Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 11, 2013

H. Chan
Huawei Technologies
P. Seite
France Telecom - Orange
K. Pentikousis
Huawei Technologies
JH. Lee
Telecom Bretagne

November 7, 2012

Framework for Mobility Management Protocol Analysis
draft-chan-dmm-framework-gap-analysis-06

Abstract

This document introduces a framework for analyzing mobility management protocols in terms of their key abstracted logical functions. The framework is capable of presenting a unified view, reducing the clutter that obscures a casual reader from understanding the commonalities between different approaches in mobility management. More importantly, a first order application of this framework allows us to examine previously standardized mobility management protocols, such as MIPv6 and PMIPv6 (as well as several of their extensions), and describe their core functionality in terms of different configurations of the logical functions defined by the framework. As a result, we can use the framework to analyze the gaps between the protocols needed in a distributed mobility management environment and the functionality provided by the current generation of mobility management protocols. Our analysis points to the need for a re-configuration of logical functions identified in the framework as well as the need for new extensions which can make distributed mobility management possible in the future.

This Internet-Draft will expire on May 11, 2013.

Table of Contents

1. Introduction

While there is ongoing research on new protocols for distributed mobility management (DMM), it has also been proposed, e.g., in [Paper-Distributed.Mobility.PMIP] and in other publications, that a distributed mobility management architecture can be designed using primarily existing mobility management protocols with some extensions. This is reflected in the requirement presented in [ID-dmm-requirements]: distributed mobility management is to first use existing protocols and their extensions before considering new protocol designs.

Mobile IPv6 [RFC6275], which is a logically centralized mobility management approach addressing primarily hierarchical mobile networks, has numerous variants and extensions including, just to name a few, PMIPv6 [RFC5213], Hierarchical MIPv6 (HMIPv6) [RFC5380], Fast MIPv6 (FMIPv6) [RFC4068] [RFC4988], Proxy-based FMIPv6 (PFMIPv6) [RFC5949]. These variants or extensions of MIPv6 have been developed over the years owing to the different needs that have been arising ever since the first specification of MIP came into life.

This document argues that we can gain much more insights into this design space by abstracting functions of existing mobility management protocols in terms of logical functions. Different variants of existing mobility management protocols can then be expressed as different design variations of how these logical functions are put together. The result is a rich framework that can express sophisticated functionalities in a more straightforward manner and can be used to perform gap analysis of existing protocols. What is more, this document shows how to reconfigure these logical functions towards various distributed mobility management designs.

The following subsection presents an overview of this document.

1.1. Overview

Section 3 proposes to abstract existing mobility management protocol functions into three logical functions, namely, home address allocation, mobility routing and location management. Such functional decomposition will enable us to clearly separate data plane and the control plane functionality, and gives us the flexibility in an implementation to position said logical functions at their most appropriate places in the system design.

Section 4 shows that these logical functions can indeed perform the same functions as the major existing mobility protocols. These functions therefore become the foundation for a unified framework upon which different designs of distributed mobility management may

be built upon.

Section 6 presents the gap analysis of existing protocols by comparing them against the DMM requirements as per [ID-dmm-requirements].

Extensions to overcome the gaps are presented in Sections 5 and 7. Based on the introduced unified framework, extensions to dynamically provide mobility support are described in Section 7.1 where the home IP address of an MN is generalized to that of an application session. A distributed database architecture is described in Section 5.1. Using this distributed architecture, various route optimizations can be defined as explained in Section 7.2.

2. Conventions and Terminology

2.1. Conventions used in this document

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].

2.2. Terminology

All general mobility-related terms and their acronyms used in this document are to be interpreted as defined in the Mobile IPv6 base specification [RFC6275] and in the Proxy mobile IPv6 specification [RFC5213]. These terms include mobile node (MN), correspondent node (CN), home agent (HA), local mobility anchor (LMA), and mobile access gateway (MAG).

In addition, this document uses the following terms:

Mobility routing (MR) is the logical function that intercepts packets to/from the HoA of a mobile node and forwards them, based on internetwork location information, either directly towards their destination or to some other network element that knows how to forward the packets to their ultimate destination.

Home address allocation is the logical function that allocates the home network prefix or home address to a mobile node.

Location management (LM) is the logical function that manages and keeps track of the internetwork location information of a mobile node, which includes the mapping of the MN HoA to the MN routing address or another network element that knows where to forward packets destined for the MN.

Home network of an application session (or an HoA IP address) is the network that has allocated the IP address used as the session identifier (HoA) by the application being run in an MN. The MN may be attached to more than one home networks.

3. Mobility Management Logical Functions

The existing mobility management functions of MIPv6, PMIPv6, and HMIPv6 ca be abstracted into the following logical functions:

1. Anchoring: allocation of home network prefix or HoA to an MN that registers with the network;

2. Mobility Routing (MR) function: packets interception and forwarding to/from the HoA of the MN, based on the internetwork location information, either to the destination or to some other network element that knows how to forward the packets to their destination;

3. Internetwork Location Management (LM) function: managing and keeping track of the internetwork location of an MN, which includes a mapping of the HoA to the mobility anchoring point that the MN is anchored to;

4. Location Update (LU): provisioning of MN location information to the LM function;

5. Routing Control (RC): this logical function configures the forwarding state of the mobility routing function.

4. Functional Representation of Existing Mobility Protocols

This section shows that existing mobility management protocols can be expressed as different configurations of the logical functions introduced in Section 3 above.

Using these generic logical functions, we will build up the existing mobility protocols one step at a time in the following sequence: MIPv6, PMIPv6, HMIPv6, and HAHA. Functions are added and modified as needed in each step.

4.1. Mobile IPv6

Figure 1 shows Mobile IPv6 [RFC6275] in a functional representation. The combination of the logical functions MR, LM and HoA allocation in network1 is the home agent or the mobility anchor. The mobile node MN11 was originally attached to Network1 and was allocated the IP prefix for its home address HoA11. After some time, MN11 moved to Network3, from which it is allocated a new prefix to configure the IP address IP32. LM1 maintains the binding HoA11:IP32 so that packets from CN21 in Network2 destined to HoA11 will be intercepted by MR1, which will then tunnel them to IP32. MN11 must perform mobility signaling using the LU function.

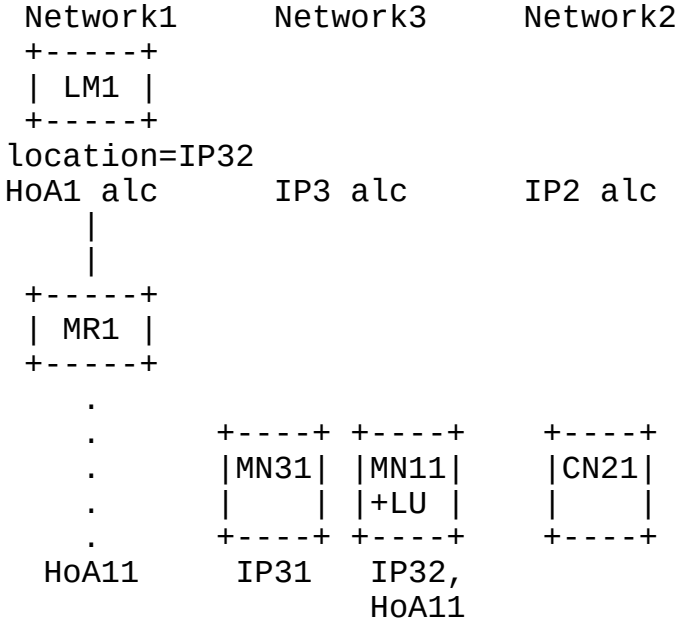

Figure 1. Functional decomposition of Mobile IPv6.

4.2. MIPv6 versus PMIPv6

MIPv6 and PMIPv6 both employ the same concept of separating the session identifier from the routing address into the HoA and CoA, respectively. Figure 2 contrasts (a) MIPv6 and (b) PMIPv6 by showing the destination IP address in the network-layer header as a packet traverses from a CN to an MN.

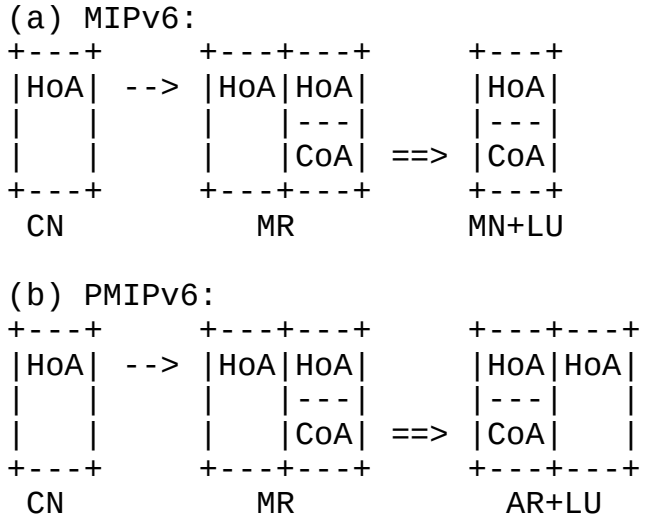

Figure 2. Network layer in the protocol stack of packets sent from the CN and tunneled (a) to the MN+LU in MIPv6; and (b) to the AR+LU in PMIPv6 showing the destination IP address as the packet traverses from the CN to the MN.

Figure 2 shows that, as far as data-plane traffic is concerned, routing from CN to MN+LU in MIPv6 is similar to the route from CN to AR+LU in PMIPv6. The difference is in that the MN with the LU function is substituted by the combination of the AR with the LU function and the MN. While additional signaling is needed to enable the combination of AR+LU and MN to behave like MN+LU, such signaling can be confined between the AR+LU and MN only. It can therefore be seen under this unified formulation, that a host-based mobility management protocol can be translated using this substitution into a network-based mobility management protocol and vice versa.

MIPv6 and PMIPv6 bundle all three mobility management logical functions: LM1, IP1 prefix allocation, and MR1 into the home agent (HA) and Local Mobility Anchor (LMA) respectively.

The functional representation of Proxy Mobile IPv6 [RFC5213] is shown in Figure 3. In PMIPv6, the combination of LM, MR, and HoA allocation is the Local Mobility Anchor (LMA), whereas the AR+LU combination together with additional signaling with MN comprises the Mobile Access Gateway (MAG). Here MN11 is attached to the access router AR31 which has the IP address IP31 in Network3. LM1 maintains the binding HoA11:IP31. The access router AR31 also behaves like a home link to MN11 so that MN11 can use its original IP address HoA11.

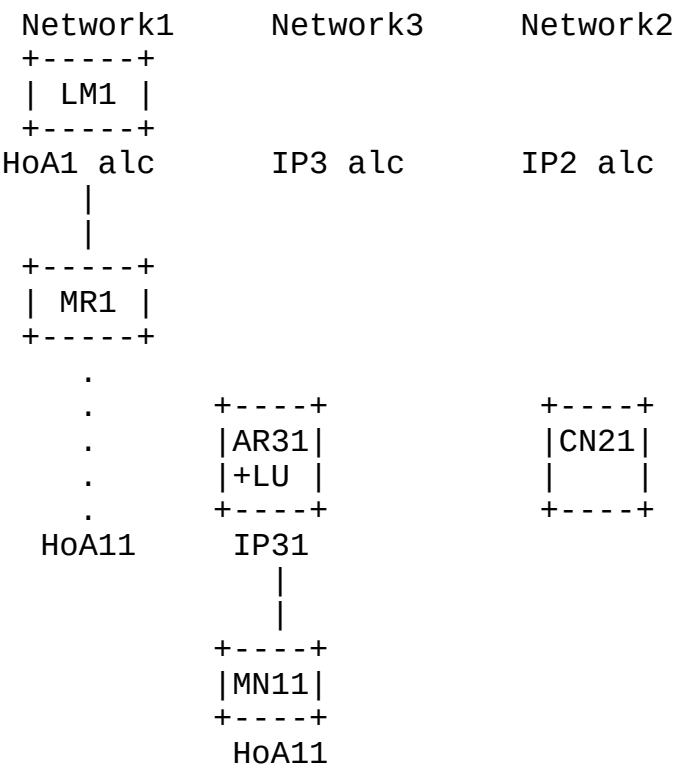

Figure 3. Functional representation of PMIPv6.

4.3. Hierarchical Mobile IPv6

The functional representation of Hierarchical Mobile IPv6 [RFC5380] is shown in Figure 4.

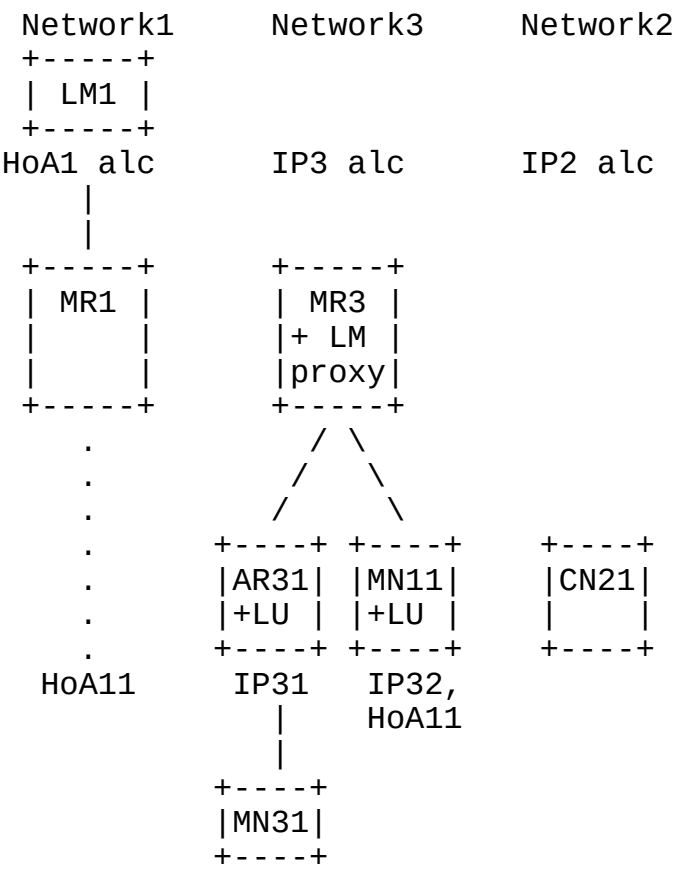

Figure 4. Functional representation of Hierarchical Mobile IPv6.

Besides the logical functions: LM1, MR1, and HoA1 prefix allocation in Network1 as MIPv6 in Figure 2 and PMIPv6 in Figure 3, there is an MR function (MR3) in the visited network (Network3). MR3 is also a proxy between LM1 and MN11 in the hierarchical LM function LM1--MR3--MN11. That is, LM1 maintains the LM binding HoA11:MR3 while MR3 keeps the LM binding HoA11:IP32. The combined function of MR and the LM proxy function is the Mobility Anchor Point (MAP).

In Figure 4, if MN11 takes the place of MN31 which is attached to AR31, the resulting mobility management becomes network-based.

4.4. Distributing mobility anchors

It is possible to repeat the mobility anchoring function for any of MIPv6, PMIPv6, or HMIPv6, in multiple networks as shown in Figure 5 which shows such an example with three networks.

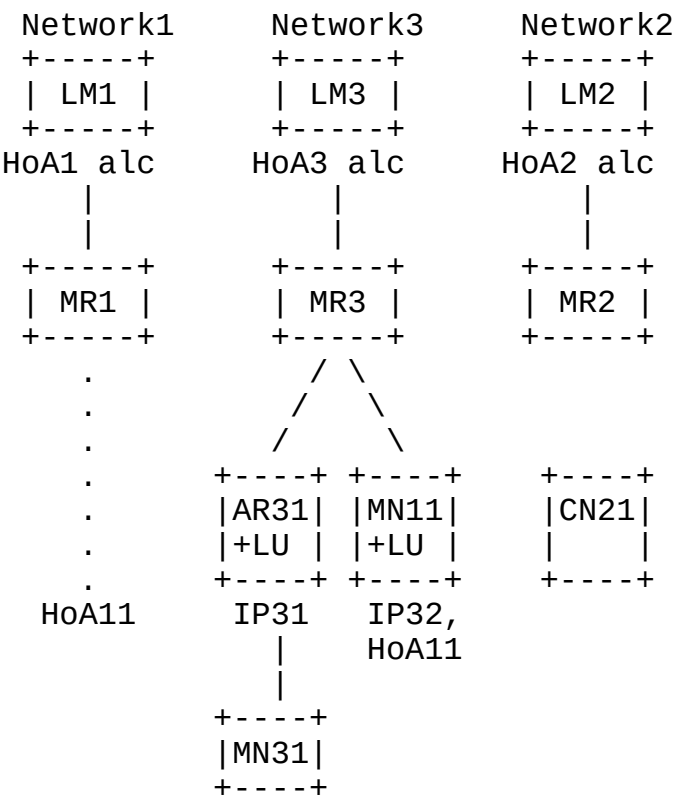

Figure 5. Functional representation of distributing mobility anchors.

4.5. Migrating Home Agents

When all these logical functions are bundled into one single entity e.g., a home agent in MIPv6 or a local mobility anchor in PMIPv6, in a single network, the result is triangular routing when the MN and the CN are in networks close to each other but are far from the anchor point.

A method to solve the triangle routing problem is to duplicate the anchor points in many networks in different geographic locations as in [Paper-Migrating.Home.Agents]. A functional representation of Migrating Home Agents is shown in Figure 6.

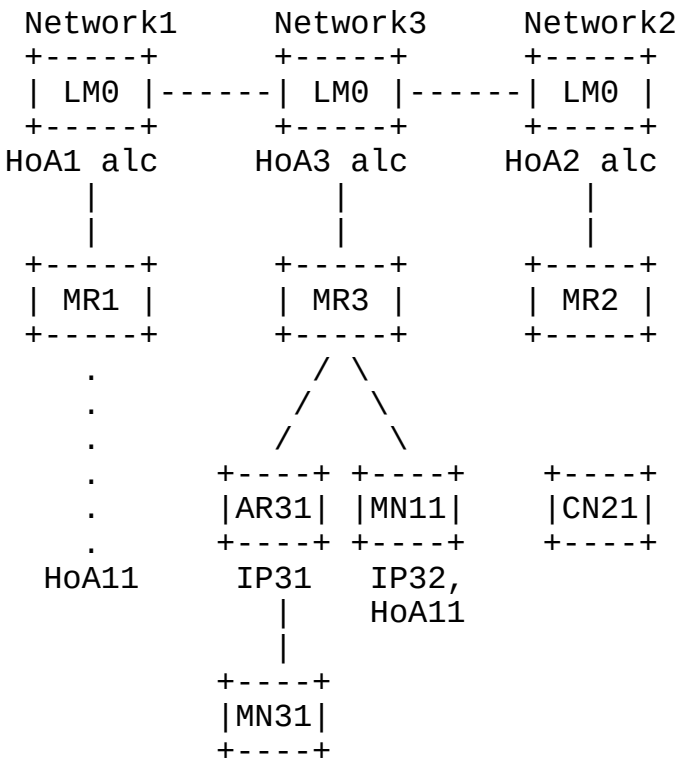

Figure 6. Functional representation of Migrating Home Agents.

Here, the MR function is available in each of the three networks Network1, Network2, and Network3. The LM function in each network (LM0) contains the LM information for all networks. Each MR in each network advertises the HoA IP prefixes of all these networks using anycast. Traffic from CN21 in Network2 destined to HoA11 will therefore be intercepted by the MR nearest to CN, which is MR2. Using the LM information in LM0, MR2 will use the binding HoA11:IP32 to tunnel the packets to MN11.

Similarly, traffic originating from MN11 will be served by its nearest MR (MR3). Triangular routing is therefore avoided. Yet the synchronization of all home agents becomes a challenge as discussed in [Paper-SMGI]. In addition, the amount of signaling traffic needed in synchronizing the home agents may become excessive when both the number of mobile nodes and the number of home agents increase.

As before, if MN11 in Figure 6 takes the place of MN31 which is attached to AR31, the resulting mobility management becomes network-based.

5. DMM Functional Scenarios

This section covers the functional description of DMM. Basically, the scenario presents a way to distribute the logical mobility functions. Gap analysis will be made on the functional scenarios.

5.1. Flat Network Scenario

In a flat network, the logical functions in the functional representation may all be located at the AR as shown in Figures 7 and 8, respectively. These two figures depict the network- and client-based distributed mobility management scenarios. The AR is expected to support the HoA allocation function. Then, depending on the mobility situation of the MN, the AR can run different functions:

1. the AR can act as a legacy IP router;

2. the AR can provide the MR function (i.e. act as mobility anchor);

3. the AR can provide the LU functions;

4. the AR can provide both MR and LU functions.

For example, [I-D.seite-dmm-dma] and [I-D.bernardos-dmm-distributed-anchoring] are PMIPv6 based implementation of this scenario.

5.1.1. Network-based Mobility Management

The functional description of network-based mobility management is depicted in Figure 7.

In case (1), MN1 attaches to AR1. AR advertises prefix HoA1 to MN1 and then acts as a legacy IP router. MN1 initiates a communication with CN11.

In case (2), MN1 performs a handover from AR1 to AR3 while maintaining ongoing IP communication with CN11. AR1 becomes the mobility anchor for the MN1-CN11 IP communication: AR1 runs MR and LM functions for MN1. AR3 performs LU up to the LM in AR1: AR3 indicates to AR1 the new location of the MN1. AR3 allocates a new IP prefix (HoA3) for new IP communications. HoA3 is supposed to be used for new IP communication, e.g., if MN1 initiates IP communication with CN21. AR3 shall act as a legacy IP router for MN1-CN21 communication.

In case (3), MN1 performs a handover from AR1 to AR2 with ongoing IP communication with CN11 and CN21. AR1 is the mobility anchor for the

MN1-CN11 IP communication. AR3 becomes the mobility anchor for the MN1-CN21 IP communication. Both AR1 and AR3 run MR and LM functions for MN1, respectively, anchoring HoA1 and HoA3. AR2 performs location updates up to the LMs in AR1 and AR3 for respectively relocate HoA1 and HoA3.

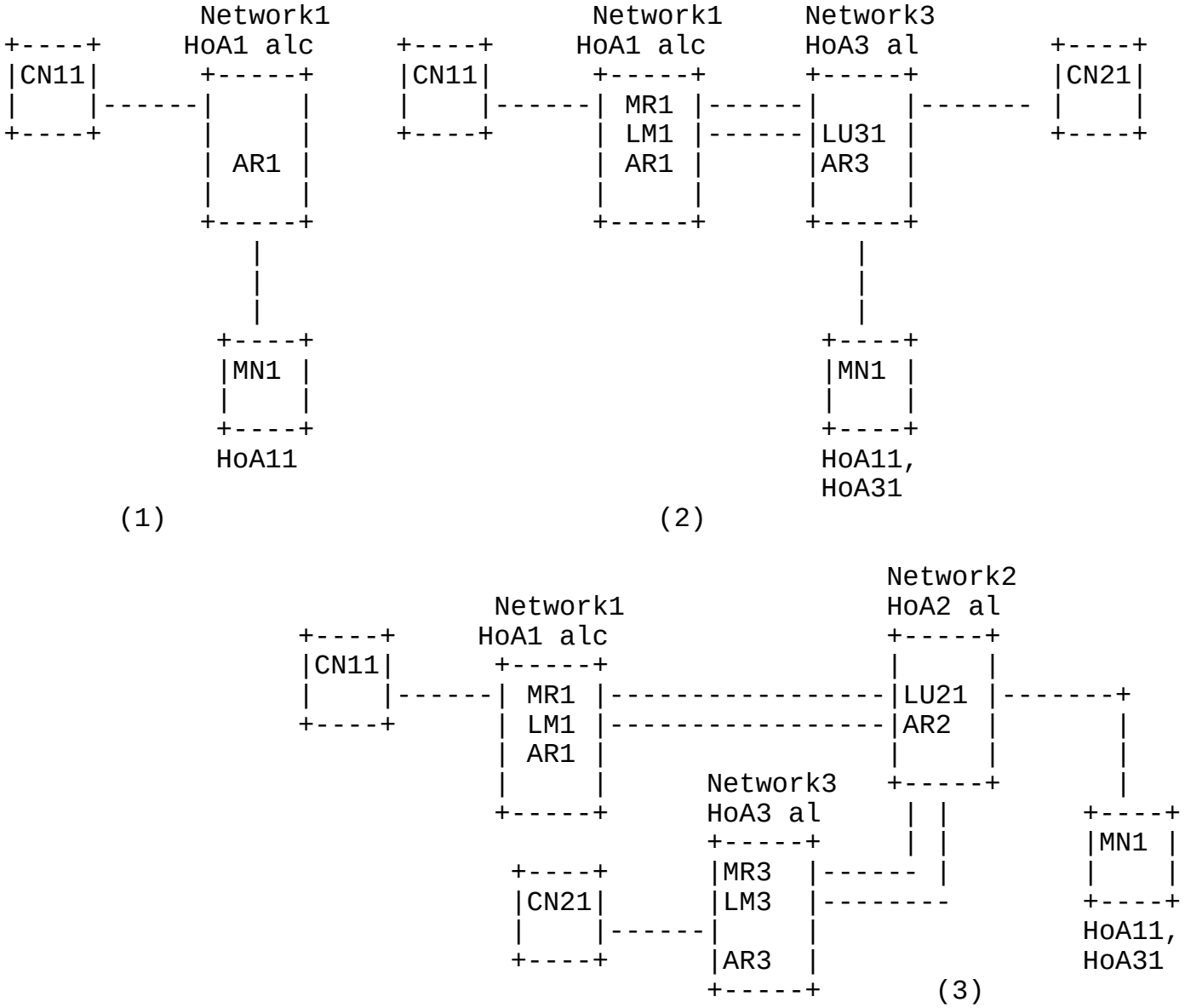

Figure 7. Network-based DMM architecture for a flat network.

5.1.2. Client-based Mobility Management

The functional description of client-based mobility management is depicted in Figure 8.

In case (1), MN1 attaches to AR1. AR advertises the prefix HoA1 to MN1 then acts as a legacy IP router. MN1 initiates a communication with CN11.

In case (2), MN1 performs a handover from AR1 to AR3 with ongoing IP communication with CN11. AR1 becomes the mobility anchor for the MN1-CN11 IP communication: AR1 runs MR and LM functions for MN1. The MN performs LU directly up to the LM in AR1 or via AR3; in this case AR3 acts as a proxy locator (pLU) (e.g. as a FA in MIPv4). AR3 allocates a new IP prefix (HoA3) for new IP communications. HoA3 is supposed to be used for new IP communications, e.g., if MN1 initiates IP communication with CN21. AR3 shall act as a legacy IP router for MN1-CN21 communication.

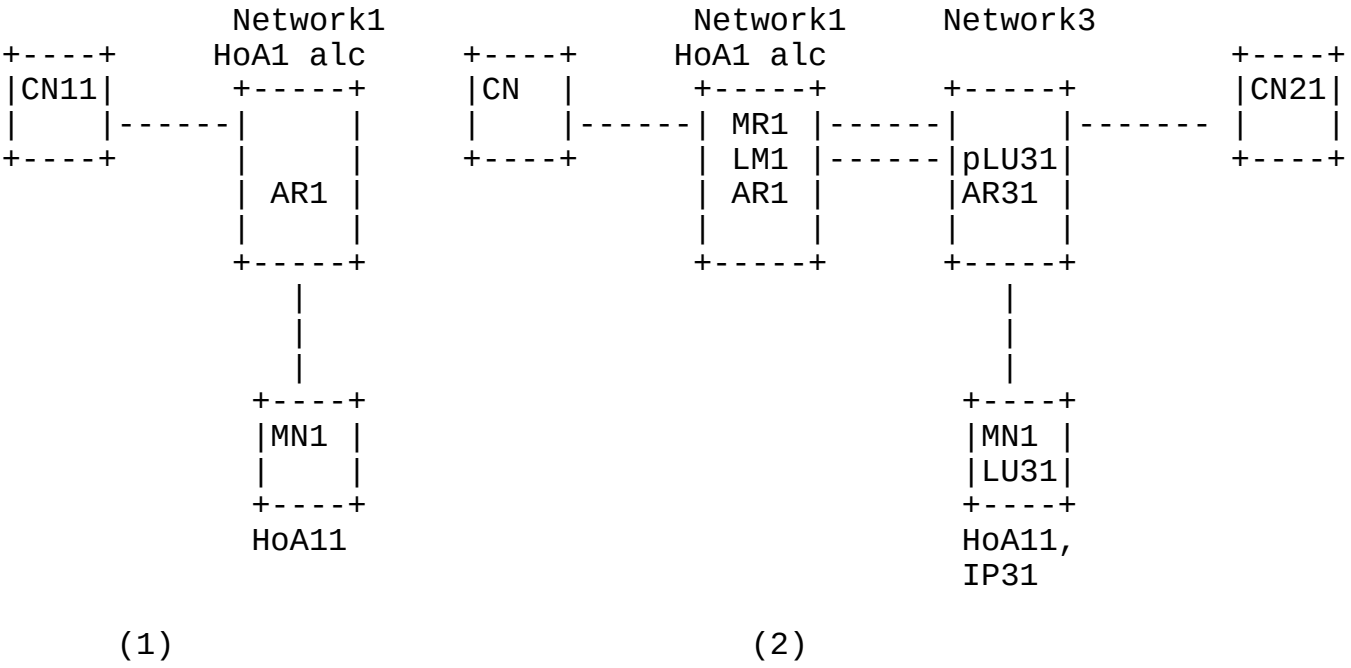

Figure 8. Client-based DMM architecture for a flat network.

5.2. Fully distributed scenario with separation of control and data planes

This scenario considers multiple MRs and a distributed LM database.

The different use case scenarios of distributed mobility management are described in [I-D.yokota-dmm-scenario] as well as in [Paper-Distributed.Mobility.Review]. The architecture described in this document is mainly on separating the data plane from the control plane.

Figure 9 shows an example DMM architecture with the same three networks as in Figure 5. As is in Figure 5, each network in Figure 9 has its own IP prefix allocation function. In the data plane, the mobility routing function is distributed to multiple locations at the MRs so that routing can be optimized. In the control plane, the MRs may exchange signaling with each other. In addition to these features in Figure 5, the LM function in Figure 9 is a distributed database, with multiple servers, of the mapping of HoA to CoA.

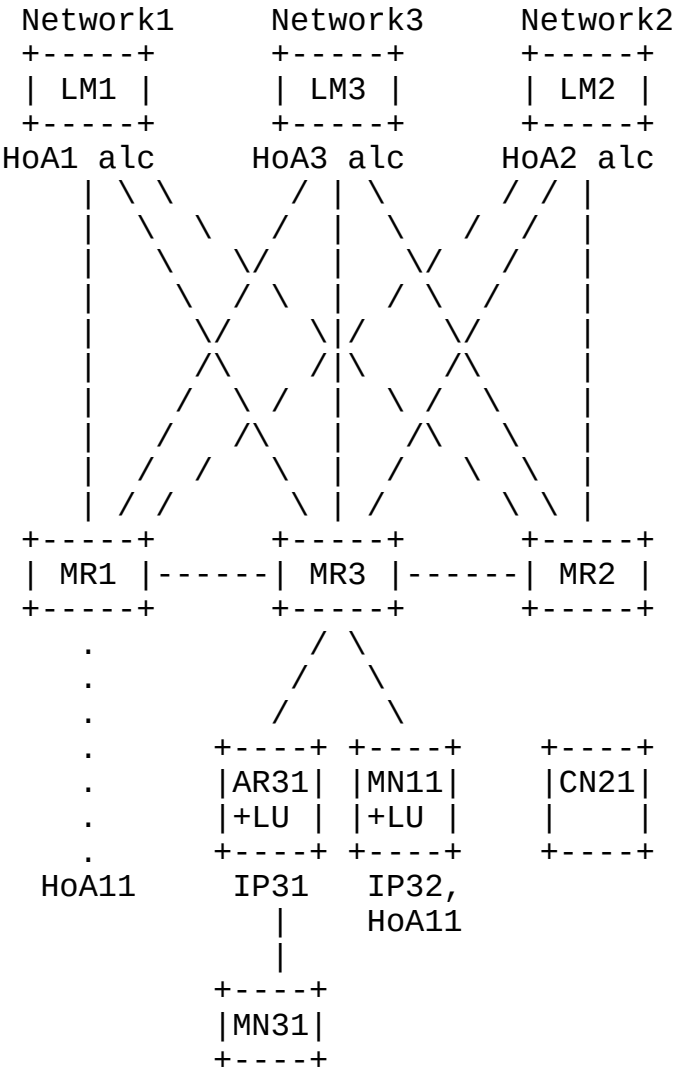

Figure 9. A distributed architecture for mobility management.

To perform mobility routing, the MRs need the location information which is maintained at the LMs. The MRs are therefore the clients of the LM servers and may also send location updates to the LM as the MNs perform the handover. The location information may either be

pulled from the LM servers by the MR, or pushed to the MR by the LM servers. In addition, the MR may also cache a limited amount of location information.

This figure shows three MRs (MR1, MR2, and MR3) in three networks. MN11 has moved from the first network supported by MR1 and LM1 to the third network supported by MR3 and LM3. It may use an HoA (HoA11) allocated to it when it was in the first network for those application sessions that had already started when MN11 was attached there and that require session continuity after the handover to the third network. When MN11 was in the first network, no location management is needed so that LM1 will not keep an entry of HoA11. After MN11 has performed its handover to the third network, the database server LM1 maintains a mapping of HoA11 to MR3. That is, LM1 points to the third network and it is the third network that will keep track of how to reach MN11. Such a hierarchical mapping can prevent frequent update signaling to LM1 as MN11 performs intra-network handover within the third network. In other words, the concept of hierarchical mobile IP [RFC5380] is applied here but only in location management and not in routing in the data plane.

6. Gap analysis

6.1. DMM Requirements

6.1.1. Considering existing protocols first

The fourth DMM requirement is on existing mobility protocols [ID-dmm-requirements:

REQ4: A DMM solution SHOULD first consider reusing and extending IETF-standardized protocols before specifying new protocols.

Abstracting the existing protocol functions into logical functions in this draft is a way to see how one can maximize the use of existing protocols. It remains to be seen whether all DMM requirements can be met. One needs to check the rest of the requirements to identify the gaps.

In addition, individual DMM proposals available at the IETF DMM working group are mostly based on the existing IETF-standardized protocols.

6.1.2. Compatibility

The first part of the fifth DMM requirement is on compatibility:

REQ5: (first part) The DMM solution MUST be able to co-exist with existing network deployments and end hosts. For example, depending on the environment in which DMM is deployed, DMM solutions may need to be compatible with other deployed mobility protocols or may need to interoperate with a network or mobile hosts/routers that do not support DMM protocols.

Different deployments using the same abstract functions are basically reconfiguration of these same functions if their functions use common message formats between these functions. A design principle of the IPv6 message format accommodates the use of common message formats as it allows to define extension headers, e.g., use of mobility header and options. It is shown in Section 4 that MIPv6, PMIPv6, HMIPv6, Distributing mobility anchors can be constructed from the abstract functions by adding more features and additional messages one on top of the other in the above order. The later protocol will therefore support the one from which the later is constructed by adding more messages.

6.1.3. IPv6 deployment

The third DMM requirement on IPv6 deployment is the following.

REQ3: DMM solutions SHOULD target IPv6 as the primary deployment environment and SHOULD NOT be tailored specifically to support IPv4, in particular in situations where private IPv4 addresses and/or NATs are used.

This is not an issue with MIPv6, PMIPv6 and their extensions. Using the unified scheme here based on abstracting these existing protocol functions will meet the DMM requirements as these protocols are originally designed for IPv6.

6.1.4. Security considerations

The first part of the fourth requirement as well as the sixth DMM requirement [ID-dmm-requirements] are as follows:

REQ5 (second part): Furthermore, a DMM solution SHOULD work across different networks, possibly operated as separate administrative domains, when allowed by the trust relationship between them.

REQ6: DMM protocol solutions MUST consider security aspects, including confidentiality and integrity. Examples of aspects to be considered are authentication and authorization mechanisms that allow a legitimate mobile host/router to use the mobility support provided by the DMM solution; signaling message protection in terms of authentication, encryption, etc.; data integrity and confidentiality;

opt-in or opt-out data confidentiality to signaling messages depending on network environments or user requirements.

It is preferred that these security requirements are considered as an integral part of the DMM design.

6.1.5. Distributed deployment

The first DMM requirement has 2 parts. The first part is on distributed deployment whereas the second part is on avoiding longer routes.

REQ1: (part 1)IP mobility, network access and routing solutions provided by DMM MUST enable distributed deployment for mobility management of IP sessions (part 2) so that traffic does not need to traverse centrally deployed mobility anchors and thus can be routed in an optimal manner.

With the first part, multiple MRs will become available in MIPv6 by simply having an HA for each home network. This is illustrated in terms of the logical functions as in Figure 9. Note that [Paper-Host.based.DMM] shows an example of a host-based DMM protocol based on MIPv6.

With the second part, one can examine dynamic mobility and route optimization to be discussed later.

6.1.6. Transparency to Upper Layers when needed

To see how to avoid traversing centralized deployed mobility anchors, let us look at the second requirement on non-optimal routes [ID-dmm-requirements].

REQ2: DMM solutions MUST provide transparent mobility support above the IP layer when needed. Such transparency is needed, for example, when, upon change of point of attachment to the Internet, an application flow cannot cope with a change in the IP address. Otherwise, support for maintaining a stable home IP address or prefix during handovers may be declined.

In order to avoid traversing long routes after the MN has moved to a new network, the new network can simply be used as the home network for new sessions. The sessions that had already started in the previous network would still need to use the original network in which the session had started as the home network. There may then be different IP sessions using different IP prefixes/addresses in the same MN.

The capability to use different IP addresses for different IP sessions are therefore needed.

The association with the HoA of an MN is not sufficient to support the above use of IP for an application. This gap can be overcome by generalizing the concept of the HoA of the MN to the HoA of an application running on the MN as will be discussed in Section 7.1 below.

Using the dynamic mobility management scheme has avoided routing back to the home network when the application does not have such a need. There are, however, application sessions that had originated from a prior network and that require mobility support. Longer routes than the natural IP route can therefore emerge. Route optimization schemes already exist, but one needs to deal with multiple HA's when using multiple HA's.

6.1.7. Route optimization

The second part of first requirement is on route optimization.

REQ1: (part 1)IP mobility, network access and routing solutions provided by DMM MUST enable distributed deployment for mobility management of IP sessions (part 2) so that traffic does not need to traverse centrally deployed mobility anchors and thus can be routed in an optimal manner.

One generalization in terms of the unified framework is that the LM functions can be considered as a distributed database as will be shown in the next section. There, the MN and the LM have a client-server relationship, with optionally a proxy in between and the proxy can be co-located with an MR. A distributed database may have different servers to store different data. The data in each server need not be pushed to all other servers but the database system only needs to know which data resides on which server. In addition, each client (i.e., MN) needs to be able to query the database.

Existing functions, such as BU and BA messages, can be considered as a method of database update function for the mobility context of the MN. Completing the design of messages for the database update functions will enable the distributed database design for route optimization.

In the unified scheme, complete with database and mobility routing functionalities, numerous route optimizations can be designed as described in Section 7.2.

6.2. Mobility Protocols Gap Analysis

6.2.1. Gap analysis with the unified framework

The use of the unified framework meets the following requirements:

REQ4: Considering existing protocols first

REQ5: (first part) compatibility

REQ3: IPv6 deployment

The unified framework has separated the HA function into an MR and an LM function. The following is needed in addition:

REQ6: Security - Trust between MR and LM is needed when they are not co-located.

6.2.2. Gap analysis with MIPv6

MIPv6 using the unified framework follows the above gap analysis with the unified framework. In addition, the following is needed.

REQ6: Security consideration

Trust between MN and MR is needed.

6.2.3. Gap analysis with PMIPv6

In terms of the unified framework, PMIPv6 differs from MIPv6 only in the sense that the combination of an AR and the MN in the network-based solution behaves like an MN in the host-based solution. While the gap analysis with MIPv6 applies here, the following change is needed: The trust between MN and MR in MIPv6 is therefore replaced by the trust between AR and MR, and trust between the AR and the MN is needed.

REQ6: Security consideration

Trust between AR and MR is needed.

Trust between MN and MR is needed.

6.2.4. Gap analysis with HMIPv6

In terms of the unified framework, HMIPv6 differs from MIPv6 and PMIPv6 only in the addition that packets are routed in the hierarchy MR(home network) -- MR(visited network) -- MN in MIPv6 or AR in

PMIPv6. While the gap analysis with MIPv6 and PMIPv6 applies to HMIPv6, the following additional trust relationship is needed between the MR's of different networks.

REQ6: Security consideration

Trust between MRs in different networks is needed.

6.2.5. Gap analysis with Distributing Mobility Anchors

The scenario of distributing mobility anchors is simply achieved with the implementation of the unified framework for MIPv6, PMIPv6, or HMIPv6 in each network of the multiple network. Therefore the gap analysis for MIPv6, PMIPv6, or HMIPv6 apply depending on which of these variants of MIP is used in these networks. In addition, the MR function is now available in different networks. The following requirement of distributed deployment is then met.

REQ1: Distributed deployment

The unified framework functions can be deployed in each of the multiple networks.

6.2.6. Gap analysis with HAHA

The scenario for Migrating Home Agent can be constructed from that of the distributing mobility anchors and modifying the LM in each network to propagate its data to all LM servers in all other networks. Therefore the gap analysis with distributing mobility anchors apply.

In addition, trust between the LM servers is needed.

REQ6: Security consideration

Trust among the LM servers is needed.

6.2.7. Gap analysis with Dynamic mobility management

In Section 6, the unified framework functions are built by extending that of the distributing mobility anchors scenario. Therefore the gap analyses with distributing mobility anchors apply to the dynamic mobility management. In addition,

REQ2: Transparency to upper layers when needed.

The home network and HoA was previously associated with an MN. By extending the concept to that of an application rather than an MN

which has multiple applications, dynamic mobility management can be achieved.

6.2.8. Gap Analysis with Multiple MRs and Distributed LM Database

In Section 7, an architecture of distributed mobility management is constructed from the unified framework functions and can be seen as an extension of the distributing mobility anchor scenario with dynamic mobility management support. Therefore the gap analyses for the dynamic mobility management also apply. In addition, the following gap analysis applies.

REQ1: (part 2) Distributed deployment

The LMs may generalize into a distributed database.

REQ6: Security considerations

Trust between the LM in a different network and the MR is needed.

6.2.9. Gap Analysis with Route Optimization Mechanisms

In Section 8, different possibilities to optimize the route using the architecture in Section 7 is described. Therefore the gap analyses for the DMM architecture in Section 7 apply. In addition, the following gap analyses apply.

REQ1: (part 2) Distributed deployment

MR may cache the LM information when needed.

MR function is needed in the CN’s network.

REQ6: Security considerations

Trust between the MR and the LM is needed.

6.3. Gap analysis summary

The gap analyses for different protocols are summarized in this section.

Table 1. Summary of Gap Analysis

	Existing protocols first	Compatibility	IPv6 deployment	Security considerations	Distributed deployment	Upper-layer transparency when needed	Route Optimization
Unified framework	Y	Y	Y				
MIPv6	Y	Y	Y	Y	N	N	N
PMIPv6	Y	Y (supports above)	Y	Y (MN-AR)	N	N	N
HMIPv6	Y	Y (supports above)	Y	Y (MN-AR)	N	N	N
Optimize route	Y	Y (supports above)	Y	Y	N	N	location privacy
Distribute mobility anchors	Y	Y (supports above)	Y	Y	Y	N	N
Multiple MRs and Distributed LM database	Y	Y (supports above)	Y	Y (LM-MR in different networks)	Y	Y	
Dynamic mobility	Y	Y (supports above)	Y	Y (LM,MR-MR in different networks)	Y	Y (HoA of appl)	most cases
DMM	Y	Y (supports above)	Y	Y (LM,MR-MR in different networks)	Y	Y (HoA of appl)	except 1st pkts

7. DMM analysis

This section analyses how DMM proposals meet above requirements.

7.1. DMM scenarios and Dynamic mobility management requirement

The distributed architecture described in Section 5.1, which has an MR and an HoA allocation function in each network, enables dynamic mobility management.

When new applications are started after the MN moves to a new network, the device can simply use a new IP address allocated by the new network. Dynamic mobility management, i.e., invoking mobility management only when needed, has been proposed in [Paper-Distributed.Dynamic.Mobility] and [Paper-Host.based.DMM].

The architecture with multiple mobility routing functions compared with a centralized approach is more appropriate for achieving dynamic mobility management. In Figure 9 above, the LM function and the IP address allocation function may be co-located. The device MN11, originally attached to the first network (Network1), may simply be using a dynamic IP address HoA11 which is leased from Network1 with a finite lifetime of, say, 24 hours. As MN11 leaves the first network and attaches to the third network (Network3), it acquires a new IP address IP33 from Network3. MN11 may or may not have ongoing sessions requiring session continuity. If it does not have, there is no need for LM1 to keep a binding for the home address HoA11 of MN11. If it does, it may use the existing MIPv6 signaling mechanism so that the LM1 will maintain the binding HoA11:MR3. MR3 in turn will maintain the binding HoA11:IP33. Such a hierarchy of binding with MR3 acting as the proxy location maintenance function between LM1 and MN11 will also cause MR3 to act as a proxy MR function between MR1 and MN11 so that packets destined to MR1 will be redirected to MR3.

When all ongoing sessions requiring session continuity terminate, it is possible for MN11 to deregister from LM1. Yet one may not assume the device will always perform the de-registration. Alternatively the lease of the dynamic IP address HoA11 will expire upon which LM1 will remove the binding.

In the event that the ongoing session outlives the lease of HoA11, MN11 will need to renew the lease with the IP address allocation function in the first network.

More details on dynamically providing mobility support are found in [ID.seite-dmm-dma], [ID.liu-dmm-dynamic-anchor-discussion], [ID.bernardos-dmm-pmip], [I-D.ma-dmm-armip], and [ID.sarikaya-dmm-dmipv6].

[I-D.seite-dmm-dma] describes dynamic mobility management using PMIPv6. In that document, MR, LM, and the HoA allocation functions are co-located at the access router in a flat network.

[Paper-Net.based.DMM], or equivalently the draft [I-D.seite-dmm-dma], also describes dynamic mobility management in which the MR and the HoA allocation functions are both co-located at the access router, whereas the LM information in each of these access routers are linked together under the hierarchy of a centralized LM server.

[Paper-Host.based.DMM] described fully distributed dynamic mobility management using MIPv6. An access mobility anchor (AMA) is introduced as a mobility anchor that provides the MR, LM, and HoA allocation functions. As a host-based DMM protocol, an MN is allowed to signal its movement to a serving AMA co-located at an access router. The serving AMA signals to other AMAs associated to the active sessions of the MN that enable session continuity for the sessions anchored to the other AMAs. No centralized LM server is required.

[ID.sarikaya-dmm-dmipv6] also described dynamic mobility management for a flat network, with separate data plane and control plane. The needed authentication is also described.

[ID.bernardos-dmm-pmip] co-locates the home prefix allocation function and the mobility routing function at the access router, which is then named Mobility Anchor and Access Router (MAAR) in that draft. The LM function is centralized and is named Central Mobility Database (CMD).

[I-D.ma-dmm-armip] again describes dynamic mobility management in which the MR and the HoA allocation function are both co-located at the access router.

[ID.liu-dmm-dynamic-anchor-discussion] describes the gaps and extensions needed to accomplish dynamic mobility management.

7.2. Route optimization of DMM scenarios

The distributed architecture has already enabled dynamic mobility management, as is described in [I-D.seite-dmm-dma], even when the routes are not optimized. Route optimization mechanism can be achieved in addition to dynamic mobility.

With the above architecture, there are a number of ways to enable reachability of an MN by packets sent from a CN using the mobility routing function.

The target to avoid unnecessarily long route is the direct route instead of a triangular route. In general, when a packet is sent from a CN in one network to an MN in another network, the direct route consists of the following 3 routing segments (RS):

RS1.CN-MR(CN): the route segment from the CN to the nearest MR;

RS2.MR(CN)-MR(MN): the route segment from the MR serving (and therefore being closest to) the CN to the MR serving the MN; and

RS3.MR(MN)-MN: the route segment from the MR serving the MN to the MN.

One may therefore examine the route optimization mechanism in terms of these 3 routing segments. In the first segment RS1:CN-MR(CN), the alternatives are:

RS1.CN-MR(CN).anycast: Use anycast to route the packet to the nearest MR function. Here, each MR includes all the HoAs in its route announcement as if each of them is the destination for the HoA. Such route announcements will affect the routing table such that the packet destined to an HoA will be routed to the nearest MR. The use of anycast to reach the nearest HA has been used in [Paper-Migrating.Home.Agents] but with a different distributed architecture of duplicating many HAs. It is again proposed in [Paper-Distributed.Mobility.PMIP].

RS1.CN-MR(CN).gw/ar: Co-locate the MR function at a convenient location to which the packet will always pass. Such locations may be the gateway router or the access router. This approach will be described later.
It is noted here that in a PMIPv6 design with a hierarchical network, the MAG generally is at the access router but LMA can be in the gateway router of a network. Whether a distributed mobility design enhances the MAG or the LMA may involve quite different mechanisms. Yet when looking at the logical function, it is basically the same MR function whether this function co-locates with the access router or the gateway router. This draft therefore put both approaches together. There is however a difference that the access router needs to perform proxy function when using PMIPv6. Yet the logical MR functions are the same.
It is again noted that in flattened network, the access router and the gateway router may merge together. With they are merged, the needed function is again the same logical MR function.

In the second segment RS2.MR(CN)-MR(MN), the alternatives are:

RS2.MR(CN)-MR(MN).query: The MR query the LM database and use the result to tunnel the packet to the MR serving the MN. In order words, the MR pulls the needed internetwork location information from the LM server. There will be a delay owing to the time taken to send this query and to receive the reply. Optionally, before receiving the reply, the first packet or the first few packets may

be forwarded using mip or pmip. Then the first packet may incur a triangle route rather than to wait for the query reply. After receiving the reply, the packet will be tunneled to the MR(MN). The result may be cached for forwarding subsequent packets.

RS2.MR(CN)-MR(MN).push: The MR routes the first packet to the home network using the existing MIPv6 or PMIPv6 mechanism. It will then be intercepted by the MR of the MN which, with the help of LM, knows whether the MN has moved to a different network and use the mapping in LM to tunnel the packet to the MR of the MN. Then the MR of the MN will inform MR of the CN to tunnel the packet directly to the MR of the MN in future. In order words, after MR(CN) has forwarded the first packet to MR(MN), the MR(MN) is triggered to push the location information to MR(CN). The MR of the CN may keep this information in its cache memory for forwarding subsequent packets.

In the final segment RS3.MR(MN)-MN, the MR may keep track of the location of MN and route to it using its intra-network mobility management mechanism.

Different designs using the above architecture can be made by taking different combinations of the different designs in the different route segments. For example, the overall design of DMM may be:

1. RS1.CN-MR(CN).anycast followed by RS2.MR(CN)-MR(MN).query:

2. RS1.CN-MR(CN).anycast followed by RS2.MR(CN)-MR(MN).push:

   An example is [Paper-Distributed.Mobility.PMIP] which is explained for network-based mobile IP but is also applicable to host-based mobile IP.

3. RS1.CN-MR(CN).gw/ar followed by RS2.MR(CN)-MR(MN).query:

   An example is in [I-D.luo-dmm-pmip-based-dmm-approach] or [I-D.liu-dmm-pmip-based-dmm-approach] in which the MR function is co-located at the MAG which is usually at the access router. Here, when CN is also an MN using PMIPv6, the packet sent from it naturally goes to the access router which takes the logical function of MR so that it will query the LM, which resides in the LMA. It then uses the query result to tunnel the packet to the MR(MN), which resides in the AR/MAG of the destination MN. The signaling flow and other details are described in the referenced draft.

   Another example is in [I-D.jikim-dmm-pmip]. In the signal driven approach, the MR is co-located the access router, which is

considered as an extension of MAG. The MR, i.e., the extended MAG, serving the CN queries the LM and cache the result so that it can tunnel packets to the MR serving the destination MN.

[I-D.liebsch-mext-dmm-nat-phl] also co-locates the MR at the gateways. The gateway which serves the network of transmitting node and where the MR is co-located is called the Ingress router, whereas that at the network of the MN at the receiving side is called egress router. Instead of tunneling between these 2 gateways, header rewrite using NAT is used to forward the packet through the internetwork route segment.

4. RS1.CN-MR(CN).gw/ar followed by RS2.MR(CN)-MR(MN).push:

Another example is described in [Paper-Distributed.Mobility.Management].

8. Security Considerations

TBD

9. IANA Considerations

None

10. References

10.1. Normative References

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

10.2. Informative References

[I-D.bernardos-dmm-distributed-anchoring]
Bernardos, CJ. and JC. Zuniga, "PMIPv6-based distributed anchoring", draft-bernardos-dmm-distributed-anchoring-01 (work in progress), September 2012.

[I-D.bernardos-dmm-pmip]
Bernardos, C., Oliva, A., Giust, F., Melia, T., and R. Costa, "A PMIPv6-based solution for Distributed Mobility Management", draft-bernardos-dmm-pmip-01 (work in progress), March 2012.

[I-D.jikim-dmm-pmip]
Kim, J., Koh, S., Jung, H., and Y. Han, "Use of Proxy Mobile IPv6 for Distributed Mobility Management", draft-jikim-dmm-pmip-00 (work in progress), March 2012.

[I-D.liebsch-mext-dmm-nat-phl]
Liebsch, M., "Per-Host Locators for Distributed Mobility Management", draft-liebsch-mext-dmm-nat-phl-02 (work in progress), October 2012.

[I-D.liu-dmm-dynamic-anchor-discussion]
Liu, D., Deng, H., and W. Luo, "DMM Dynamic Anchor Discussion", draft-liu-dmm-dynamic-anchor-discussion-00 (work in progress), March 2012.

[I-D.liu-dmm-pmip-based-approach]
Liu, D., Song, J., and W. Luo, "PMIP Based DMM Approaches", draft-liu-dmm-pmip-based-approach-02 (work in progress), March 2012.

[I-D.luo-dmm-pmip-based-dmm-approach]
Luo, W. and J. Liu, "PMIP Based DMM Approaches", draft-luo-dmm-pmip-based-dmm-approach-01 (work in progress), March 2012.

[I-D.ma-dmm-armip]
Ma, Z. and X. Zhang, "An AR-level solution support for Distributed Mobility Management", draft-ma-dmm-armip-00 (work in progress), February 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.sarikaya-dmm-dmipv6]
Sarikaya, B., "Distributed Mobile IPv6", draft-sarikaya-dmm-dmipv6-00 (work in progress), February 2012.

[I-D.seite-dmm-dma]
Seite, P. and P. Bertin, "Distributed Mobility Anchoring", draft-seite-dmm-dma-05 (work in progress), July 2012.

[I-D.xue-dmm-routing-optimization]
Xue, K., Li, L., Hong, P., and P. McCann, "Routing optimization in DMM",

draft-xue-dmm-routing-optimization-00 (work in progress), June 2012.

[I-D.yokota-dmm-scenario]
Yokota, H., Seite, P., Demaria, E., and Z. Cao, "Use case scenarios for Distributed Mobility Management", draft-yokota-dmm-scenario-00 (work in progress), October 2010.

[MHA] Wakikawa, R., Valadon, G., and J. Murai, "Migrating Home Agents Towards Internet-scale Mobility Deployments", Proceedings of the ACM 2nd CoNEXT Conference on Future Networking Technologies, Lisboa, Portugal, December 2006.

[Paper-Distributed.Centralized.Mobility]
Bertin, P., Bonjour, S., and J-M. Bonnin, "Distributed or Centralized Mobility?", Proceedings of Global Communications Conference (GlobeCom), December 2009.

[Paper-Distributed.Dynamic.Mobility]
Bertin, P., Bonjour, S., and J-M. Bonnin, "A Distributed Dynamic Mobility Management Scheme Designed for Flat IP Architectures", Proceedings of 3rd International Conference on New Technologies, Mobility and Security (NTMS), 2008.

[Paper-Distributed.Mobility.Management]
Chan, H., "Distributed Mobility Management with Mobile IP", Proceedings of IEEE ICC 2012 Workshop on Telecommunications: from Research to Standards, June 2012.

[Paper-Distributed.Mobility.PMIP]
Chan, H., "Proxy Mobile IP with Distributed Mobility Anchors", Proceedings of GlobeCom Workshop on Seamless Wireless Mobility, December 2010.

[Paper-Distributed.Mobility.Review]
Chan, H., Yokota, H., Xie, J., Seite, P., and D. Liu, "Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues", February 2011.

[Paper-Host.based.DMM]
Lee, JH., Bonnin, JM., and X. Lagrange, "Host-based Distributed Mobility Management Support Protocol for IPv6 Mobile Networks", Proceedings of IEEE WiMob, Barcelona, Spain, October 2012.

[Paper-Migrating.Home.Agents]

Wakikawa, R., Valadon, G., and J. Murai, "Migrating Home Agents Towards Internet-scale Mobility Deployments", Proceedings of the ACM 2nd CoNEXT Conference on Future Networking Technologies, December 2006.

[Paper-Net.based.DMM]
Giust, F., de la Oliva, A., Bernardos, CJ., and RPF. Da Costa, "A network-based localized mobility solution for Distributed Mobility Management", Proceedings of 14th International Symposium on Wireless Personal Multimedia Communications (WPMC), October 2011.

[Paper-SMGI]
Zhang, L., Wakikawa, R., and Z. Zhu, "Support Mobility in the Global Internet", Proceedings of ACM Workshop on MICNET, MobiCom 2009, Beijing, China, September 2009.

[RFC4068] Koodli, R., "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.

[RFC4988] Koodli, R. and C. Perkins, "Mobile IPv4 Fast Handovers", RFC 4988, 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.

[RFC5949] Yokota, H., Chowdhury, K., Koodli, R., Patil, B., and F. Xia, "Fast Handovers for Proxy Mobile IPv6", RFC 5949, September 2010.

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

Authors' Addresses

H Anthony Chan
Huawei Technologies
5340 Legacy Dr. Building 3, Plano, TX 75024, USA
Email: h.a.chan@ieee.org

Pierrick Seite
France Telecom - Orange
4, rue du Clos Courtel, BP 91226, Cesson-Sevigne 35512, France
Email: pierrick.seite@orange-ftgroup.com

Kostas Pentikousis
Huawei Technologies
Carnotstr. 4 10587 Berlin, Germany
Email: k.pentikousis@huawei.com

Jong-Hyouk Lee
Telecom Bretagne
RSM Department, Telecom Bretagne, Cesson-Sevigne, 35512, France
Email: jh.lee@telecom-bretagne.eu