs to resolve MN2's virtual IP address into a routable IP address, such as LMA2's address. LMA1 can use LMA2's IP address as forwarding information.

o Route Optimization Signaling: The IETF's NetExt WG is specifying extensions to PMIPv6 for Route Optimization (Localized Routing) [I-D.ietf-netext-pmip6-lr-ps]. Associated scenarios include the communication between two MNs, MN1 and MN2, which are attached to the same PMIPv6 domain but are registered with different LMAs, LMA1 and LMA2. Protocol solutions for route optimization may require signaling between the two LMAs within the same PMIPv6 domain to set up a direct forwarding path between the two MNs' MAGs. As a result, data packets between the two MNs can be forwarded locally without traversing any LMA. In such case, LMA1

may need to resolve MN2's virtual IP address into LMA2's routable IP address. LMA1 can now send signaling messages to LMA2.

[RFC5213] assumes that the LMA is responsible for assigning an HNP to the MN during the PMIPv6 registration, but means to determine a unique HNP are out of scope of the specification. [I-D.ietf-dime-pmip6] specifies extensions to network access service to retrieve information about a responsible LMA for an MN during the MN's authentication procedure. Furthermore, generic protocol extensions to the Diameter protocol are specified to operate between an LMA, which implements a Diameter client, and the AAA server. These extensions are used to authorize mobility service for an MN after an LMA received a Proxy Binding Update (PBU) from the MN's MAG and to retrieve a valid and unique HNP for the MN from the AAA server.

Figure 2 depicts the registration procedure of MN1 with LMA1 and of MN2 with LMA2 according to [I-D.ietf-dime-pmip6]. MN1 attaches to MAG1, whereas MN2 attaches to MAG2. As a result of mobility service authorization, MN1 gets assigned HNP1, whereas MN2 gets assigned HNP2.

```
   +---+  +---+ +----+ +----+   +----+              +---+        +----+
   |MN1|  |MN2| |MAG1| |MAG2|   |LMA1|              |AAA|        |LMA2|
   +---+  +---+ +----+ +----+   +----+              +---+        +----+
     |      |    |       |        |                    |               |
     |      |    |       |        |                    |               |
     |- attach- -|       |        |                    |               |
     |      |    |-----AA-Request[MN1]---------------->|               |
     |      |    |<----AA-Answer[LMA1]-----------------|               |
     |      |    |----PBU[MN1]--->|                    |               |
     |      |    |       |        |----AA-Req[MN1]---->|               |
     |      |    |       |        |              [Authorization]       |
     |      |    |       |        |<--AA-Answer[HNP1]--|               |
     |      |    |<---PBA[HNP1]---|                    |               |
     |      |    |       |        |                    |               |
     |      |- -attach - |        |                    |               |
     |      |    |       |----------AA-Request[MN2]--->|               |
     |      |    |       |<---------AA-Answer[LMA2]----|               |
     |      |    |       |-------------PBU[MN2]----------------------->|
     |      |    |       |        |                    |<-AA-Req[MN2]--|
     |      |    |       |        |                    |     [Authoriz.]
     |      |    |       |        |                    |-AA-Ans[HNP2]->|
     |      |    |       |<------------PBA[HNP2]-----------------------|
     |      |    |       |        |                    |               |
     |      |    |       |        |                    |               |
     |      |    |       |        |                    |               |
```

   Figure 2: MN Authentication, LMA discovery, service authorization and
                 Prefix delegation in a multi-LMA scenario

## 4. Information Query extension to Diameter for LMA Resolution

According to [I-D.ietf-dime-pmip6], the AAA server is a suitable entity to maintain MNs' profile information and to store further dynamically assigned information during an MN's mobility session. Such information includes the assigned LMA and the HNP, which has been assigned to the MN during access authorization. This makes the AAA server a suitable information database for trusted Diameter clients to request some information from the policy store.

This document proposes an extension to the Diameter protocol interface as per [I-D.ietf-dime-pmip6] to support resolving an MN's HNP into its LMA's IP address by means of a new message type INFO_QUERY. Any Diameter client, which is associated with the AAA server, may send an INFO_QUERY to the AAA server, having the unknown MN's HNP or complete IP address included. The AAA server performs a lookup in its policy store and a longest prefix match to resolve the HNP into the associated LMA's IP address. Subsequently, the AAA server replies to the requesting Diameter client with an INFO_RESPONSE (INFO_RESP), including the requested binding between the unknown MN's HNP and its assigned LMA's IP address. Now, the requesting LMA can contact the unknown LMA directly for signaling reasons or take the resolved IP address as forwarding information for data packets.

Figure 3 illustrates exemplarily the resolution of the IP address/HNP of MN2, which is registered with LMA2, into the IP address of LMA2 with the help of the proposed LMA Resolution extension to Diameter. MN1 sends a data packet to MN2, which traverses MN1's LMA1. In case LMA1 needs to know a routable IP address of MN2's mobility anchor, LMA1 performs LMA Resolution with the AAA server to resolve MN2's IP address/HNP (IP MN2) into LMA2's IP address (IP LMA2).

```
    +---+     +----+         +----+                +---+          +----+
    |MN1|     |MAG1|         |LMA1|                |AAA|          |LMA2|
    +---+     +----+         +----+                +---+          +----+
      |  data    |    data     |                       |              |
      |- - - - ->|-==========->|                       |              |
      |          |             |--INFO_QUERY[IP MN2]->|              |
      |          |             |                       |              |
      |          |             |<--INFO_RESP[IP LMA2]-|              |
      |          |             |                       |              |
      |          |             |-----data/signaling----------------->|
      |          |             |                       |              |
      |          |             |                       |              |
```

Figure 3: LMA resolution at a AAA server

In large domains, multiple AAA servers may distribute load. To assign a unique HNP to registering MNs, AAA servers may use administratively assigned prefix pools. In such case, it may happen that an LMA tries to resolve an unknown MN's IP/HNP into the associated LMA's IP address, but the requested AAA server does not have an entry for the unknown MN as well. Here, the concept of the Diameter redirect agent [RFC3588] may help to support LMA resolution beyond the scope of a single AAA server. Such an architecture is illustrated in Figure 4.

```
                   +------------------------------------+
                   (                      AAA           )
                   (     +--------+     Backend         )
                   (     |Redirect|                     )
                   (     | Agent  |                     )
                   (     +--------+                     )
                   (         ^                          )
                   (         |                          )
                   (         |                          )
                   (         v                          )
                   (  +---------+          +---------+  )
                +---->| AAA1 &  |          | AAA2 &  |<---+
                |  (  | Policy  |<-------->| Policy  |  ) |
                |  (  | Profile |          | Profile |  ) |
                |  (  +---------+          +---------+  ) |
                |  (      ^                     ^       ) |
                |  +----- | ------------------- |-------+ |
                |         A1                    A2        |
                |         |                     |         |
                |         |                     |         |
             Diameter     v                     v      Diameter
                B1       +----+  LMA2 ?     +----+        B2
                |        |LMA1| ------>     |LMA2|        |
                |        +----+             +----+        |
                |          |                  |           |
                |         //                  \\          |
                |        //                    \\         |
                |       //                      \\        |
                |       |                        |        |
                |     +----+                   +----+     |
                +---->|MAG1|                   |MAG2|<----+
                      +----+                   +----+
                         :                        :
                      +---+                     +---+
                      |MN1|                     |MN2|
                      +---+                     +---+
```

Figure 4: Use of a Diameter redirect agent to support LMA resolution in networks with multiple AAA servers

Referring to an architecture with multiple AAA servers according to Figure 4, AAA1 may not be able to resolve the HNP of MN2 into the IP address of LMA2, as AAA2 holds this information in its policy store. In such case, AAA1 contacts a Diameter redirect agent [RFC3588] to request the AAA server being responsible for the assignment from the address space where MN2's HNP belongs to.  The redirect agent informs

AAA1 about AAA2's address in a Redirection Notification message, which allows AAA1 to forward the INFO_QUERY to AAA2. AAA2 resolves MN2's HNP into the IP address of LMA2 and sends the results back in an INFO_RESPONSE message to LMA2 via AAA1. Details about the use of redirection agents in this context are for further study.

## 5. Security Considerations

As LMA resolution according to this draft is performed between a Diameter client on an LMA and the AAA server using the Diameter protocol, an existing security association between the LMA and the AAA server can be assumed to protect the new signaling messages. One important difference to the existing protocol operation between a Diameter client and the Diameter server according to [I-D.ietf-dime-pmip6] is that the requesting LMA cannot include a Diameter Session-ID or the MNID of the MN, whose HNP should be resolved into an anchor address (MN2), in the INFO_QUERY message. The AAA server must rather use the HNP or the IP address of MN2 as key to perform a lookup in its policy store. Since the requesting Diameter client on the LMA and the AAA server share a trust relationship and associated signaling can be protected, there should be no security threat with such operation.

## 6. Acknowledgments

Many thanks to Rafael Richter for his valuable input on AAA-based anchor resolution.

May thanks to Glen Zorn, Dan Romascanu, Hannes Tschofenig and Qin Wu for their valuable comments on the initial version of this draft.

# 7. References

## 7.1. Normative References

[I-D.ietf-dime-pmip6]
Korhonen, J., Bournelle, J., Chowdhury, K., Muhanna, A., and U. Meyer, "Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor  Interaction with Diameter Server", draft-ietf-dime-pmip6-04 (work in progress), September 2009.

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

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

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

## 7.2. Informative References

[I-D.ietf-netext-pmip6-lr-ps]
Liebsch, M., Jeong, S., and W. Wu, "PMIPv6 Localized Routing Problem Statement", draft-ietf-netext-pmip6-lr-ps-00 (work in progress), September 2009.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

Authors' Addresses

Marco Liebsch
NEC Laboratories Europe
NEC Europe Ltd.
Kurfuersten-Anlage 36
69115 Heidelberg,
Germany

Phone: +49 6221 4342146
Email: liebsch@nw.neclab.eu

Paulo Loureiro
NEC Laboratories Europe
NEC Europe Ltd.
Kurfuersten-Anlage 36
69115 Heidelberg,
Germany

Phone: +49 6221 4342177
Email: loureiro@nw.neclab.eu

Jouni Korhonen
Nokia Siemens Network
Linnoitustie 6
Espoo FI-02600
Finland

Email: jouni.nospam@gmail.com