DMM
Internet-Draft
Intended status: Informational
Expires: April 2, 2015

D. Liu, Ed.
China Mobile
JC. Zuniga, Ed.
InterDigital
P. Seite
Orange
H. Chan
Huawei Technologies
CJ. Bernardos
UC3M

September 29, 2014

Distributed Mobility Management: Current practices and gap analysis
draft-ietf-dmm-best-practices-gap-analysis-08

Abstract

This document analyzes deployment practices of existing IP mobility protocols in a distributed mobility management environment. It then identifies existing limitations when compared to the requirements defined for a distributed mobility management solution.

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 April 2, 2015.

Copyright Notice

Table of Contents

1. Introduction

Existing network-layer mobility management protocols have primarily employed a mobility anchor to ensure connectivity of a mobile node by forwarding packets destined to, or sent from, the mobile node after the node has moved to a different network. The mobility anchor has been centrally deployed in the sense that the traffic of millions of mobile nodes in an operator network is typically managed by the same anchor. This centralized deployment of mobility anchors to manage IP sessions poses several problems. In order to address these problems, a distributed mobility management (DMM) architecture has been

proposed. This document investigates whether it is feasible to deploy current IP mobility protocols in a DMM scenario in a way that can fulfill the requirements as defined in [RFC7333]. It discusses current deployment practices of existing mobility protocols and identifies the limitations (gaps) in these practices from the standpoint of satisfying DMM requirements. The analysis is primarily towards IPv6 deployment, but can be seen to also apply to IPv4 whenever there are IPv4 counterparts equivalent to the IPv6 mobility protocols.

The rest of this document is organized as follows. Section 3 analyzes existing IP mobility protocols by examining their functions and how these functions can be configured and used to work in a DMM environment. Section 4 presents the current practices of IP wireless networks and 3GPP architectures. Both network- and host-based mobility protocols are considered. Section 5 presents the gap analysis with respect to the current practices.

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], in the Proxy Mobile IPv6 specification [RFC5213], and in the Distributed Mobility Management Requirements [RFC7333]. These terms include mobile node (MN), correspondent node (CN), home agent (HA), Local Mobility Anchor (LMA), Mobile Access Gateway (MAG), centrally depoyed mobility anchors, distributed mobility management, hierarchical mobile network, flatter mobile network, and flattening mobile network.

In addition, this document also introduces some definitions of IP mobility functions in Section 3.

In this document there are also references to a "distributed mobility management environment." By this term, we refer to a scenario in which the IP mobility, access network and routing solutions allow for setting up IP networks so that traffic is distributed in an optimal way, without relying on centrally deployed mobility anchors to manage IP mobility sessions.

3. Functions of existing mobility protocols

The host-based Mobile IPv6 (MIPv6) [RFC6275] and its network-based extension, Proxy Mobile IPv6 (PMIPv6) [RFC5213], as well as Hierarchical Mobile IPv6 (HMIPv6) [RFC5380] are logically centralized mobility management approaches addressing primarily hierarchical mobile networks. Although these approaches are centralized, they have important mobility management functions resulting from years of

extensive work to develop and to extend these functions. It is therefore useful to take these existing functions and examine them in a DMM scenario in order to understand how to deploy the existing mobility protocols to provide distributed mobility management.

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

1. Anchoring Function (AF): allocation to a mobile node of an IP address, i.e., Home Address (HoA), or prefix, i.e., Home Network Prefix (HNP) topologically anchored by the advertising node. That is, the anchor node is able to advertise a connected route into the routing infrastructure for the allocated IP prefixes. This function is a control plane function.

2. Internetwork Location Information (LI) function: managing and keeping track of the internetwork location of an MN. The location information may be a binding of the IP advertised address/prefix, e.g., HoA or HNP, to the IP routing address of the MN or of a node that can forward packets destined to the MN. It is a control plane function.

   In a client-server protocol model, location query and update messages may be exchanged between a location information client (LIc) and a location information server (LIs).

3. Forwarding Management (FM) function: packet interception and forwarding to/from the IP address/prefix assigned to 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.

   FM may optionally be split into the control plane (FM-CP) and data plane (FM-DP).

In Mobile IPv6, the home agent (HA) typically provides the anchoring function (AF); the location information server (LIs) is at the HA whereas the location information client (LIc) is at the MN; the Forwarding Management (FM) function resides in both ends of the tunnel at the HA and the MN.

In Proxy Mobile IPv6, the Local Mobility Anchor (LMA) provides the anchoring function (AF); the location information server (LIs) is at the LMA whereas the location information client (LIc) is at the mobile access gateway (MAG); the Forwarding Management (FM) function resides in both ends of the tunnel at the HA and the MAG.

In Hierarchical Mobile IPv6 (HMIPv6) [RFC5380], the Mobility Anchor Point (MAP) serves as a location information aggregator between the LIs at the HA and the LIc at the MN. The MAP also provides the FM function to enable tunneling between HA and itself as well as tunneling between MN and itself.

4. DMM practices

This section documents deployment practices of existing mobility protocols to satisfy distributed mobility management requirements. This description considers both IP wireless, e.g., evolved Wi-Fi hotspots, and 3GPP flattening mobile network.

While describing the current DMM practices, the section provides references to the generic mobility management functions described in Section 3 as well as some initial hints on the identified gaps with respect to the DMM requirements documented in [RFC7333].

4.1. Assumptions

There are many different approaches that can be considered to implement and deploy a distributed anchoring and mobility solution. The focus of the gap analysis is on certain current mobile network architectures and standardized IP mobility solutions, considering any kind of deployment options which do not violate the original protocol specifications. In order to limit the scope of our analysis of DMM practices, we consider the following list of technical assumptions:

1. Both host- and network-based solutions are considered.

2. Solutions should allow selecting and using the most appropriate IP anchor among a set of available candidates.

3. Mobility management should be realized by the preservation of the IP address across the different points of attachment (i.e., provision of IP address continuity). This is in contrast to certain transport-layer based approaches such as Stream Control Transmission Protocol (SCTP) [RFC4960] or application-layer mobility.

Applications which can cope with changes in the MN’s IP address do not depend on IP mobility management protocols such as DMM. Typically, a connection manager together with the operating system will configure the source address selection mechanism of the IP stack. This might involve identifying application capabilities and triggering the mobility support accordingly. Further considerations on application management and source address selection are out of the scope of this document, but the reader might consult [RFC6724].

4.2. IP flat wireless network

This section focuses on common IP wireless network architectures and how they can be flattened from an IP mobility and anchoring point of view using common and standardized protocols. We take Wi-Fi as an useful wireless technology, since it is widely known and deployed nowadays. Some representative examples of Wi-Fi deployment architectures are depicted in Figure 1.

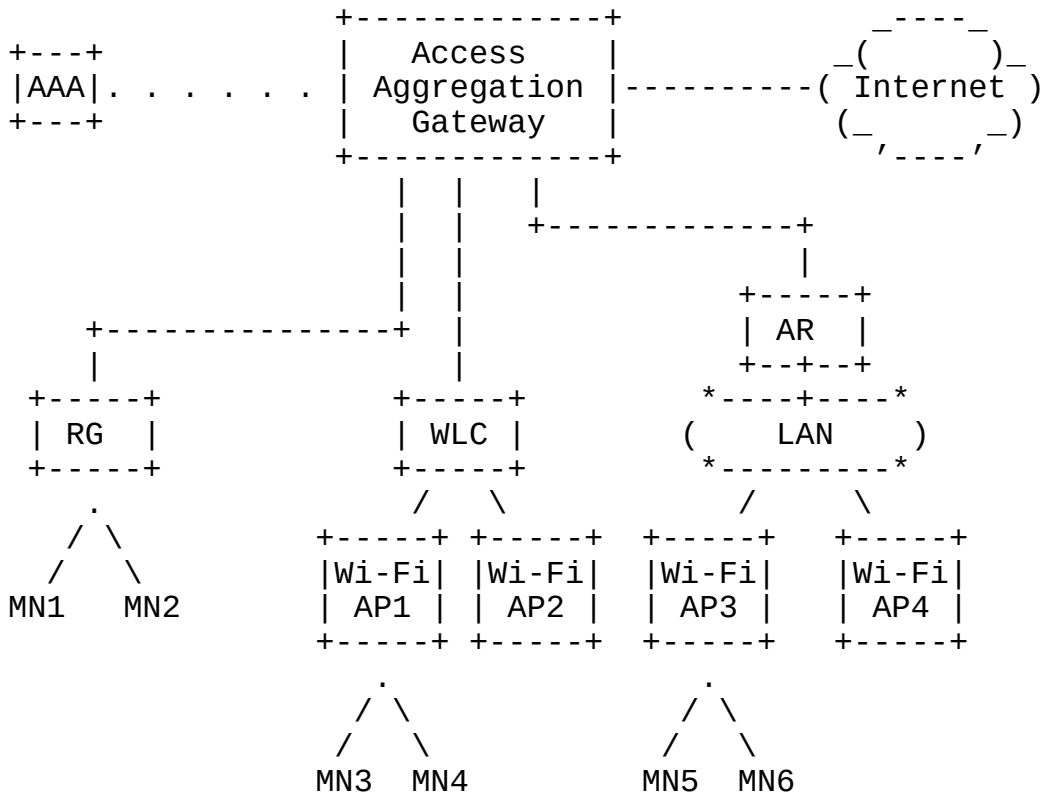

Figure 1: IP Wi-Fi network architectures

In Figure 1, three typical deployment options are shown [I-D.gundavelli-v6ops-community-wifi-svcs]. On the left hand side of the figure, mobile nodes MN1 and MN2 directly connect to a Residential Gateway (RG) at the customer premises. The RG hosts the 802.11 Access Point (AP) function to enable wireless layer-2 access connectivity and also provides layer-3 routing functions. In the middle of the figure, mobile nodes MN3 and MN4 connect to Wi-Fi Access Points (APs) AP1 and AP2 that are managed by a Wireless LAN Controller (WLC), which performs radio resource management on the APs, domain-wide mobility policy enforcement and centralized forwarding function for the user traffic. The WLC could also implement layer-3 routing functions, or attach to an access router (AR). Last, on the right-hand side of the figure, access points AP3

and AP4 are directly connected to an access router. This can also be used as a generic connectivity model.

IP mobility protocols can be used to provide heterogeneous network mobility support to users, e.g., handover from Wi-Fi to cellular access. Two kind of protocols can be used: Proxy Mobile IPv6 [RFC5213] or Mobile IPv6 [RFC5555], with the role of mobility anchor, e.g., Local Mobility Anchor or home agent, typically being played by the edge router of the mobile network [SDO-3GPP.23.402].

Although this section has made use of the example of Wi-Fi networks, there are other flattening mobile network architectures specified, such as WiMAX [IEEE.802-16.2009], which integrates both host- and network-based IP mobility functions.

Existing IP mobility protocols can also be deployed in a flatter manner, so that the anchoring and access aggregation functions are distributed. We next describe several practices for the deployment of existing mobility protocols in a distributed mobility management environment. The analysis in this section is limited to protocol solutions based on existing IP mobility protocols, either host- or network-based, such as Mobile IPv6 [RFC6275], [RFC5555], Proxy Mobile IPv6 (PMIPv6) [RFC5213], [RFC5844] and Network Mobility Basic Support protocol (NEMO) [RFC3963]. Extensions to these base protocol solutions are also considered. The analysis is divided into two parts: host- and network-based practices.

4.2.1. Host-based IP DMM practices

Mobile IPv6 (MIPv6) [RFC6275] and its extension to support mobile networks, the NEMO Basic Support protocol (hereafter, simply referred to as NEMO) [RFC3963] are well-known host-based IP mobility protocols. They depend on the function of the Home Agent (HA), a centralized anchor, to provide mobile nodes (hosts and routers) with mobility support. In these approaches, the Home Agent typically provides the Anchoring Function (AF), Forwarding Management (FM), and Internetwork Location Information server (LIs) functions. The mobile node possesses the Location Information client (LIc) function and the FM function to enable tunneling between HA and itself. We next describe some practices that show how MIPv6/NEMO and several other protocol extensions can be deployed in a distributed mobility management environment.

One approach to distribute the anchors can be to deploy several HAs (as shown in Figure 2), and assign the topologically closest anchor to each MN [RFC4640], [RFC5026], [RFC6611]. In the example shown in Figure 2, the mobile node MN1 is assigned to the home agent HA1 and uses a home address anchored by HA1 to communicate with the

correspondent node CN1. Similarly, the mobile node MN2 is assigned to the home agent HA2 and uses a home address anchored by HA2 to communicate with the correspondent node CN2. Note that MIPv6/NEMO specifications do not prevent the simultaneous use of multiple home agents by a single mobile node. In this deployment model, the mobile node can use several anchors at the same time, each of them anchoring IP flows initiated at a different point of attachment. However, there is currently no mechanism specified in IETF to enable an efficient dynamic discovery of available anchors and the selection of the most suitable one.

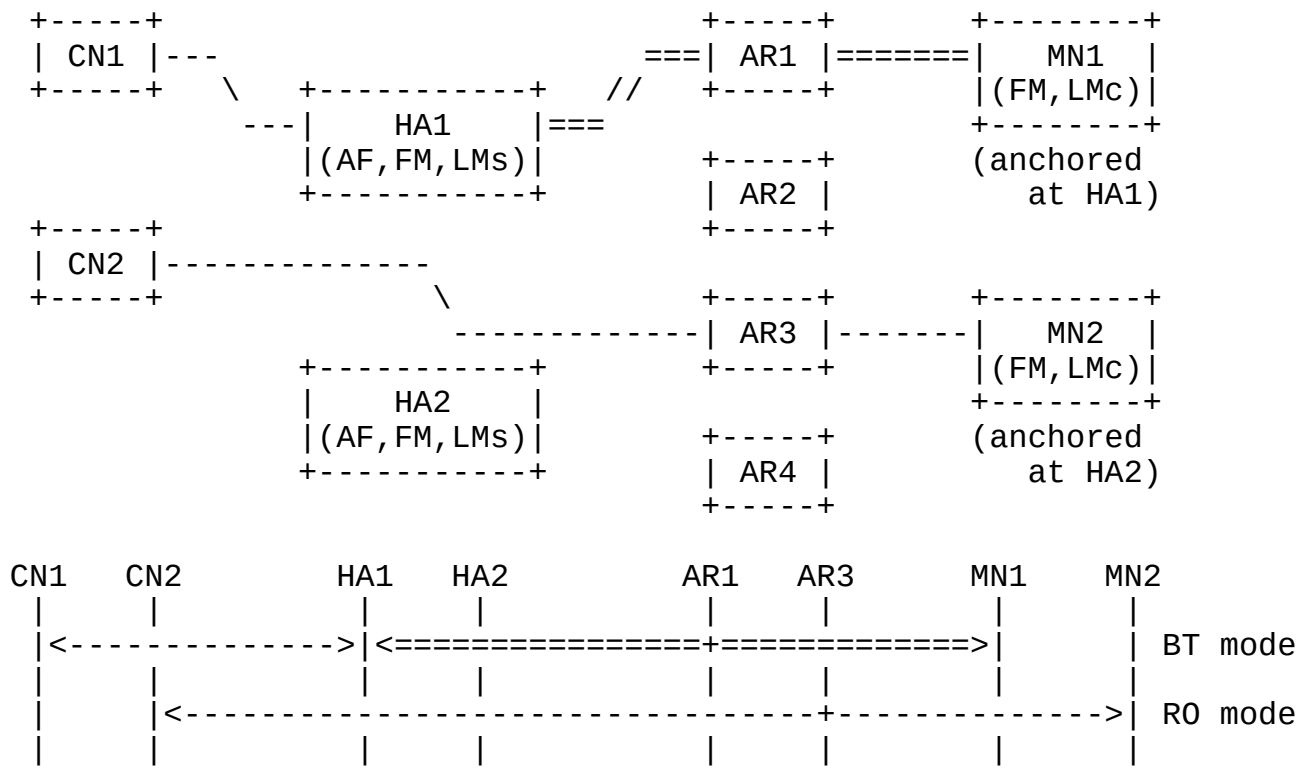

Figure 2: Distributed operation of Mobile IPv6 (BT and RO) / NEMO

One goal of the deployment of mobility protocols in a distributed mobility management environment is to avoid the suboptimal routing caused by centralized anchoring. Here, the Route Optimization (RO) support provided by Mobile IPv6 can be used to achieve a flatter IP data forwarding. By default, Mobile IPv6 and NEMO use the so-called Bidirectional Tunnel (BT) mode, in which data traffic is always encapsulated between the MN and its HA before being directed to any other destination. The RO mode allows the MN to update its current location on the CNs, and then use the direct path between them. Using the example shown in Figure 2, MN1 is using BT mode with CN1,

while MN2 is in RO mode with CN2. However, the RO mode has several drawbacks:

- The RO mode is only supported by Mobile IPv6. There is no route optimization support standardized for the NEMO protocol because of the security problems posed by extending return routability tests for prefixes, although many different solutions have been proposed [RFC4889].

- The RO mode requires signaling that adds some protocol overhead.

- The signaling required to enable RO involves the home agent and is repeated periodically for security reasons [RFC4225]. Therefore the HA remains a single point of failure.

- The RO mode requires support from the CN.

Notwithstanding these considerations, the RO mode does offer the possibility of substantially reducing traffic through the Home Agent, in cases when it can be supported by the relevant correspondent nodes. Note that a mobile node can also use its care-of-address (CoA) directly [RFC5014] when communicating with CNs on the same link or anywhere in the Internet, although no session continuity support would be provided by the IP stack in this case.

Hierarchical Mobile IPv6 (HMIPv6) [RFC5380] (as shown in Figure 3), is another host-based IP mobility extension which can be considered as a complement to provide a less centralized mobility deployment. It allows the reduction of the amount of mobility signaling as well as improving 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. It provides LI intermediary function between the LI server (LIs) at the HA and the LI client (LIc) at the MN. It also performs the FM function to tunnel with the HA and also with the MN.

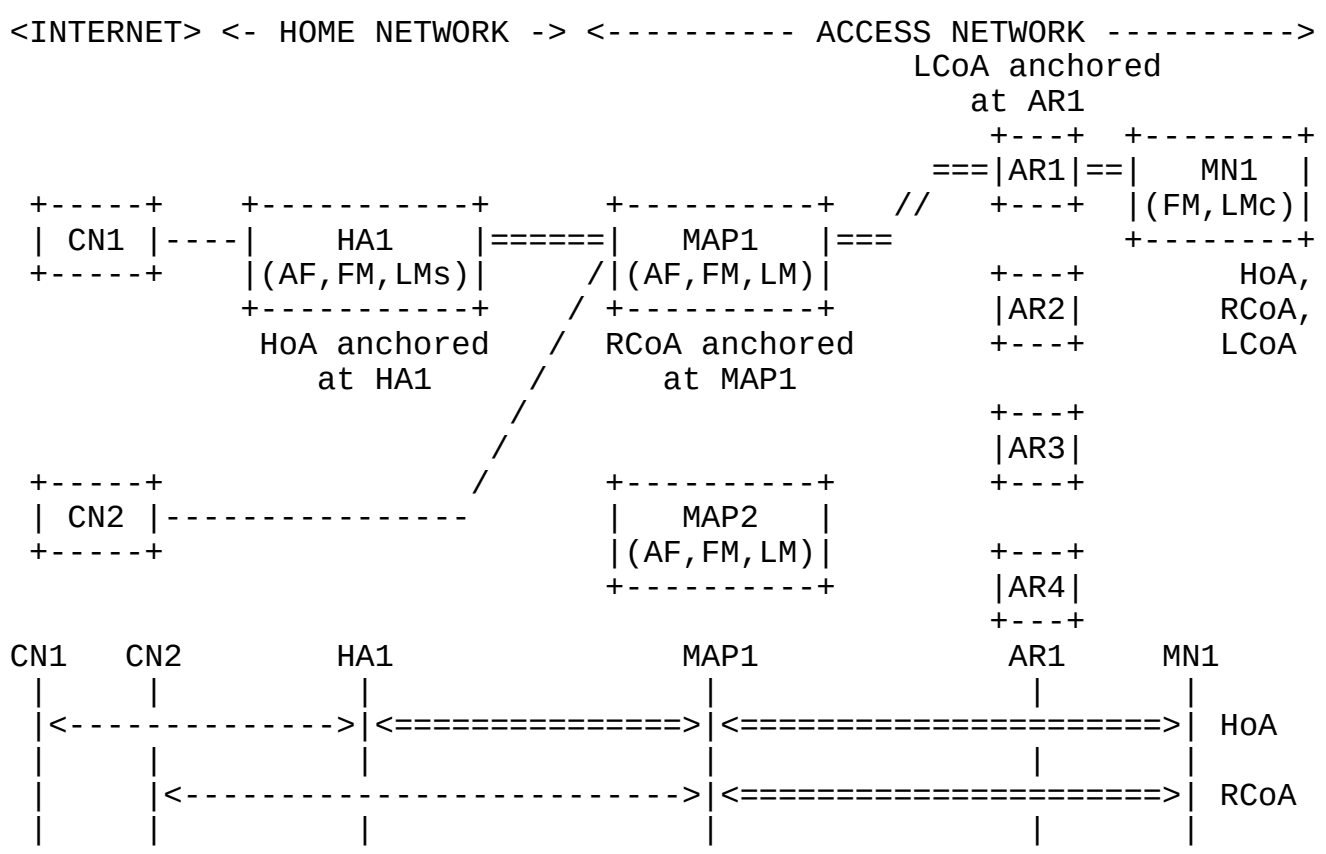

Figure 3: Hierarchical Mobile IPv6

When HMIPv6 is used, the MN has two different temporary addresses: the Regional Care-of Address (RCoA) and the Local Care-of Address (LCoA). The RCoA is anchored at one MAP, which plays the role of local home agent, while the LCoA is anchored at the access router level. The mobile node uses 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 its RCoA.

The use of HMIPv6 enables some form of route optimization, since a mobile node may decide to directly use the RCoA as source address for a communication with a given correspondent node, particularly 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, though it fails to provide session continuity if and when the MN moves outside the local domain. 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.

Furthermore, a local domain might have several MAPs deployed, enabling therefore a different kind of HMIPv6 deployments which are

flattening and distributed. The HMIPv6 specification supports a flexible selection of the MAP, including those based on the distance between the MN and the MAP, or taking into consideration the expected mobility pattern of the MN.

Another extension that can be used to help distributing mobility management functions is the Home Agent switch specification [RFC5142], which defines a new mobility header for signaling a mobile node that it should acquire a new home agent. [RFC5142] does not specify the case of changing the mobile node's home address, as that might imply loss of connectivity for ongoing persistent connections. Nevertheless, that specification could be used to force the change of home agent in those situations where there are no active persistent data sessions that cannot cope with a change of home address.

There are other host-based approaches standardized that can be used to provide mobility support. For example MOBIKE [RFC4555] allows a mobile node encrypting traffic through IKEv2 [RFC5996] to change its point of attachment while maintaining a Virtual Private Network (VPN) session. The MOBIKE protocol allows updating the VPN Security Associations (SAs) in cases where the base connection initially used is lost and needs to be re-established. The use of the MOBIKE protocol avoids having to perform an IKEv2 re-negotiation. Similar considerations to those made for Mobile IPv6 can be applied to MOBIKE; though MOBIKE is best suited for situations where the address of at least one endpoint is relatively stable and can be discovered using existing mechanisms such as DNS.

Extensions have been defined to the mobility protocol to optimize the handover performance. Mobile IPv6 Fast Handovers (FMIPv6) [RFC5568] is the extension to optimize handover latency. It defines new access router discovery mechanism before handover to reduce the new network discovery latency. It also defines a tunnel between the previous access router and the new access router to reduce the packet loss during handover. The Candidate Access Router Discovery (CARD) [RFC4066] and Context Transfer Protocol (CXTP) [RFC4067] protocols were standardized to improve the handover performance. The DMM deployment practice discussed in this section can also use those extensions to improve the handover performance.

4.2.2. Network-based IP DMM practices

Proxy Mobile IPv6 (PMIPv6) [RFC5213] is the main network-based IP mobility protocol specified for IPv6. Proxy Mobile IPv4 [RFC5844] defines some IPv4 extensions. With network-based IP mobility protocols, the Local Mobility Anchor (LMA) typically provides the Anchoring Function (AF), Forwarding Management (FM) function, and Internetwork Location Information server (LIs) function. The mobile

access gateway (MAG) provides the Location Information client (LIc) function and Forwarding Management (FM) function to tunnel with LMA. PMIPv6 is architecturally almost identical to MIPv6, as the mobility signaling and routing between LMA and MAG in PMIPv6 is similar to those between HA and MN in MIPv6. The required mobility functionality at the MN is provided by the MAG so that the involvement in mobility support by the MN is not required.

We next describe some practices that show how network-based mobility protocols and several other protocol extensions can be deployed in a distributed mobility management environment.

One way to decentralize Proxy Mobile IPv6 operation can be to deploy several Local Mobility Anchors and use some selection criteria to assign LMAs to attaching mobile nodes. An example of this type of assignment is shown in Figure 4. As with the client based approach, a mobile node may use several anchors at the same time, each of them anchoring IP flows initiated at a different point of attachment. This assignment can be static or dynamic. The main advantage of this simple approach is that the IP address anchor, i.e., the LMA, could be placed closer to the mobile node. Therefore the resulting paths are close-to-optimal. On the other hand, as soon as the mobile node moves, the resulting path will start deviating from the optimal one.

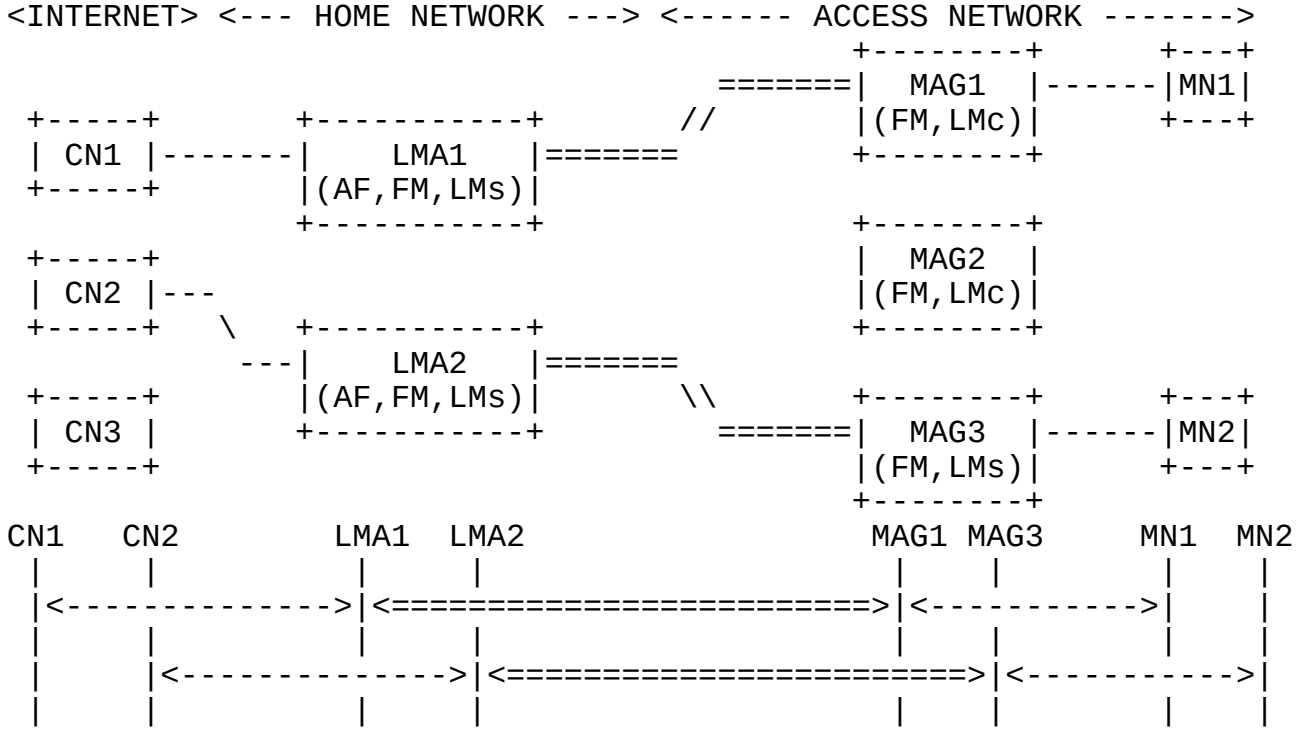

Figure 4: Distributed operation of Proxy Mobile IPv6

In a similar way to the host-based IP mobility case, network-based IP mobility has some extensions defined to mitigate the suboptimal routing issues that may arise due to the use of a centralized anchor. The Local Routing extensions [RFC6705] enable optimal routing in Proxy Mobile IPv6 in three cases: i) when two communicating MNs are attached to the same MAG and LMA, ii) when two communicating MNs are attached to different MAGs but to the same LMA, and iii) when two communicating MNs are attached to the same MAG but have different LMAs. In these three cases, data traffic between the two mobile nodes does not traverse the LMA(s), thus providing some form of path optimization since the traffic is locally routed at the edge. The main disadvantage of this approach is that it only tackles the MN-to-MN communication scenario, and only under certain circumstances.

An interesting extension that can also be used to facilitate the deployment of network-based mobility protocols in a distributed mobility management environment is the support of LMA runtime assignment described in [RFC6463]. This extension 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 the Proxy Binding Update / Proxy Binding Acknowledgment message exchange between a mobile access gateway and a local mobility anchor. While this mechanism is mainly aimed for load-balancing purposes, it can also be used to select an optimal LMA from the routing point of view. A runtime LMA assignment can be used to change the assigned LMA of an MN, for example, in cases when the mobile node does not have any active session, or when the running sessions can survive an IP address change. Note that several possible dynamic Local Mobility Anchor discovery solutions can be used, as described in [RFC6097].

4.3. Flattening 3GPP mobile network approaches

The 3rd Generation Partnership Project (3GPP) is the standards development organization that specifies the 3rd generation mobile network and the Evolved Packet System (EPS) [SDO-3GPP.23.402], which mainly comprises the Evolved Packet Core (EPC) and a new radio access network, usually referred to as LTE (Long Term Evolution).

Architecturally, the 3GPP Evolved Packet Core (EPC) network is similar to an IP wireless network running PMIPv6 or MIPv6, as it relies on the Packet Data Network Gateway (PGW) anchoring services to provide mobile nodes with mobility support (see Figure 5). There are client-based and network-based mobility solutions in 3GPP, which for simplicity will be analyzed together. We next describe how 3GPP mobility protocols and several other completed or ongoing extensions can be deployed to meet some of the DMM requirements [RFC7333].

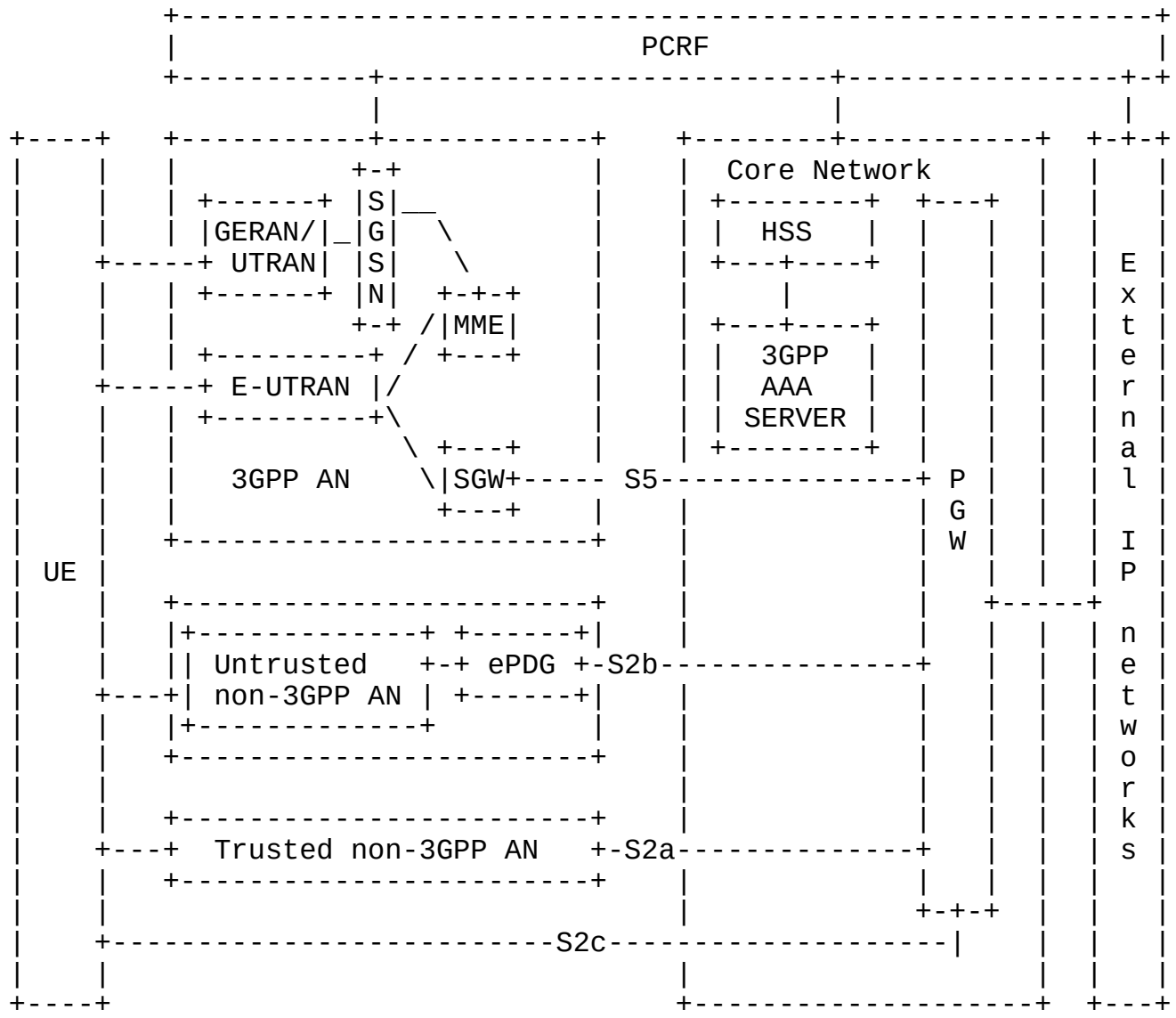

Figure 5: EPS (non-roaming) architecture overview

The GPRS Tunneling Protocol (GTP) [SDO-3GPP.29.060] [SDO-3GPP.29.281] [SDO-3GPP.29.274] is a network-based mobility protocol specified for 3GPP networks (S2a, S2b, S5 and S8 interfaces). In a similar way to PMIPv6, it can handle mobility without requiring the involvement of the mobile nodes. In this case, the mobile node functionality is provided in a proxy manner by the Serving Data Gateway (SGW), Evolved Packet Data Gateway (ePDG), or Trusted Wireless Access Gateway (TWAG [SDO-3GPP.23.402]) .

3GPP specifications also include client-based mobility support, based on adopting the use of Dual-Stack Mobile IPv6 (DSMIPv6) [RFC5555] for the S2c interface [SDO-3GPP.24.303]. In this case, the User

Equipment (UE) implements the binding update functionality, while the home agent role is played by the PGW.

A Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO) enabled network [SDO-3GPP.23.401] allows offloading some IP services at the local access network above the Radio Access Network (RAN) without the need to travel back to the PGW (see Figure 6).

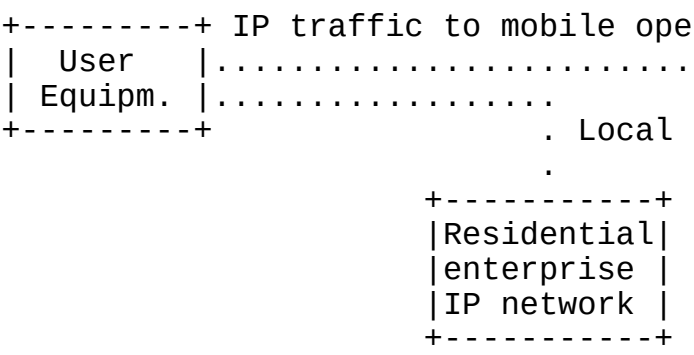

Figure 6: LIPA scenario

SIPTO enables an operator to offload certain types of traffic at a network node close to the UE's point of attachment to the access network, by selecting a set of GWs (SGW and PGW) that are geographically/topologically close to the UE's point of attachment.

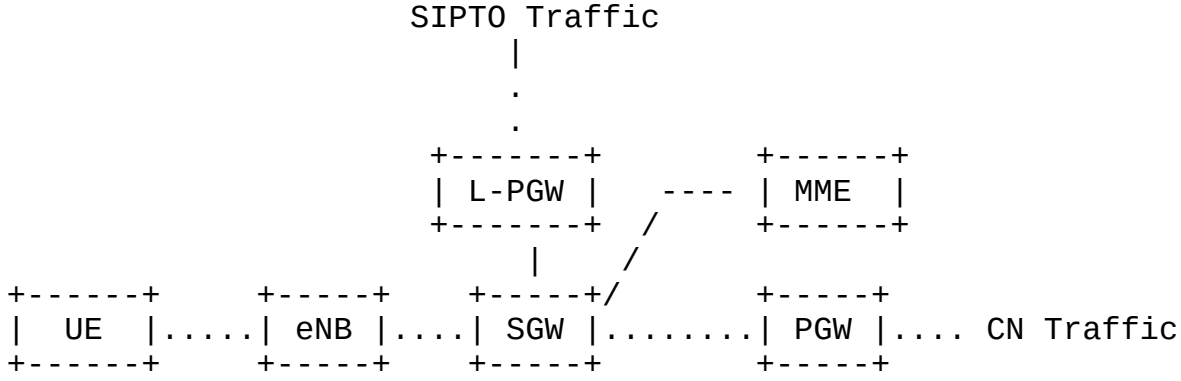

Figure 7: SIPTO architecture

LIPA, on the other hand, enables an IP addressable UE connected via a Home eNB (HeNB) to access other IP addressable entities in the same residential/enterprise IP network without traversing the mobile operator's network core in the user plane. In order to achieve this, a Local GW (LGW) collocated with the HeNB is used. LIPA is established by the UE requesting a new Public Data Network (PDN) connection to an access point name for which LIPA is permitted, and

the network selecting the Local GW associated with the HeNB and enabling a direct user plane path between the Local GW and the HeNB.

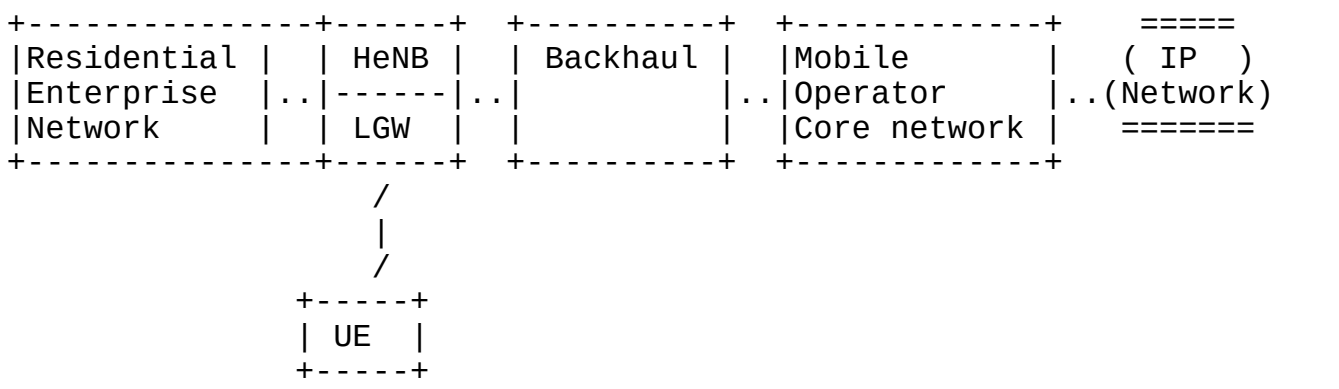

Figure 8: LIPA architecture

The 3GPP architecture specifications also provide mechanisms to allow discovery and selection of gateways [SDO-3GPP.29.303]. These mechanisms enable decisions taking into consideration topological location and gateway collocation aspects, relying upon the DNS as a "location database."

Both SIPTO and LIPA have a very limited mobility support, especially in 3GPP specifications up to Rel-12. Briefly, LIPA mobility support is limited to handovers between HeNBs that are managed by the same LGW (i.e., mobility within the local domain). There is no guarantee of IP session continuity for SIPTO.

5. Gap analysis

This section identifies the limitations in the current practices, described in Section 4, with respect to the DMM requirements listed in [RFC7333].

5.1. Distributed mobility management - REQ1

According to requirement REQ1 stated in [RFC7333], IP mobility, network access and forwarding solutions provided by DMM must make it possible for traffic to avoid traversing a single mobility anchor far from the optimal route.

From the analysis performed in Section 4, a DMM deployment can meet the requirement "REQ1 Distributed mobility management" usually relying on the following functions:

- Multiple (distributed) anchoring: ability to anchor different sessions of a single mobile node at different anchors. In order

to provide improved routing, some anchors might need to be placed closer to the mobile node or the corresponding node.

- o Dynamic anchor assignment/re-location: ability to i) assign the initial anchor, and ii) dynamically change the initially assigned anchor and/or assign a new one (this may also require the transfer of mobility context between anchors). This can be achieved either by changing anchor for all ongoing sessions or by assigning new anchors just for new sessions.

GAP1-1: Both the main client- and network-based IP mobility protocols, namely (DS)MIPv6 and PMIPv6 allow deploying multiple anchors (i.e., home agents and localized mobility anchors), thereby providing the multiple anchoring function. However, existing solutions only provide an initial anchor assignment, thus the lack of dynamic anchor change/new anchor assignment is a gap. Neither the HA switch nor the LMA runtime assignment allows changing the anchor during an ongoing session. This actually comprises several gaps: ability to perform anchor assignment at any time (not only at the initial MN's attachment), ability of the current anchor to initiate/trigger the relocation, and ability to transfer registration context between anchors.

GAP1-2: Dynamic anchor assignment may lead the MN to manage different mobility sessions served by different mobility anchors. This is not an issue with client based mobility management where the mobility client natively knows the anchor associated with each of its mobility sessions. However, there is one gap, as the MN should be capable of handling IP addresses in a DMM-friendly way, meaning that the MN can perform smart source address selection (i.e., deprecating IP addresses from previous mobility anchors, so they are not used for new sessions). Besides, managing different mobility sessions served by different mobility anchors may raise issues with network based mobility management. In this case, the mobile client located in the network, e.g., MAG, usually retrieves the MN's anchor from the MN's policy profile as described in Section 6.2 of [RFC5213]. Currently, the MN's policy profile implicitly assumes a single serving anchor and thus does not maintain the association between home network prefix and anchor.

GAP1-3: The consequence of the distribution of the mobility anchors is that there might be more than one available anchor for a mobile node to use, which leads to an anchor discovery and selection issue. Currently, there is no efficient mechanism specified to allow the dynamic discovery of the presence of

nodes that can play the anchor role, discovering their capabilities and selecting the most suitable one. There is also no mechanism to allow selecting a node that is currently anchoring a given home address/prefix (capability sometimes required to meet REQ#2). However, there are some mechanisms that could help to discover anchors, such as the Dynamic Home Agent Address Discovery (DHAAD) [RFC6275], the use of the home agent flag (H) in Router Advertisements (which indicates that the router sending the Router Advertisement is also functioning as a Mobile IPv6 home agent on the link) or the MAP option in Router Advertisements defined by HMIPv6. Note that there are 3GPP mechanisms providing that functionality defined in [SDO-3GPP.29.303].

Regarding the ability to transfer registration context between anchors, there are already some solutions that could be reused or adapted to fill that gap, such as Fast Handovers for Mobile IPv6 [RFC5568] -- to enable traffic redirection from the old to the new anchor --, the Context Transfer protocol [RFC4067] -- to enable the required transfer of registration information between anchors --, or the Handover Keying architecture solutions [RFC6697], to speed up the re-authentication process after a change of anchor. Note that some extensions might be needed in the context of DMM, as these protocols were designed in the context of centralized client IP mobility, focusing on the access re-attachment and authentication.

GAP1-4: Also note that REQ1 is intended to prevent the data plane traffic from taking a suboptimal route. Distributed processing of the traffic may then be needed only in the data plane. Provision of this capability for distributed processing should not conflict with the use of a centralized control plane. Other control plane solutions such as charging, lawful interception, etc. should not be constrained by the DMM solution. On the other hand combining the control plane and data plane forwarding management (FM) function may limit the choice of solutions to those that distribute both data plane and control plane together. In order to enable distribution of only the data plane without distributing the control plane, it would be necessary to split the forwarding management function into the control plane (FM-CP) and data plane (FM-DP) components; there is currently a gap here.

5.2. Bypassable network-layer mobility support for each application session - REQ2

The requirement REQ2 for "bypassable network-layer mobility support for each application session" introduced in [RFC7333] requires flexibility in determining whether network-layer mobility support is needed. This requirement enables one to choose whether or not to use network-layer mobility support. The following two functions are also needed:

- o Dynamically assign/relocate anchor: a mobility anchor is assigned only to sessions which use the network-layer mobility support. The MN may thus manage more than one session; some of them may be associated with anchored IP address(es), while the others may be associated with local IP address(es).

- o Multiple IP address management: this function is related to the preceding and is about the ability of the mobile node to simultaneously use multiple IP addresses and select the best one (from an anchoring point of view) to use on a per-session/application/service basis. This requires MN to acquire information regarding the properties of the available IP addresses.

GAP2-1: The dynamic anchor assignment/relocation needs to ensure that IP address continuity is guaranteed for sessions that uses such mobility support (e.g., in some scenarios, the provision of mobility locally within a limited area might be enough from the mobile node or the application point of view) at the relocated anchor. Implicitly, when no applications are using the network-layer mobility support, DMM may release the needed resources. This may imply having the knowledge of which sessions at the mobile node are active and are using the mobility support. This is something typically known only by the MN, e.g., by its connection manager, and would also typically require some signaling support such as socket API extensions from applications to indicate to the IP stack whether mobility support is required or not. Therefore, (part of) this knowledge might need to be transferred to/shared with the network.

GAP2-2: Multiple IP address management provides the MN with the choice to pick the correct address, e.g., from those provided or not provided with mobility support, depending on the application requirements. When using client based mobility management, the mobile node is itself aware of the anchoring capabilities of its assigned IP addresses. This

is not necessarily the case with network based IP mobility management; current mechanisms do not allow the MN to be aware of the properties of its IP addresses. For example, the MN does not know whether the allocated IP addresses are anchored. However, there are proposals, such as [I-D.bhandari-dhc-class-based-prefix], [I-D.korhonen-6man-prefix-properties] and [I-D.anipko-mif-mpvd-arch] that the network could indicate such IP address properties during assignment procedures. Although these individual efforts exist and they could be considered as attempts to fix the gap, there is no solution adopted as a work item within any IETF working group.

GAP2-3: The handling of mobility management to the granularity of an individual session of a user/device needs proper session identification in addition to user/device identification.

5.3. IPv6 deployment - REQ3

This requirement states that DMM solutions should primarily target IPv6 as the primary deployment environment. IPv4 support is not considered mandatory and solutions should not be tailored specifically to support IPv4.

All analyzed DMM practices support IPv6. Some of them, such as MIPv6/NEMO including the support of dynamic HA selection, MOBIKE, SIPTO also have IPv4 support. Some solutions, e.g., PMIPv6, also have some limited IPv4 support. In conclusion, this requirement is met by existing DMM practices.

5.4. Considering existing mobility protocols - REQ4

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

As stated in [RFC7333], a DMM solution could reuse existing IETF and standardized protocols before specifying new protocols. Besides, Section 4 of this document discusses various ways to flatten and distribute current mobility solutions. Actually, nothing prevents the distribution of mobility functions within IP mobility protocols. However, as discussed in Section 5.1 and Section 5.2, limitations exist.

The 3GPP data plane anchoring function, i.e., the PGW, can also be distributed, but with limitations; e.g., no anchoring relocation, no context transfer between anchors and centralized control plane. The 3GPP architecture is also going in the direction of flattening with SIPTO and LIPA, though they do not provide full mobility support.

For example, mobility support for SIPTO traffic can be rather limited, and offloaded traffic cannot access operator services. Thus, the operator must be very careful in selecting which traffic to offload.

5.5. Coexistence with deployed networks/hosts and operability across different networks - REQ5

According to [RFC7333], DMM implementations are required to co-exist with existing network deployments, end hosts and routers. Additionally, DMM solutions are expected to work across different networks, possibly operated as separate administrative domains, when the necessary mobility management signaling, forwarding, and network access are allowed by the trust relationship between them. All current mobility protocols can co-exist with existing network deployments and end hosts. There is no gap between existing mobility protocols and this requirement.

5.6. Operation and management considerations - REQ6

This requirement actually comprises several aspects, as summarized below.

- A DMM solution needs to consider configuring a device, monitoring the current operational state of a device, responding to events that impact the device, possibly by modifying the configuration and storing the data in a format that can be analyzed later.

- A DMM solution has to describe in what environment and how it can be scalably deployed and managed.

- A DMM solution has to support mechanisms to test if the DMM solution is working properly.

- A DMM solution is expected to expose the operational state of DMM to the administrators of the DMM entities.

- A DMM solution, which supports flow mobility, is also expected to support means to correlate the flow routing policies and the observed forwarding actions.

- A DMM solution is expected to support mechanisms to check the liveness of the forwarding path.

- A DMM solution has to provide fault management and monitoring mechanisms to manage situations where update of the mobility session or the data path fails.

- o A DMM solution is expected to be able to monitor the usage of the DMM protocol.

- o DMM solutions have to support standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules, which are expected to be created for DMM when needed for such configuration.

GAP6-1: Existing mobility management protocols have not thoroughly documented how, or whether, they support the above list of operation and management considerations. Each of the above needs to be considered from the beginning in a DMM solution.

GAP6-2: Management information base (MIB) objects are currently defined in [RFC4295] for MIPv6 and in [RFC6475] for PMIPv6. Standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules is lacking.

5.7. Security considerations - REQ7

As stated in [RFC7333], a DMM solution has to support any security protocols and mechanisms needed to secure the network and to make continuous security improvements. In addition, with security taken into consideration early in the design, a DMM solution cannot introduce new security risks, or amplify existing security risks, that cannot be mitigated by existing security protocols and mechanisms.

Any solutions that are intended to fill in gaps identified in this document need to meet this requirement. At present, it does not appear that using existing solutions to support DMM has introduced any new security issues. For example, Mobile IPv6 defines security features to protect binding updates both to home agents and correspondent nodes. It also defines mechanisms to protect the data packets transmission for Mobile IPv6 users. Proxy Mobile IPv6 and other variations of mobile IP also have similar security considerations.

5.8. Multicast - REQ8

It is stated in [RFC7333] that DMM solutions are expected to allow the development of multicast solutions to avoid network inefficiency in multicast traffic delivery.

Current IP mobility solutions address mainly the mobility problem for unicast traffic. Solutions relying on the use of an anchor point for tunneling multicast traffic down to the access router, or to the mobile node, introduce the so-called "tunnel convergence problem." This means that multiple instances of the same multicast traffic can

converge to the same node, diminishing the advantage of using multicast protocols.

[RFC6224] documents a baseline solution for the previous issue, and [RFC7028] a routing optimization solution. The baseline solution suggests deploying a Multicast Listener Discovery (MLD) proxy function at the MAG, and either a multicast router or another MLD proxy function at the LMA. The routing optimization solution describes an architecture where a dedicated multicast tree mobility anchor or a direct routing option can be used to avoid the tunnel convergence problem.

Besides the solutions highlighted before, there are no other mechanisms for mobility protocols to address the multicast tunnel convergence problem.

5.9. Summary

We next list the main gaps identified from the analysis performed above:

GAP1-1: Existing solutions only provide an optimal initial anchor assignment, a gap being the lack of dynamic anchor change/ new anchor assignment. Neither the HA switch nor the LMA runtime assignment allows changing the anchor during an ongoing session. MOBIKE allows change of GW but its applicability has been scoped to a very narrow use case.

GAP1-2: The MN needs to be able to perform source address selection. Proper mechanism to inform the MN is lacking to provide the basis for the proper selection.

GAP1-3: Currently, there is no efficient mechanism specified by the IETF that allows the dynamic discovery of the presence of nodes that can play the role of anchor, discover their capabilities and allow the selection of the most suitable one. However, the following mechanisms could help discovering anchors:

Dynamic Home Agent Address Discovery (DHAAD): the use of the home agent (H) flag in Router Advertisements (which indicates that the router sending the Router Advertisement is also functioning as a Mobile IPv6 home agent on the link) and the MAP option in Router Advertisements defined by HMIPv6.

GAP1-4: While existing network-based DMM practices may allow the deployment of multiple LMAs and dynamically select the best

one, this requires to still keep some centralization in the control plane, to access the policy database (as defined in RFC5213). Although [I-D.ietf-netext-pmip-cp-up-separation] allows a MAG to perform splitting of its control and user planes, there is a lack of solutions/extensions that support a clear control and data plane separation for IETF IP mobility protocols in a DMM context.

GAP2-1: The information of which sessions at the mobile node are active and are using the mobility support need to be transferred to or shared with the network. Such mechanism has not been defined.

GAP2-2: The mobile node needs to simultaneously use multiple IP addresses with different properties. There is a lack of mechanism to expose this information to the mobile node which can then update accordingly its source address selection mechanism.

GAP2-3: The handling of mobility management has not been to the granularity of an individual session of a user/device before. The combination of session identification and user/device identification may be lacking.

GAP6-1: Mobility management protocols have not thoroughly documented how, or whether, they support the following list of operation and management considerations:

* A DMM solution needs to consider configuring a device, monitoring the current operational state of a device, responding to events that impact the device, possibly by modifying the configuration and storing the data in a format that can be analyzed later.

* A DMM solution has to describe in what environment and how it can be scalably deployed and managed.

* A DMM solution has to support mechanisms to test if the DMM solution is working properly.

* A DMM solution is expected to expose the operational state of DMM to the administrators of the DMM entities.

* A DMM solution, which supports flow mobility, is also expected to support means to correlate the flow routing policies and the observed forwarding actions.

* A DMM solution is expected to support mechanisms to check the liveness of the forwarding path.

* A DMM solution has to provide fault management and monitoring mechanisms to manage situations where update of the mobility session or the data path fails.

* A DMM solution is expected to be able to monitor the usage of the DMM protocol.

* DMM solutions have to support standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules, which are expected to be created for DMM when needed for such configuration.

GAP6-2: Management information base (MIB) objects are currently defined in [RFC4295] for MIPv6 and in [RFC6475] for PMIPv6. Standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules is lacking.

6. Security Considerations

The deployment of DMM using existing IP mobility protocols raises similar security threats as those encountered in centralized mobility management systems. Without authentication, a malicious node could forge signaling messages and redirect traffic from its legitimate path. This would amount to a denial of service attack against the specific node or nodes for which the traffic is intended. Distributed mobility anchoring, while keeping current security mechanisms, might require more security associations to be managed by the mobility management entities, potentially leading to scalability and performance issues. Moreover, distributed mobility anchoring makes mobility security problems more complex, since traffic redirection requests might come from previously unconsidered origins, thus leading to distributed points of attack. Consequently, the DMM security design needs to account for the distribution of security associations between additional mobility entities.

7. Contributors

This document has benefited to valuable contributions from

Charles E. Perkins
Huawei Technologies
EMail: charliep@computer.org

who had produced a matrix to compare the different mobility protocols and extensions against a list of desired DMM properties. They were

useful inputs in the early work of gap analysis. He had continued to give suggestions as well as extensive review comments to this documents.

8. References

8.1. Normative References

[RFC7333] Chan, H., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", RFC 7333, August 2014.

8.2. Informative References

[I-D.anipko-mif-mpvd-arch]
Anipko, D., "Multiple Provisioning Domain Architecture", draft-anipko-mif-mpvd-arch-05 (work in progress), November 2013.

[I-D.bhandari-dhc-class-based-prefix]
Systems, C., Halwasia, G., Gundavelli, S., Deng, H., Thiebaut, L., Korhonen, J., and I. Farrer, "DHCPv6 class based prefix", draft-bhandari-dhc-class-based-prefix-05 (work in progress), July 2013.

[I-D.gundavelli-v6ops-community-wifi-svcs]
Gundavelli, S., Grayson, M., Seite, P., and Y. Lee, "Service Provider Wi-Fi Services Over Residential Architectures", draft-gundavelli-v6ops-community-wifi-svcs-06 (work in progress), April 2013.

[I-D.ietf-netext-pmip-cp-up-separation]
Wakikawa, R., Pazhyannur, R., Gundavelli, S., and C. Perkins, "Separation of Control and User Plane for Proxy Mobile IPv6", draft-ietf-netext-pmip-cp-up-separation-07 (work in progress), August 2014.

[I-D.korhonen-6man-prefix-properties]
Korhonen, J., Patil, B., Gundavelli, S., Seite, P., and D. Liu, "IPv6 Prefix Properties", draft-korhonen-6man-prefix-properties-02 (work in progress), July 2013.

[IEEE.802-16.2009]
"IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems", IEEE Standard 802.16, 2009, <http://standards.ieee.org/getieee802/download/802.16-2009.pdf>.

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

[RFC4066] Liebsch, M., Singh, A., Chaskar, H., Funato, D., and E. Shim, "Candidate Access Router Discovery (CARD)", RFC 4066, July 2005.

[RFC4067] Loughney, J., Nakhjiri, M., Perkins, C., and R. Koodli, "Context Transfer Protocol (CXTP)", RFC 4067, July 2005.

[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.

[RFC4295] Keeni, G., Koide, K., Nagami, K., and S. Gundavelli, "Mobile IPv6 Management Information Base", RFC 4295, April 2006.

[RFC4555] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006.

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

[RFC4889] Ng, C., Zhao, F., Watari, M., and P. Thubert, "Network Mobility Route Optimization Solution Space Analysis", RFC 4889, July 2007.

[RFC4960] Stewart, R., "Stream Control Transmission Protocol", RFC 4960, September 2007.

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

[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.

[RFC5555] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.

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

[RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

[RFC6020] Bjorklund, M., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, October 2010.

[RFC6097] Korhonen, J. and V. Devarapalli, "Local Mobility Anchor (LMA) Discovery for Proxy Mobile IPv6", RFC 6097, February 2011.

[RFC6224] Schmidt, T., Waehlisch, M., and S. Krishnan, "Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains", RFC 6224, April 2011.

[RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 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.

[RFC6475] Keeni, G., Koide, K., Gundavelli, S., and R. Wakikawa, "Proxy Mobile IPv6 Management Information Base", RFC 6475, May 2012.

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

[RFC6697] Zorn, G., Wu, Q., Taylor, T., Nir, Y., Hoeper, K., and S. Decugis, "Handover Keying (HOKEY) Architecture Design", RFC 6697, July 2012.

[RFC6705] Krishnan, S., Koodli, R., Loureiro, P., Wu, Q., and A. Dutta, "Localized Routing for Proxy Mobile IPv6", RFC 6705, September 2012.

[RFC6724] Thaler, D., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, September 2012.

[RFC7028] Zuniga, JC., Contreras, LM., Bernardos, CJ., Jeon, S., and Y. Kim, "Multicast Mobility Routing Optimizations for Proxy Mobile IPv6", RFC 7028, September 2013.

[SDO-3GPP.23.401] 3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", 3GPP TS 23.401 10.10.0, March 2013.

[SDO-3GPP.23.402] 3GPP, "Architecture enhancements for non-3GPP accesses", 3GPP TS 23.402 10.8.0, September 2012.

[SDO-3GPP.24.303] 3GPP, "Mobility management based on Dual-Stack Mobile IPv6; Stage 3", 3GPP TS 24.303 10.0.0, June 2013.

[SDO-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.

[SDO-3GPP.29.274] 3GPP, "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3", 3GPP TS 29.274 10.11.0, June 2013.

[SDO-3GPP.29.281] 3GPP, "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)", 3GPP TS 29.281 10.3.0, September 2011.

[SDO-3GPP.29.303] 3GPP, "Domain Name System Procedures; Stage 3", 3GPP TS 29.303 10.4.0, September 2012.

Authors' Addresses

Dapeng Liu (editor)
China Mobile
Unit2, 28 Xuanwumenxi Ave, Xuanwu District
Beijing 100053
China

Email: liudapeng@chinamobile.com

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

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

Pierrick Seite
Orange
4, rue du Clos Courtel, BP 91226
Cesson-Sevigne 35512
France

Email: pierrick.seite@orange.com

H Anthony Chan
Huawei Technologies
5340 Legacy Dr. Building 3
Plano, TX 75024
USA

Email: h.a.chan@ieee.org

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/