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

D. Liu
China Mobile
H. Chan
Huawei Technologies
P. Seite
France Telecom - Orange
December 8, 2012

Distributed Mobility Management: Current practices and gap analysis
draft-liu-dmm-best-practices-gap-analysis-00

Abstract

This document discusses how to best deploy the current IP mobility protocols in distributed mobility management (DMM) scenarios and analyzes the gaps of such best current practices against the DMM requirements. These best current practices are achieved by redistributing the existing MIPv6 and PMIPv6 functions in the DMM scenarios. The analyses is also applied to the real world deployment of IP mobility in WiFi network and in cellular network.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

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

Copyright Notice

Table of Contents

1. Introduction

The distributed mobility management (DMM) WG has studied the problems of centralized deployment of mobility management protocols and the requirements of DMM [ID-dmm-requirements]. In order to guide the deployment and before defining any new DMM protocol, the DMM WG is chartered to investigate first whether it is feasible to deploy current IP mobility protocols in DMM scenario in a way that can meet the requirements of DMM. This document discusses how to best deploy existing mobility protocols in DMM scenarios to solve the problems of centralized deployment. It then analyzes the gaps of such best practices against the DMM requirements.

The rest of this document is organized as follows:

Section 3 analyzes the current IP mobility protocols by examining their existing functions and how these functions can be reconfigured to achieve the best practices in DMM scenarios. Section 4 presents the current practices of WiFi network and 3GPP network. With WiFi, a DMM scenario is the flattened WiFi network. After presenting the fundaments what one can do to achieve distribution, the existing mobility management functions are reconfigured in the flattened networks for both network- and host-based mobility protocols using these fundaments as guiding priciples. The current practices in 3GPP are also described, and the DMM scenarios are LIPA and SIPTO. Section 5 presents the gap analyses on the best practice achieved by reconfiguring currently existing functions in the DMM scenario which applies to both those in the WiFi and the 3GPP networks.

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. Current IP mobility protocol analysis

3.1. IP mobility protocols and their mobility management functions

The host-based Mobile IPv6 [RFC6275] and its network-based extension, PMIPv6 [RFC5213], are both a logically centralized mobility management approach addressing primarily hierarchical mobile networks. Although they are a centralized approach, they have important mobility management functions resulting from years of extensive work to develop and to extend these functions. It is therefore fruitful to take these existing functions and reconfigure them in a DMM scenario in order to understand how to best deploy the existing mobility protocols in a distributed mobility management environment.

The existing mobility management functions of MIPv6, PMIPv6, and HMIPv6 are the following:

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;

Figure 1 shows Mobile IPv6 [RFC6275] and Proxy Mobile IPv6 [RFC5213] with their existing mobility management functions. In Network1, the combination of the functions MR, LM and HoA allocation in network1 is the home agent in MIPv6 and is the local mobility anchor in PMIPv6. In Network3, the AR32+LU combination together with additional signaling with MN comprises the Mobile Access Gateway (MAG) in PMIPv6. The mobile nodes MN11 and MN12 were originally attached to Network1 and were allocated the IP prefixes for their respective home addresses HoA11 and HoA12.

Using MIPv6, MN11 has moved to Network3, from which it is allocated a new prefix to configure the IP address IP31. LM1 maintains the binding HoA11:IP31 so that packets from CN21 in Network2 destined to HoA11 will be intercepted by MR1, which will then tunnel them to IP31. MN11 must perform mobility signaling using the LU function.

Using PMIPv6, MN12 has moved to Network3 and attached to the access router AR32 which has the IP address IP32 in Network3. LM1 maintains the binding HoA12:IP32. The access router AR32 also behaves like a home link to MN12 so that MN12 can use its original IP address HoA12.

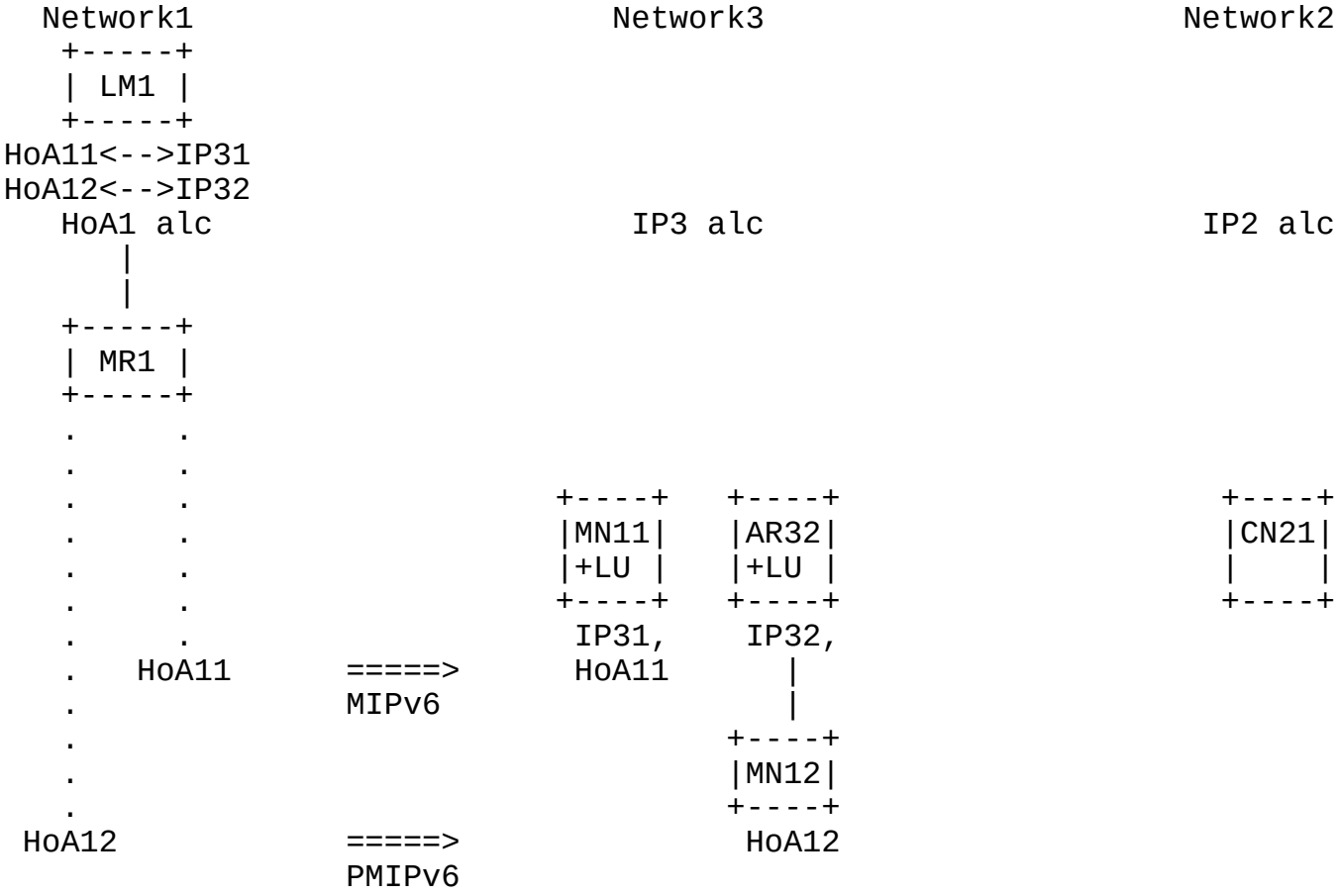

Figure 1. MIPv6, PMIPv6 and their functions.

3.2. Reconfiguring existing functions in DMM scenario

In order to best deploy current protocols in DMM scenario, the existing mobility functions of MIPv6, PMIPv6, and HMIPv6 configured into a DMM scenario as follows.

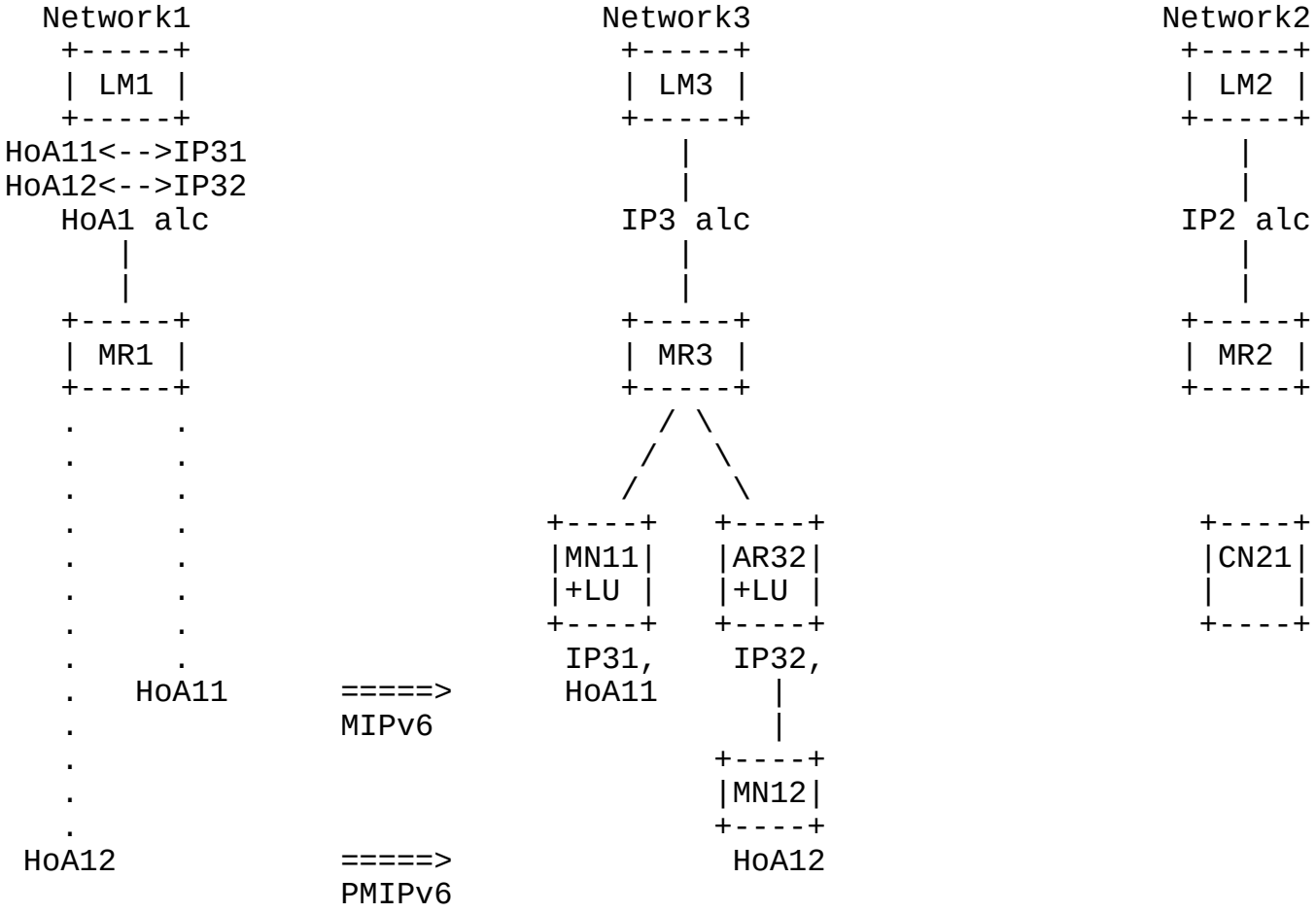

Figure 2. Reconfiguring existing functions in DMM scenario.

Achieving the best practices by reconfiguring the existing functions in this manner will be applied to the DMM scenario of a flattened WiFi network in Section 4.2.

4. Current practices of IP mobility protocols

This section covers the practices for distribution of IP mobility management. Basically, the scenario presents a way to distribute the logical mobility functions. Gap analysis will be made on these scenarios.

4.1. Fundamentals of distribution

There are many possibilities to implement a distributed mobility management system and this document could not be exhaustive. However, this document is supposed to focus on current mobility architectures and to reuse existing mobility protocol as much as

possible; it thus allows fixing the main technical guidelines and assumptions for current practices. Then, gap analysis will analyze these basic solution guidelines with respect to the requirements from [ID.ietf.dmm.requirements] and pave the way for optimizations. Technical guidelines for DMM current practices are as follows:

The technical assumptions or guidelines are:

1. When mobility support is required, the system will select the mobility anchor closest to the MN.
2. This document focuses on mobility management realized by preservation of the IP address across the different points of attachment during the mobility. IP flows of applications which do not need constant IP address are not handled by DMM. It is typically the role of a connection manager to distinguish application capabilities and trigger the mobility support accordingly. Further considerations on application management are out of the scope of this document.
3. IP address preservation is ensured thanks to traffic redirection.
4. Mobility traffic redirection is limited within the access network, e.g., traffic redirection taking place between access routers. In this document, traffic redirection relies on Network based mobility management protocols like PMIP [RFC 5213] or GTP [TS 23.402]. Mobility management and traffic redirection come into play only when the MN moves from the point of attachment where the IP flow has been initiated; in case of mobility, this point of attachment becomes the anchoring point. It implies that the MN could be managed by more the one anchor when more than one IP flow, initiated within different points of attachment, are running.
5. An access router will advertise anchored prefixes and a local prefix, i.e., a prefix topologically valid at the access router. When being initiated, an IP communication must prefer the local prefix to the anchored prefix. Prefix management is realized with IPv6 prefix deprecation.

4.2. Flattening the WiFi Network

The most common Wi-Fi architectures are depicted on figure 3. In some cases, these architectures can rely on Proxy Mobile IPv6, where the access aggregation gateway plays the role of LMA and the MAG is supported either by the Residential Gateway (RG), the WLAN Controller (WLC) or an Access Router (AR) [ID. gundavelli-v6ops-community-wifi-svcs].

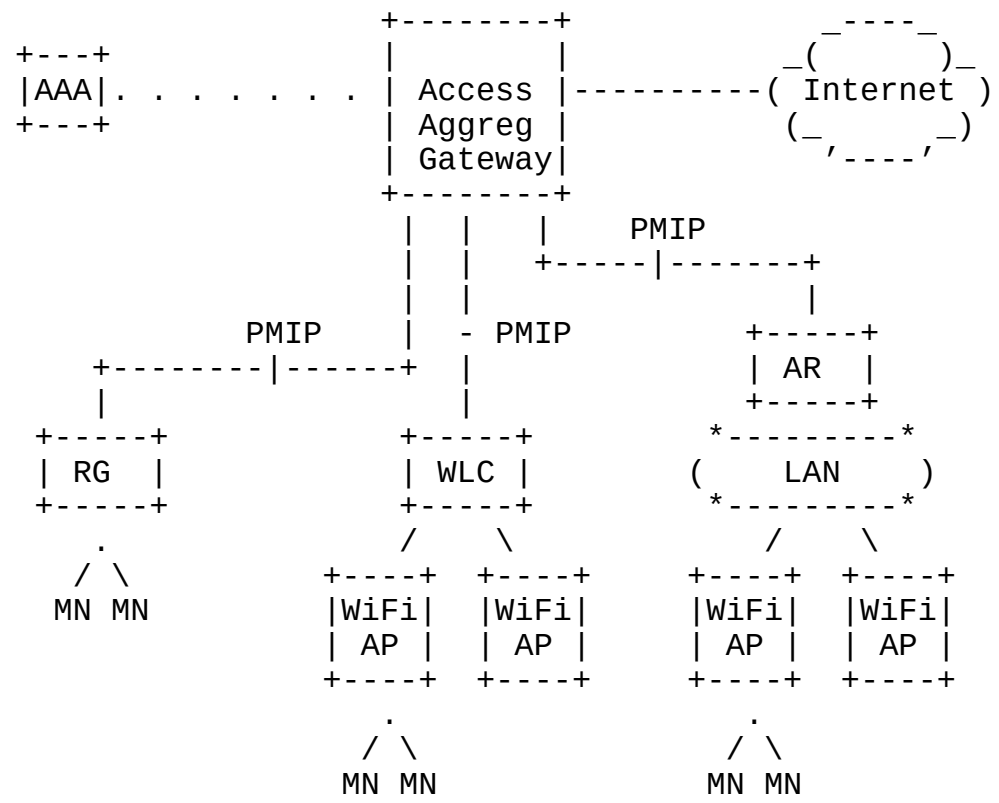

Figure 3. WiFi network architectures.

Because of network densification and distribution of content, it may be necessary to distribute the access aggregation gateway functions closer to the MN; see [ID.ietf-dmm-requirements] for motivation of network flattening. In an extreme distribution case, the access aggregation gateway functions, including the mobility management functions, may all be located at the AR as shown in Figures 4 and 5, 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.

4.2.1. Network-based Mobility Management

Basic practices for distribution of network-based mobility management is depicted in Figure 4.

Initially, MN1 attaches to AR1, (1). According to vanilla IPv6 operations, AR1 advertises a prefix (HoA1) to MN1 and then, AR1, acts as a legacy IP router. Then, MN1 initiates a communication with CN11 using an IP address formed from the prefix HoA1. So, AR1 runs usual IP routing? and mobility management does not come into play.

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 advertises both HoA1 and a new IP prefix (HoA3) which is supposed to be used for new IP communication, e.g., if MN1 initiates IP communication with CN21. Prefix HoA1 is deprecated as it is expected to be used only for communications anchored to AR1. AR3 shall act as a legacy IP router for MN1-CN21 communication, i.e., mobility management does not come.

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. AR2 advertises a new prefix (HoA2), expected to be used for new IP communications, and deprecates HoA1 and HoA3 used by the anchored IP sessions.

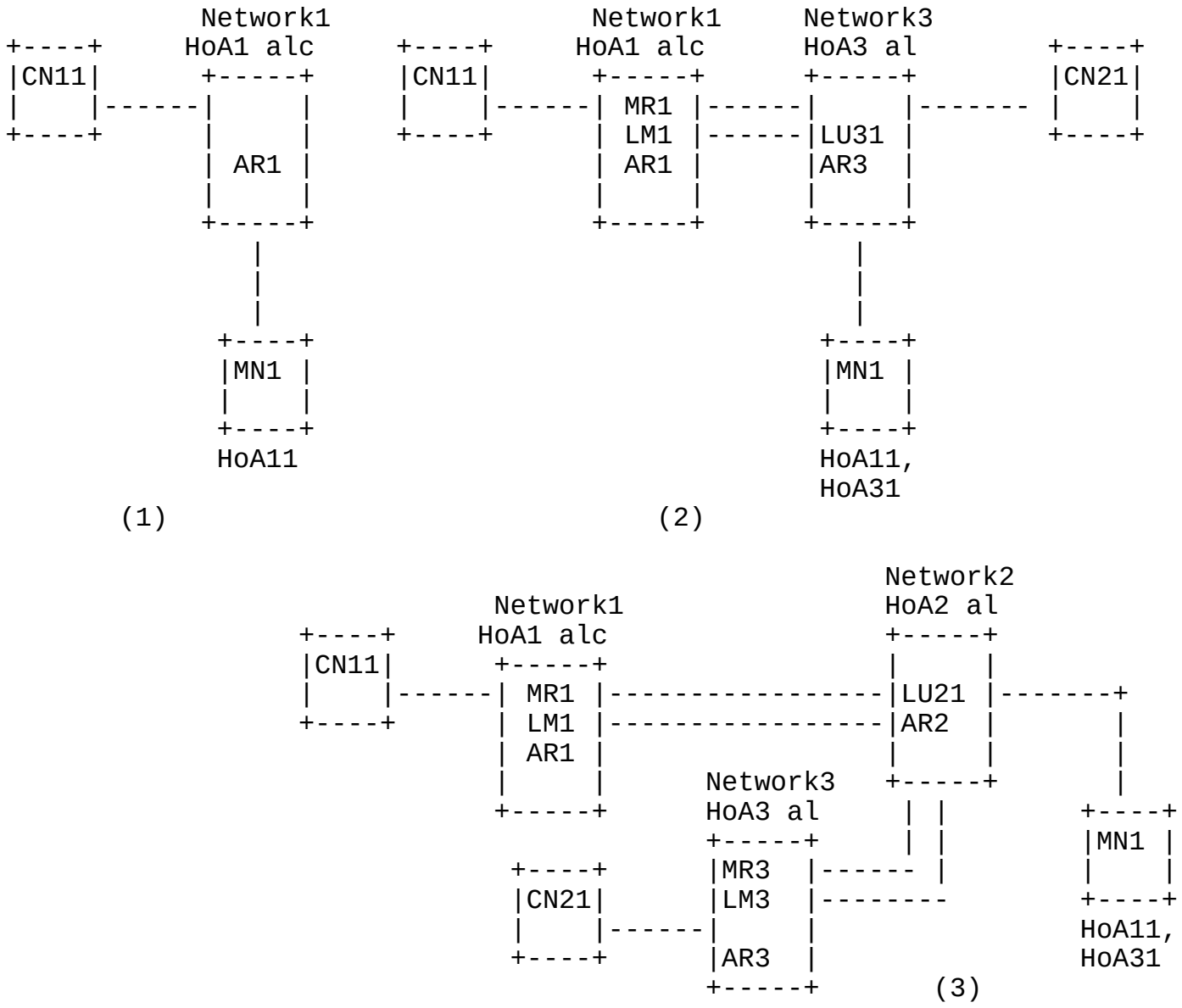

Figure 4. Network-based DMM architecture for a flat network.

4.2.2. Client-based Mobility Management

Basic practices for distribution of client-based mobility management is depicted in Figure 5. Here, client-based mobility management does not necessary implies Mobile IP because, according to distribution fundamentals (section 4.1), current practices rely on principles inherited from PMIP and traffic redirection takes place only between access routers. However, with client based mobility, the MN is authorized to send information on its ongoing mobility session; for example in order to facilitate localization update operations [I-D.seite-dmm-dma].

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.

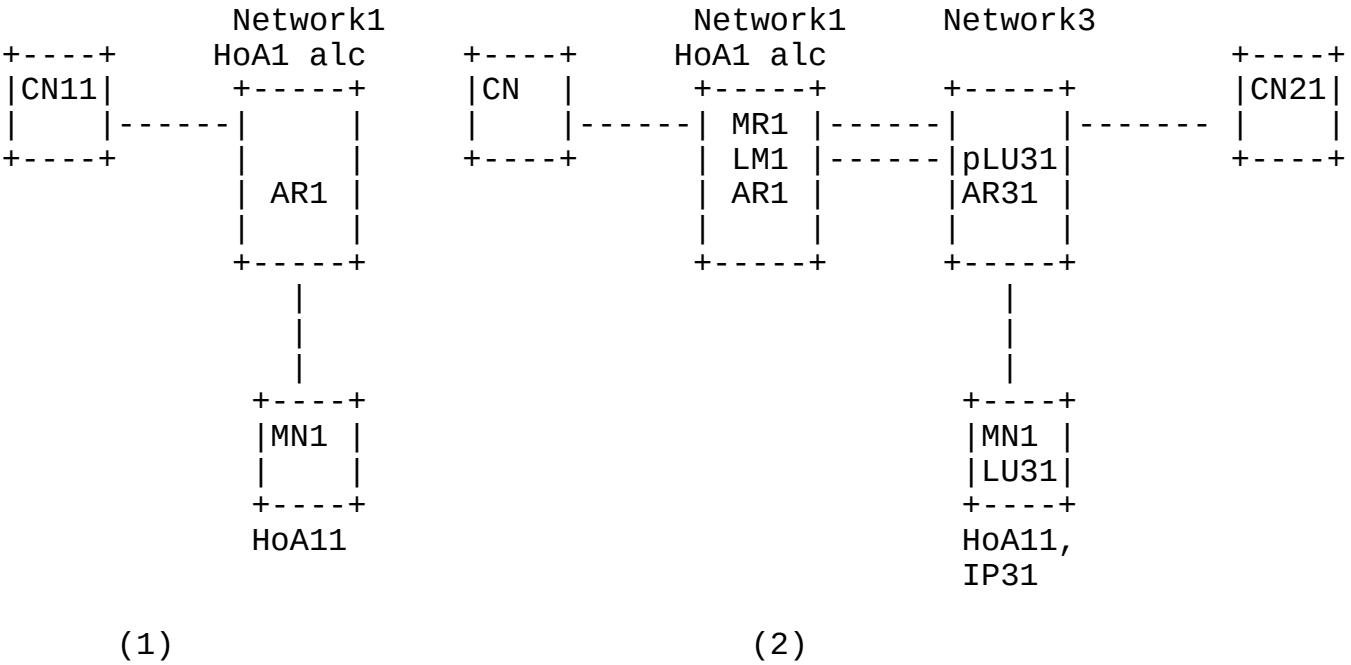

Figure 5. Client-based DMM architecture for a flat network.

4.3. IP mobility protocol deployment in 3GPP network

The 3rd Generation Partnership Project (3GPP) is the standard development organization that specifies the 3rd generation mobile network and LTE (Long Term Evolution). By November 2, 2012, there are 113 commercial LTE networks in 51 countries already deployed, and there are 360 operators in 105 countries investing in LTE. GSA forecasts 166 commercial LTE networks in 70 countries by end of 2012.

The 3GPP SAE network architecture is visualized in the Figure 6:

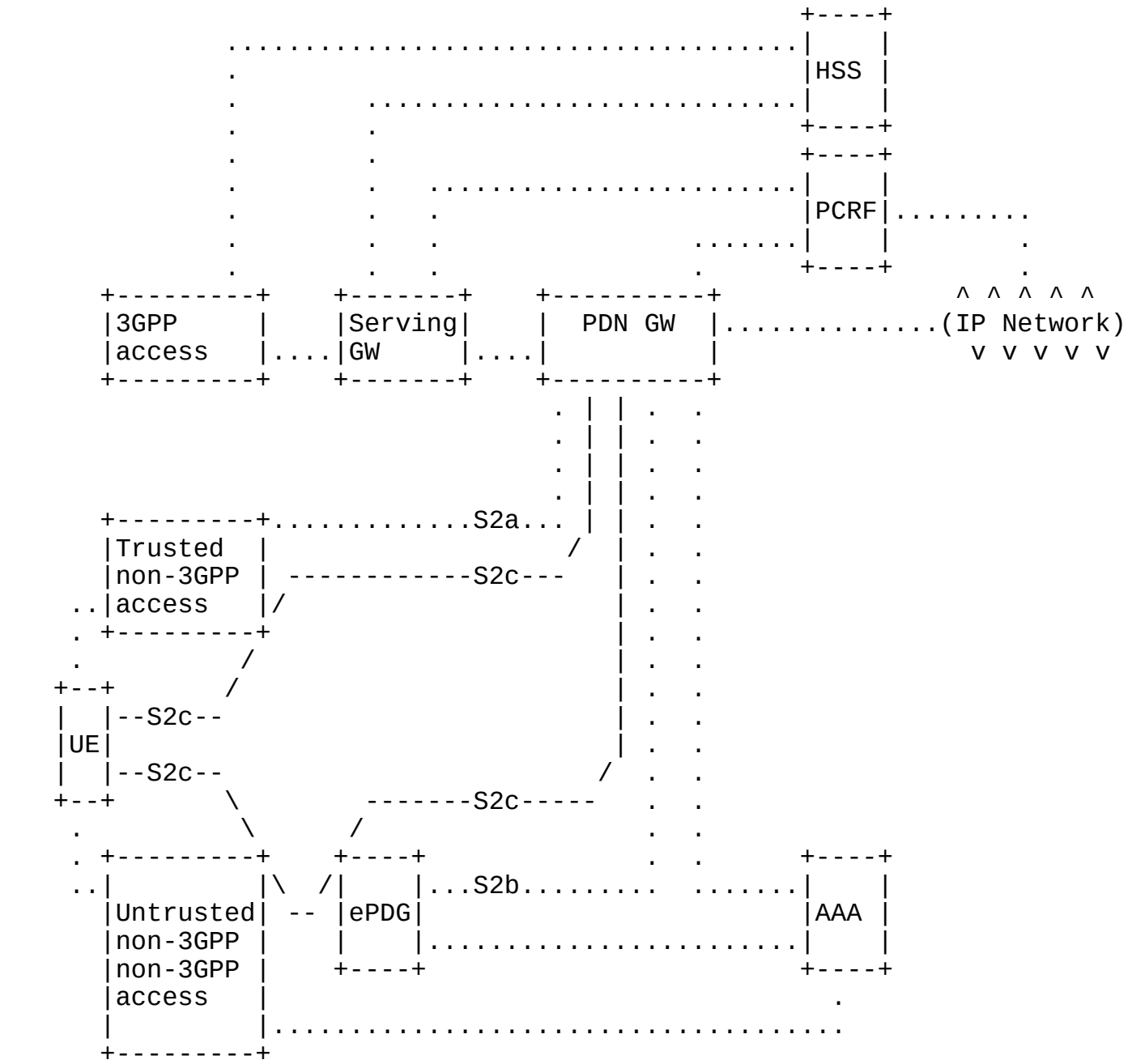

Figure 6. 3GPP SAE architecture.

In SAE architecture, there are two types of non-3GPP access network: trusted and untrusted. Trusted non-3GPP access means that the non-3GPP access network has a trust relationship with the 3GPP operator. Untrusted means the operator considers the non-3GPP network as untrusted, the non-3GPP network may either be or not be deployed by the same operator. The mobility support within the 3GPP network mostly relies on s5/s8 interface which is based on GTP or PMIP. For

the scenario which provide non-3GPP network and 3GPP network mobility, there are mainly three solutions that is using IP mobility protocol:

In 3GPP SAE architecture, there are three interfaces that use IP mobility protocol:

1. S2a Interface: S2a is the interface between trusted non-3GPP access network and the EPC. This interface could be based on GTP or PMIP. When using PMIP, the PDN gateway in the EPC will function as LMA. The mobile station will anchor at this LMA/ PDN-Gateway entity. The mobile station will maintain the session continuity when handover between the non-3GPP access network and 3GPP network.
2. S2b Interface: S2b is the interface between the trusted-non-3GPP access network and the PDN gateway. This interface is based on PMIP. The PDN-gateway functions as PMIP LMA. The mobile station will anchor at this LMA/PDN-Gateway entity. The ePDG in the EPC network will function as PMIP MAG. The mobile station will maintain the session continuity when handover between the non-3GPP access network and 3GPP network.
3. S2c Interface: S2c is the interface between the mobile station and the EPC network. It can be used in both trusted and un-trusted 3GPP access network. S2c interface uses DSMIPv6 protocol which is specified by IETF. The PDN gateway functions as DSMIPv6 Home agent in this scenario. When using non-trusted-non-3GPP access network, the mobile station will first establish IPSec tunnel toward the ePDG, and runs DSMIPv6 inside this IPSec tunnel. The mobile station will maintain the session continuity when handover between the non-3GPP access network and 3GPP network.

4.3.1. 3GPP LIPA/SIPTO

Another scenario that uses IP mobility protocol in 3GPP currently is the LIPA/SIPTO scenario. LIPA stands for Local IP Access. The following figure shows the LIPA scenario.

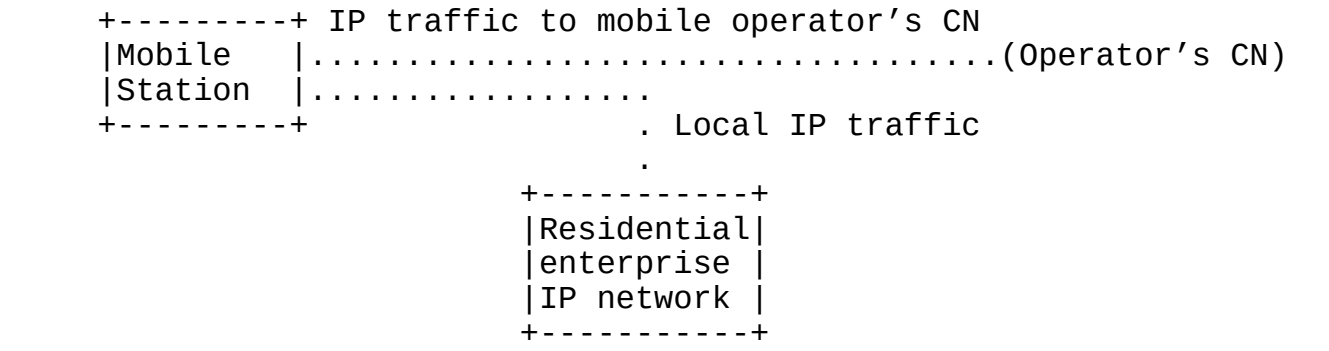

Figure 7. LIPA scenario.

The main feature of LIPA is that the mobile station can access a local IP network through H(e)NB. H(e)NB is a small, low-power cellular base station, typically designed for use in a home or enterprise. The mobile station can access the local network's service, for example, connect to a user home's TV, computers, picture libraries etc. The LIPA architecture is illustrated in Figure 8.

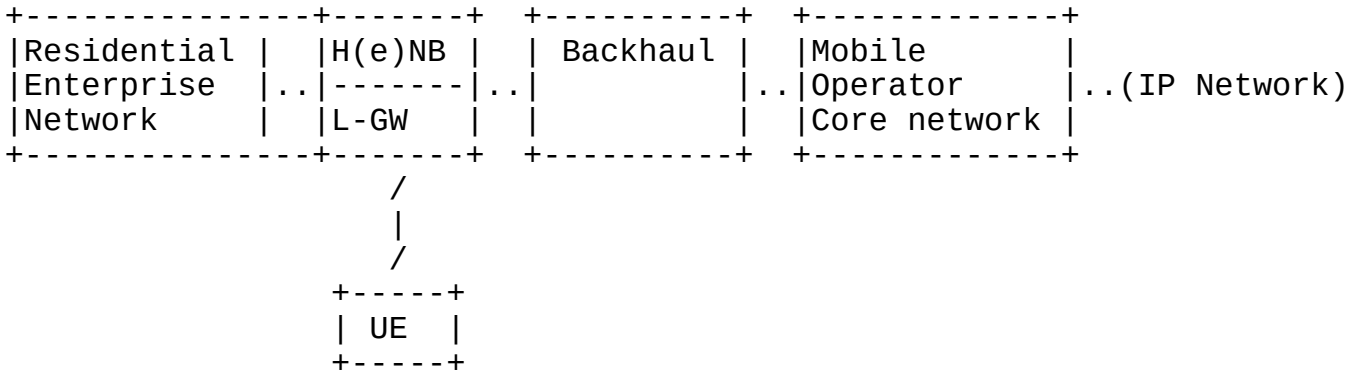

Figure 8. LIPA architecture.

There is a local gateway function in the H(e)NB. The local gateway (L-GW) function acts as a GGSN (UMTS) or P-GW (LTE). The mobile station uses a special APN to establish the PDP context or the default bearer towards the L-GW.

One thing that needs to be noted is that in 3GPP Release 10, there is no mobility support when the mobile stations moves between H(e)NBs. The bearer will be broken when the mobile moves among H(e)NBs. For example, when several H(e)NBs are deployed in an office, there is no mobility support when the mobile station needs to do handover between the H(e)NBs. The user session would be broken when a user moves from one H(e)NB coverage to another.

The SIPTO (Selected IP Traffic Offload) scenario is illustrated in the Figure 9. There is also a local gateway function near the base station. The traffic can be routed through the local gateway to offload the traffic.

In both LIPA and SIPTO architecture, the local gateway functions as the anchor point for the local traffic.

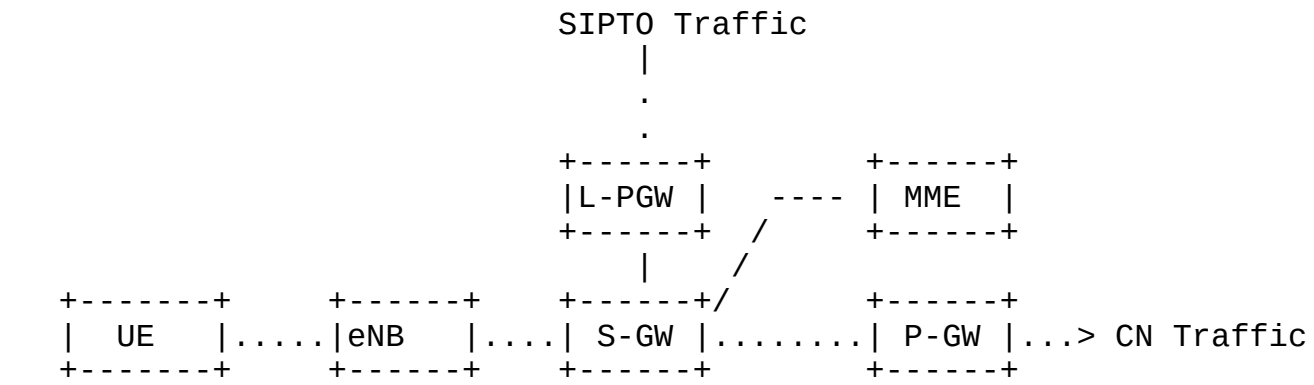

Figure 9. SIPTO architecture.

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

For either the WiFi network and cellular network such as 3GPP, the DMM scenario can be a fully distributed scenario separation of control and data planes. The reconfiguration of mobility management functions in these scenario may consist of multiple MRs and a distributed LM database. Figure 10 shows such an example DMM architecture with the same three networks as in Figure 3. As is in Figure 3, each network in Figure 10 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 3, the LM function in Figure 10 is a distributed database, with multiple servers, of the mapping of HoA to CoA.

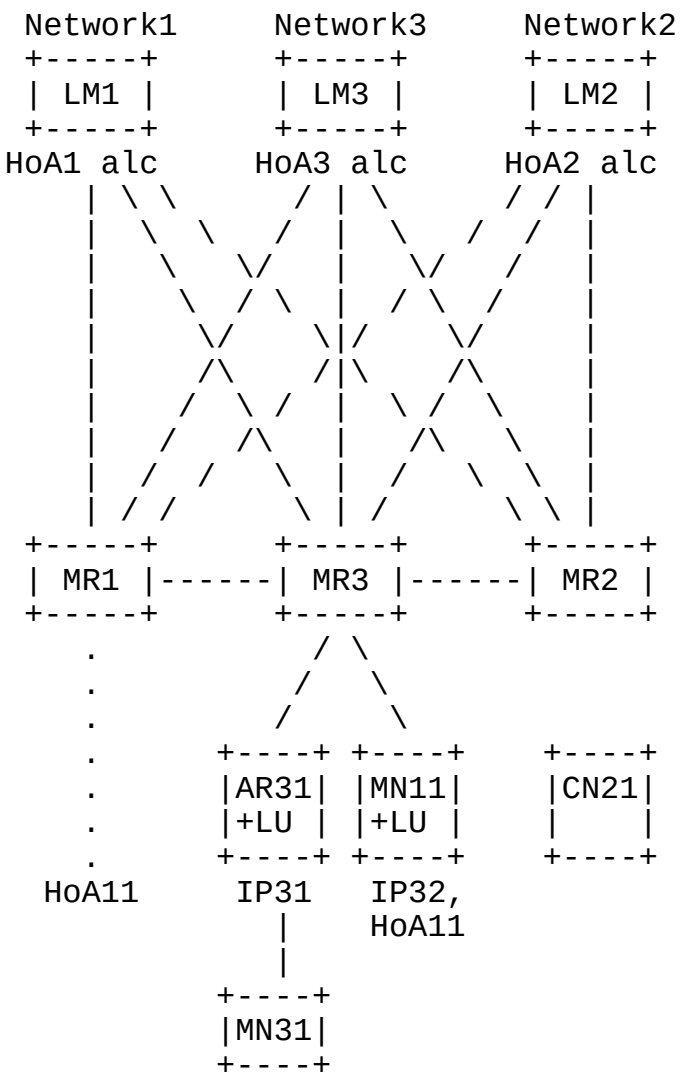

Figure 10. A distributed architecture for mobility management.

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.

5. Gap analysis

5.1. Gap analysis with reconfiguration MIPv6 and PMIPv6 functions in DMM scenario such as the flattened WiFi network

5.1.1. 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.

The best current practice is using the existing mobility management functions of the current protocols.

5.1.2. 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.

5.1.3. 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 when using the mobility management functions of MIPv6 and PMIPv6 which are originally designed for IPv6.

5.1.4. Security considerations

The second 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.

5.1.5. 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 can exist in MIPv6 by simply having an HA for each home network. Yet it is complicated for the MN to move its HA from one network to another. Therefore this requirement is not fully met in the best current practice.

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

5.1.6. 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 could simply be used as the home network for new sessions.

Yet the capability to use different IP addresses for different IP sessions are not in the existing mobility management functions. This requirement is then not met in the best practice.

5.1.7. 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.

Although there are existing route optimization extensions, they generally compromise with location privacy so that this requirement is not met.

5.2. Gap analysis summary with reconfiguration MIPv6 and PMIPv6

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
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
Reconfigure mobility functions in DMM scenario	Y	Y (supports above)	Y	Y	Y	N	N

5.3. Gap analysis from the 3GPP LIPA/SIPTO scenario

From the real deployment perspective, it need to be noted that in 3GPP LIPA/SIPTO scenario, there is no mobility support when handover between local gateways. There is no current IP mobility protocol can be used to solve this problem currently. DMM may provide a solution for this scenario.

6. Security Considerations

TBD

7. IANA Considerations

None

8. References

8.1. Normative References

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

8.2. 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

Dapeng Liu
China Mobile
Unit2, 28 Xuanwumenxi Ave, Xuanwu District, Beijing 100053, China
Email: liudapeng@chinamobile.com

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