DMM WG
Internet-Draft
Intended status: Informational
Expires: January 10, 2013

JC. Zuniga
InterDigital
CJ. Bernardos
UC3M
T. Melia
Alcatel-Lucent

July 9, 2012

DMM Practices and Gap Analysis
draft-zuniga-dmm-gap-analysis-00

Abstract

This document describes practices for the deployment of existing mobility protocols in a distributed mobility management environment, and identifies the limitations in the current practices with respect to providing the expected functionality.

The practices and gap analysis is performed for IP-based mobility protocols, dividing them into two main solution families: client- and network-based.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

The Distributed Mobility Management (DMM) approach aims at setting up IP networks so that traffic is distributed in an optimal way and does not rely on centrally deployed anchors to manage IP mobility sessions.

A first step towards the definition of DMM solutions is the definition of the problem of distributed mobility management and the identification of the main requirements for a distributed mobility management solution [I-D.ietf-dmm-requirements], which are summarized below:

- REQ1: Distributed deployment. IP mobility, network access and routing solutions provided by DMM must enable a distributed deployment of mobility management of IP sessions so that the traffic can be routed in an optimal manner without traversing centrally deployed mobility anchors.

- REQ2: Transparency to Upper Layers when needed. The DMM solutions must provide transparency above the IP layer when needed. Such transparency is needed, when the mobile hosts or entire mobile networks change their point of attachment to the Internet, for the application flows that cannot cope with a change of IP address. Otherwise the support to maintain a stable home IP address or prefix during handover may be declined.

- REQ3: IPv6 deployment. The DMM solutions should target IPv6 as primary deployment and should not be tailored specifically to support IPv4, in particular in situations where private IPv4 addresses and/or NATs are used.

- REQ4: Compatibility. The DMM solution should be able to work between trusted administrative domains when allowed by the security measures deployed between these domains. Furthermore, the DMM solution must be able to co-exist with existing network deployment and end hosts so that the existing deployment can continue to be supported. For example, depending on the environment in which DMM is deployed, the DMM solutions may need to be compatible with other existing mobility protocols that are deployed in that environment or may need to be interoperable with the network or the mobile hosts/routers that do not support the DMM enabling protocol.

- REQ5: Existing mobility protocols. A DMM solution should first consider reusing and extending the existing mobility protocols before specifying new protocols.

- REQ6: Security considerations. The protocol solutions for DMM must consider security, for example authentication and authorization mechanisms that allow a legitimate mobile host/ router to access to the DMM service, protection of signaling messages of the protocol solutions in terms of authentication, data integrity, and data confidentiality, opti-in or opt-out data confidentiality to signaling messages depending on network environments or user requirements.

We next first analyze existing practices of deployment of IP mobility solutions in a DMM environment [I-D.perkins-dmm-matrix], [I-D.patil-dmm-issues-and-approaches2dmm]. After that, a gap analysis is conducted, identifying what can be achieved with existing solutions and what is missing in order to meet the DMM requirements identified in [I-D.ietf-dmm-requirements].

2. Practices: deployment of existing solutions in a DMM environment

This section documents practices for the deployment of existing mobility protocols in a distributed mobility management (DMM) environment. This analysis is limited in scope to existing IPv6-based mobility protocols, such as Mobile IPv6 [RFC6275], NEMO Basic Support Protocol [RFC3963], Proxy Mobile IPv6 [RFC5213], and their extensions, such as Hierarchical Mobile IPv6 [RFC5380], Mobile IPv6 Fast Handovers [RFC5568] or Localized Routing for Proxy Mobile IPv6 [I-D.ietf-netext-pmip-lr], among others.

The section is divided in two parts: client-based and network-based mobility.

2.1. Client-based mobility

Mobile IPv6 (MIPv6) [RFC6275] and its extension to support mobile networks, the NEMO Basic Support protocol (NEMO B.S.) [RFC3963] are the main client-based IP mobility protocols. They heavily rely on the figure of the Home Agent (HA), a centralized anchor, to provide mobile nodes (hosts and routers) with mobility support. We next describe how Mobile IPv6/NEMO and several additional protocol extensions can be deployed to meet some of the DMM requirements [I-D.ietf-dmm-requirements].

2.1.1. Mobile IPv6 / NEMO B.S.

```
                    +-----+          +-----+
                    | CN1 |          | CN2 |
                    +-----+          +-----+
                       |                |
      +------------------------------------------------+
     (                                                  )
    (       -------                        -------       )
   (        | HA1 |     MN1 operator's     | HA2 |        )
    (       -------          core          -------       )
     (                                                  )
      +------------------------------------------------+
           /           |             |           \
          /            |             |            \
         /             |             |             \
        /              |             |              \
      -+-----        ---+---       - -+---       -----+-
      | AR1 |        | AR2 |       | AR3 |       | AR4 |
      ---+---        ---+---       ---+---       ---+---
         |              |             |             |
        (o)            (o)           (o)           (o)
                       x                           x
                      x                           x
                     x                           x
                  (o)                         (o)
                   |                           |
                +--+--+                     +--+--+
   ( anchored ) | MN1 |        ( anchored ) | MN2 |
   (  at HA1  ) +-----+        (  at HA2  ) +-----+
```

Figure 1: Distributed operation of Mobile IPv6 / NEMO B.S.

Due to the heavy dependance on the home agent role, Mobile IPv6 and NEMO B.S. plain vanilla protocols (i.e., without additional extensions) cannot be easily deployed in a distributed fashion. One approach would be to deploy several HAs (like in Figure 1, and assign to each MN the one closest to its topological location [RFC4640], [RFC5026], [RFC6611]. In the example shown in Figure 1, MN1 is assigned HA1 (and a home address anchored by HA1), while MN2 is assigned HA2. Note that current Mobile IPv6 / NEMO B.S. specifications do not allow the use of multiple home agents by a mobile node simultaneously, and therefore the benefits of this deployment model shown here are limited. For example, if MN1 moves and attaches to AR4, the path followed by data packets would be suboptimal, as they have to traverse HA1, which is no longer close to the topological attachment point of MN1.

2.1.2. Mobile IPv6 Route Optimization

```
                    +-----+          +-----+
                    | CN1 |          | CN2 |
                    +-----+          +-----+
                       |                |
      +------------------------------------------------+
     (                                                  )
    (       -------                                      )
   (        | HA1 |     MN1 operator's                    )
    (       -------          core                        )
     (                                                  )
      +------------------------------------------------+
           /           |
          /            |
         /             |
        /              |
      -+-----       ---+---
      | AR1 |       | AR2 |
      ---+---       ---+---
         |             |
        (o)           (o)
                      x
                     x    MN1      AR2      HA1      CN1      CN2
                    x      |        |        |        |        |
                  (o)      |<-------+---------------->|        | RO mode
                   |       |        |        |        |        |
                +--+--+    |<=======+=======>|<--------------->| BT mode
                | MN1 |    |        |        |        |        |
                +-----+
```

Figure 2: Mobile IPv6 Route Optimization

One of the main goals of DMM is to avoid the suboptimal routing caused by centralized anchoring. By default, Mobile IPv6 (and NEMO B.S.) uses the so-called Bidirectional Tunnel (BT) mode, in which data traffic is always encapsulated between the MN and its HA. Mobile IPv6 also specifies the Route Optimization (RO) mode, which allows the MN to update its current location on the CNs, and then use the direct path between them An example is shown in Figure 2, in which MN1 is using BT mode with CN2 and RO mode with CN1. Note that this RO mode has several drawbacks:

- o The RO mode is only supported by Mobile IPv6. There is no route optimization support standardized for the NEMO B. S. protocol, although there are many different solution proposed, mainly as academic exercises.

- o The RO mode requires additional signaling, which adds some protocol overhead.

- o The signaling required to enable RO involves the home agent, and it is repeated periodically because of security reasons [RFC4225]. This basically means that the HA remains as single point of failure, because the Mobile IPv6 RO mode does not mean HA-less operation.

- o The RO mode requires additional support on the correspondent node (CN).

2.1.3. Hierarchical Mobile IPv6

```
                    +-----+          +-----+
                    | CN1 |          | CN2 |
                    +-----+          +-----+
                       |                |
      +------------------------------------------------+
     (                                                  )
    (       -------                                      )
   (        | HA1 |     MN1 operator's                    )
    (       -------          core                        )
     (                                                  )
      +------------------------------------------------+
            /                |              \
           /                 |               \
          /                  |                \
         /                   |                 \
      --+-----            ---+----           +--+----
      | MAP1 |            | MAP2 |           | MAP3 |
      ---+----            ---+----           ---+----
        / \                 / \                 / \
       /   \               /   \               /   \
      /     \             /     \             /     \
   --+--   --+--       --+--   --+--       --+--   --+--
   |AR1|   |AR2|       |AR3|   |AR4|       |AR5|   |AR6|
   -----   -----       -----   -----       -----   -----
             |
            (o)
              x
               x        MN1    AR2    MAP1     HA1    CN1    CN2
                x        |      |      |       |      |      |
                (o)      |<=====+======+======>+----->|      |
                 |       |      |      |       |      |      |
              +--+--+    |<=====+=====>+<------------------->|
              | MN1 |    |      |      |       |      |      |
              +-----+
```

                 Figure 3: Mobile IPv6 Route Optimization

Hierarchical Mobile IPv6 (HMIPv6) [RFC5380] allows reducing the amount of mobility signaling as well as the overall handover performance of Mobile IPv6, by introducing a new hierarchy level to handle local mobility. The Mobility Anchor Point (MAP) entity is introduced as a local mobility handling node deployed closer to the mobile node.

When HMIPv6 is used, the MN two different temporal addresses: the Regional Care-of Address (RCoA) and the Local Care-of Address (LCoA).

The RCoA is anchored at one MAP, that plays the role of local home agent, while the LCoA is anchored at the access router level. The mobile node used the RCoA as the CoA signaled to its home agent. Therefore, while roaming within a local domain handled by the same MAP, the mobile node does not need to update its home agent (i.e., the mobile node does not change RCoA).

The use of HMIPv6 allows some certain route optimization, as a mobile node may decide to directly use the RCoA as source address for a communication with a given correspondent node, if the MN does not expect to move outside the local domain during the lifetime of the communication. This can be seen as a potential DMM mode of operation. In the example shown in Figure 3, MN1 is using its global HoA to communicate with CN1, while it is using its RCoA to communicate with CN2.

Additionally, a local domain might have several MAPs deployed, enabling different kind of HMIPv6 deployments (e.g., flat and distributed). HMIPv6 specification supports a flexible selection of the MAP (e.g., based on the distance between the MN and the MAP, taking into consideration the expected mobility pattern of the MN, etc.).

2.1.4. Home Agent switch

The Home Agent switch specification [RFC5142] defines a new mobility header for signaling a mobile node that it should acquire a new home agent. Although the purposes of this specification do not include the case of changing the mobile node's home address, as that might imply loss of connectivity for ongoing connections, it could be used to force the change of home agent in those situations where there are no active sessions running that cannot cope themselves with a change of home addresss.

2.1.5. Flow Mobility

There exist different protocols meant to support flow mobility with Mobile IPv6, namely the multiple care-of address registration [RFC5648], the flow bindings in Mobile IPv6 and NEMO B.S. [RFC6089] and the traffic selectors for flow bindings [RFC6088]. The use of these extensions allows a mobile node to associate different flows with different care-of addresses that the mobile owns at a given time. This could also be used, combined with the route optimization support, to improve the paths followed by data packets.

2.1.6. Source Address selection API

The IPv6 socekt API for source address selection [RFC5014], [RFC3484] can be used by an application running on a mobile node to express its preference of using a home address or a care-of address in a given connection. This allows, for example, that an application which can survive an IP address change to always prefer the use of a care-of address. Similarly, and as mentioned in [RFC6275], a mobile node can also prefer the use of a care-of address for sessions that are going to finish before the mobile node hands off to a different attachment point (e.g., short-lived connections like DNS dialogs).

2.2. Network-based mobility

Proxy Mobile IPv6 (PMIPv6) [RFC5213] and GPRS Tunneling Protocol (GTP) [3GPP.29.060] are the main network-based IP mobility protocols. PMIPv6 relies on the figure of the Local Mobility Anchor (LMA) to provide mobile nodes with mobility support, without requiring the involvement of the mobile nodes, and supplying the required functionality by the Mobile Access Gateway (MAG). We next describe how PMIPv6 and several additional protocol extensions can be deployed to meet some of the DMM requirements [I-D.ietf-dmm-requirements].

2.2.1. Proxy Mobile IPv6

```
                    +-----+          +-----+
                    | CN1 |          | CN2 |
                    +-----+          +-----+
                       |                |
      +------------------------------------------------+
     (                                                  )
    (      --------                        --------      )
   (       | LMA1 |     MN1 operator's     | LMA2 |       )
    (      --------         core           --------      )
     (                                                  )
      +------------------------------------------------+
           /           |             |           \
          /            |             |            \
         /             |             |             \
        /              |             |              \
     --+-----      ----+---      ---+----      -----+--
     | MAG1 |      | MAG2 |      | MAG3 |      | MAG4 |
     ---+----      ----+---      ---+----      ---+----
        |              |             |              |
       (o)            (o)           (o)            (o)
                      x                            x
                     x                            x
                    x                            x
                  (o)                          (o)
                   |                            |
                +--+--+                      +--+--+
   ( anchored ) | MN1 |        ( anchored ) | MN2 |
   (  at LMA1 ) +-----+        (  at LMA2 ) +-----+
```

Figure 4: Distributed operation of Proxy Mobile IPv6

As with Mobile IPv6, plain Proxy Mobile IPv6 operation cannot be easily decentralized. One simple, but still suboptimal, approach would be to deploy several local mobility anchors and use a topological position based assignment to attaching mobile nodes (an example is shown in Figure 4. This assignment can be static or dynamic (as described in Section 2.2.3. The main advantage of this simple approach is that the IP address anchor (i.e., the LMA) is placed close to the mobile node, and therefore resulting paths are close-to-optimal. On the other hand, as soon as the mobile node moves, the resulting path starts to deviate from the optimal one, unless an inter-LMA mobility protocol is in place (which is missing today).

2.2.2. Local Routing

[I-D.ietf-netext-pmip-lr] enables optimal routing in Proxy Mobile IPv6 in three cases: two MNs attached to the same MAG and LMA, two MNs attached to different MAGs but same LMA and two MNs attached to the same MAG with different LMAs. In these three cases, data traffic between two mobile nodes does not traverse the LMA(s), thus providing some form of distribution, since the traffic is locally router at the edge.

The main disadvantade of this approach is that it only tackles the MN-to-MN communication scenario, and only under certain circumstances.

2.2.3. LMA runtime assignment

[RFC6463] specifies a runtime local mobility anchor assignment functionality and corresponding mobility options for Proxy Mobile IPv6. This runtime local mobility anchor assignment takes place during a Proxy Binding Update and a Proxy Binding Acknowledgment message exchange between a mobile access gateway and a local mobility anchor. While this mechanism mainly aims for load-balancing purposes, it can also be used to select an optimal LMA from a point of view of routing. If properly complemented by an inter-LMA mobility protocol, it could also be used as part of a global DMM solution. Even without that solution, a runtime LMA assignment can be used to change the assigned LMA of an MN, for example when no session is alive (or when those running can survive an IP address change).

2.2.4. Source routing

TBD.

2.2.5. Multihoming in PMIPv6 (as per RFC 5213)

TBD.

3. Gap Analysis: limitations in current practices

This section identifies the limitations in the current practices (documented in Section 2) with respect to the requirements listed in [I-D.ietf-dmm-requirements].

The section is also divided in two parts: client-based and network-based mobility. Each section analyzes how well the requirements listed in [I-D.ietf-dmm-requirements] are covered/met by the current

practices, highlighting existing limitations and gaps.

The remaining of this section will be provided in a future version of this document.

3.1. Client-based mobility

3.1.1. REQ1: Distributed deployment

3.1.2. REQ2: Transparency to Upper Layers when needed

3.1.3. REQ3: IPv6 deployment

3.1.4. REQ4: Compatibility

3.1.5. REQ5: Existing mobility protocols

3.1.6. REQ6: Security considerations

3.2. Network-based mobility

3.2.1. REQ1: Distributed deployment

3.2.2. REQ2: Transparency to Upper Layers when needed

3.2.3. REQ3: IPv6 deployment

3.2.4. REQ4: Compatibility

3.2.5. REQ5: Existing mobility protocols

3.2.6. REQ6: Security considerations

4. IANA Considerations

No IANA considerations.

5. Security Considerations

TBD.

6. References

6.1. Normative References

[RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

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

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

[RFC5142] Haley, B., Devarapalli, V., Deng, H., and J. Kempf, "Mobility Header Home Agent Switch Message", RFC 5142, January 2008.

[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.

[RFC5568] Koodli, R., "Mobile IPv6 Fast Handovers", RFC 5568, July 2009.

[RFC5648] Wakikawa, R., Devarapalli, V., Tsirtsis, G., Ernst, T., and K. Nagami, "Multiple Care-of Addresses Registration", RFC 5648, October 2009.

[RFC6088] Tsirtsis, G., Giarreta, G., Soliman, H., and N. Montavont, "Traffic Selectors for Flow Bindings", RFC 6088, January 2011.

[RFC6089] Tsirtsis, G., Soliman, H., Montavont, N., Giaretta, G., and K. Kuladinithi, "Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support", RFC 6089, January 2011.

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

[RFC6463] Korhonen, J., Gundavelli, S., Yokota, H., and X. Cui, "Runtime Local Mobility Anchor (LMA) Assignment Support for Proxy Mobile IPv6", RFC 6463, February 2012.

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

May 2012.

6.2. Informative References

[3GPP.29.060]
3GPP, "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface", 3GPP TS 29.060 3.19.0, March 2004.

[I-D.ietf-dmm-requirements]
Chan, A., "Requirements of distributed mobility management", draft-ietf-dmm-requirements-00 (work in progress), July 2012.

[I-D.ietf-netext-pmip-lr]
Krishnan, S., Koodli, R., Loureiro, P., Wu, W., and A. Dutta, "Localized Routing for Proxy Mobile IPv6", draft-ietf-netext-pmip-lr-10 (work in progress), May 2012.

[I-D.patil-dmm-issues-and-approaches2dmm]
Patil, B., Williams, C., and J. Korhonen, "Approaches to Distributed mobility management using Mobile IPv6 and its extensions", draft-patil-dmm-issues-and-approaches2dmm-00 (work in progress), March 2012.

[I-D.perkins-dmm-matrix]
Perkins, C., Liu, D., and W. Luo, "DMM Comparison Matrix", draft-perkins-dmm-matrix-03 (work in progress), March 2012.

[RFC4225] Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E. Nordmark, "Mobile IP Version 6 Route Optimization Security Design Background", RFC 4225, December 2005.

[RFC4640] Patel, A. and G. Giaretta, "Problem Statement for bootstrapping Mobile IPv6 (MIPv6)", RFC 4640, September 2006.

[RFC5014] Nordmark, E., Chakrabarti, S., and J. Laganier, "IPv6 Socket API for Source Address Selection", RFC 5014, September 2007.

Appendix A. Acknowledgments

The work of Carlos J. Bernardos and Telemaco Melia has been partially supported by the European Community's Seventh Framework Programme (FP7-ICT-2009-5) under grant agreement n. 258053 (MEDIEVAL project).

The work of Carlos J. Bernardos has also been partially supported by the Ministry of Science and Innovation of Spain under the QUARTET project (TIN2009-13992-C02-01).

Authors' Addresses

Juan Carlos Zuniga
InterDigital Communications, LLC
1000 Sherbrooke Street West, 10th floor
Montreal, Quebec H3A 3G4
Canada

Email: JuanCarlos.Zuniga@InterDigital.com
URI: http://www.InterDigital.com/

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: http://www.it.uc3m.es/cjbc/

Telemaco Melia
Alcatel-Lucent Bell Labs
Route de Villejust
Nozay, Ile de France 91620
France

Email: telemaco.melia@alcatel-lucent.com