

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

H. Chan
Huawei Technologies
P. Seite
France Telecom - Orange
K. Pentikousis
Huawei Technologies
JH. Lee
Telecom Bretagne
November 7, 2012

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

Abstract

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

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 May 11, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	5
1.1. Overview	5
2. Conventions and Terminology	6
2.1. Conventions used in this document	6
2.2. Terminology	6
3. Mobility Management Logical Functions	7
4. Functional Representation of Existing Mobility Protocols	7
4.1. Mobile IPv6	8
4.2. MIPv6 versus PMIPv6	8
4.3. Hierarchical Mobile IPv6	10
4.4. Distributing mobility anchors	11
4.5. Migrating Home Agents	12
5. DMM Functional Scenarios	14
5.1. Flat Network Scenario	14
5.1.1. Network-based Mobility Management	14
5.1.2. Client-based Mobility Management	15
5.2. Fully distributed scenario with separation of control and data planes	16
6. Gap analysis	18
6.1. DMM Requirements	18
6.1.1. Considering existing protocols first	18
6.1.2. Compatibility	18
6.1.3. IPv6 deployment	19
6.1.4. Security considerations	19
6.1.5. Distributed deployment	20
6.1.6. Transparency to Upper Layers when needed	20
6.1.7. Route optimization	21
6.2. Mobility Protocols Gap Analysis	22
6.2.1. Gap analysis with the unified framework	22
6.2.2. Gap analysis with MIPv6	22
6.2.3. Gap analysis with PMIPv6	22
6.2.4. Gap analysis with HMIPv6	22
6.2.5. Gap analysis with Distributing Mobility Anchors	23
6.2.6. Gap analysis with HAHA	23
6.2.7. Gap analysis with Dynamic mobility management	23
6.2.8. Gap Analysis with Multiple MRs and Distributed LM Database	24
6.2.9. Gap Analysis with Route Optimization Mechanisms	24
6.3. Gap analysis summary	24
7. DMM analysis	25
7.1. DMM scenarios and Dynamic mobility management requirement	26
7.2. Route optimization of DMM scenarios	27
8. Security Considerations	30
9. IANA Considerations	30
10. References	30

10.1. Normative References	30
10.2. Informative References	30
Authors' Addresses	33

1. Introduction

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

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

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

The following subsection presents an overview of this document.

1.1. Overview

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

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

be built upon.

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

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

2. Conventions and Terminology

2.1. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2.2. Terminology

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

In addition, this document uses the following terms:

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

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

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

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

3. Mobility Management Logical Functions

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

1. Anchoring: allocation of home network prefix or HoA to an MN that registers with the network;
2. Mobility Routing (MR) function: packets interception and forwarding to/from the HoA of the MN, based on the internetwork location information, either to the destination or to some other network element that knows how to forward the packets to their destination;
3. Internetwork Location Management (LM) function: managing and keeping track of the internetwork location of an MN, which includes a mapping of the HoA to the mobility anchoring point that the MN is anchored to;
4. Location Update (LU): provisioning of MN location information to the LM function;
5. Routing Control (RC): this logical function configures the forwarding state of the mobility routing function.

4. Functional Representation of Existing Mobility Protocols

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

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

4.1. Mobile IPv6

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

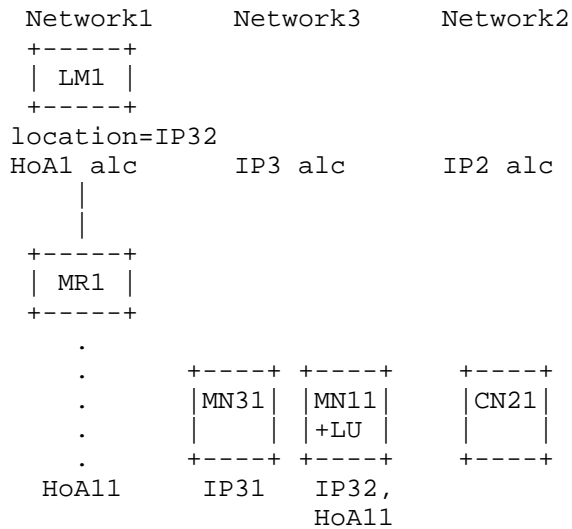


Figure 1. Functional decomposition of Mobile IPv6.

4.2. MIPv6 versus PMIPv6

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

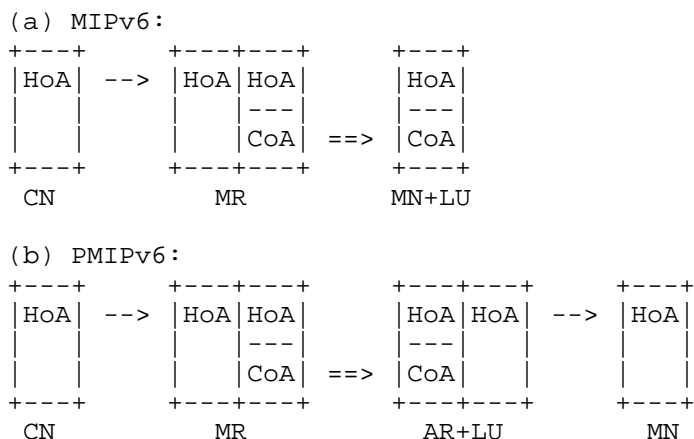


Figure 2. Network layer in the protocol stack of packets sent from the CN and tunneled (a) to the MN+LU in MIPv6; and (b) to the AR+LU in PMIPv6 showing the destination IP address as the packet traverses from the CN to the MN.

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

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

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

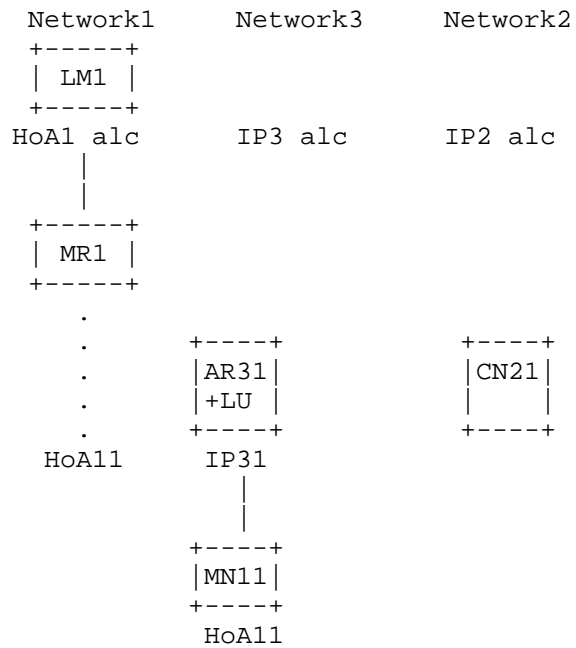


Figure 3. Functional representation of PMIPv6.

4.3. Hierarchical Mobile IPv6

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

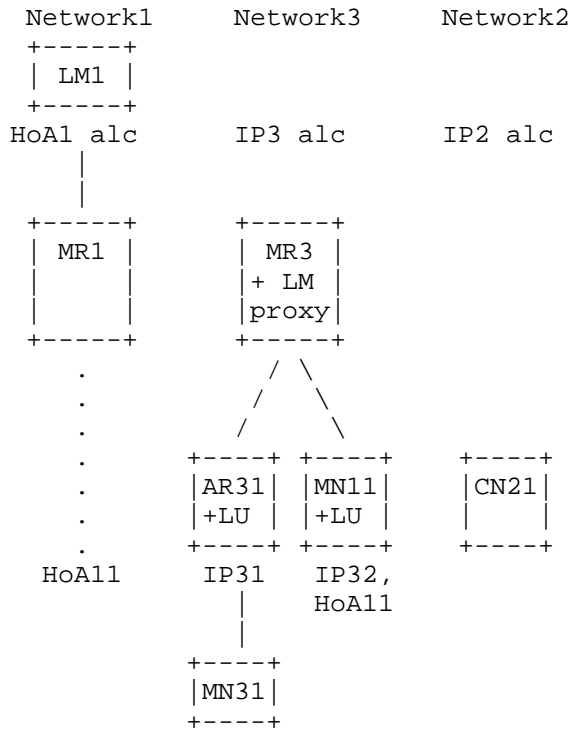


Figure 4. Functional representation of Hierarchical Mobile IPv6.

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

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

4.4. Distributing mobility anchors

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

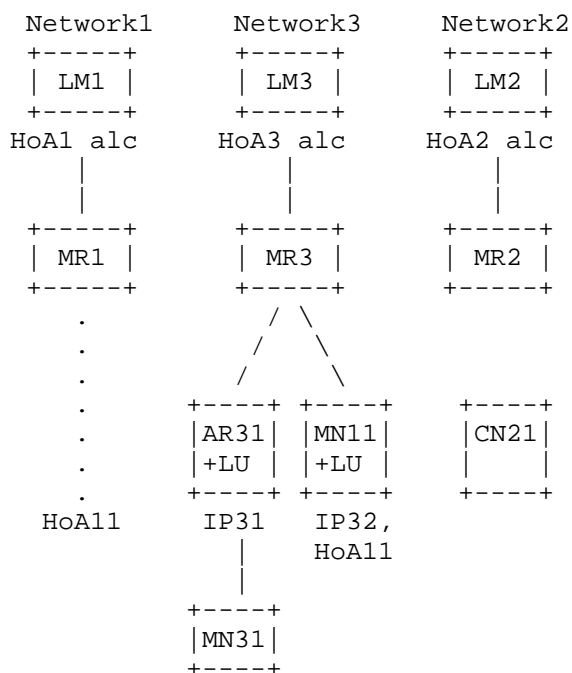


Figure 5. Functional representation of distributing mobility anchors.

4.5. Migrating Home Agents

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

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

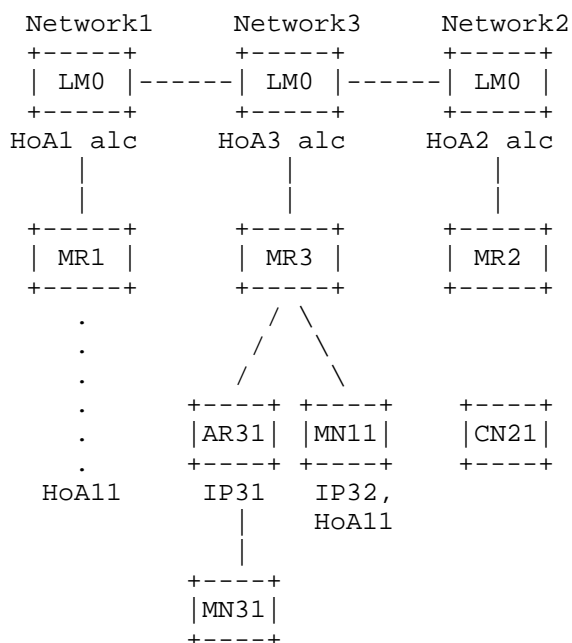


Figure 6. Functional representation of Migrating Home Agents.

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

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

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

5. DMM Functional Scenarios

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

5.1. Flat Network Scenario

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

1. the AR can act as a legacy IP router;
2. the AR can provide the MR function (i.e. act as mobility anchor);
3. the AR can provide the LU functions;
4. the AR can provide both MR and LU functions.

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

5.1.1. Network-based Mobility Management

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

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

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

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

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

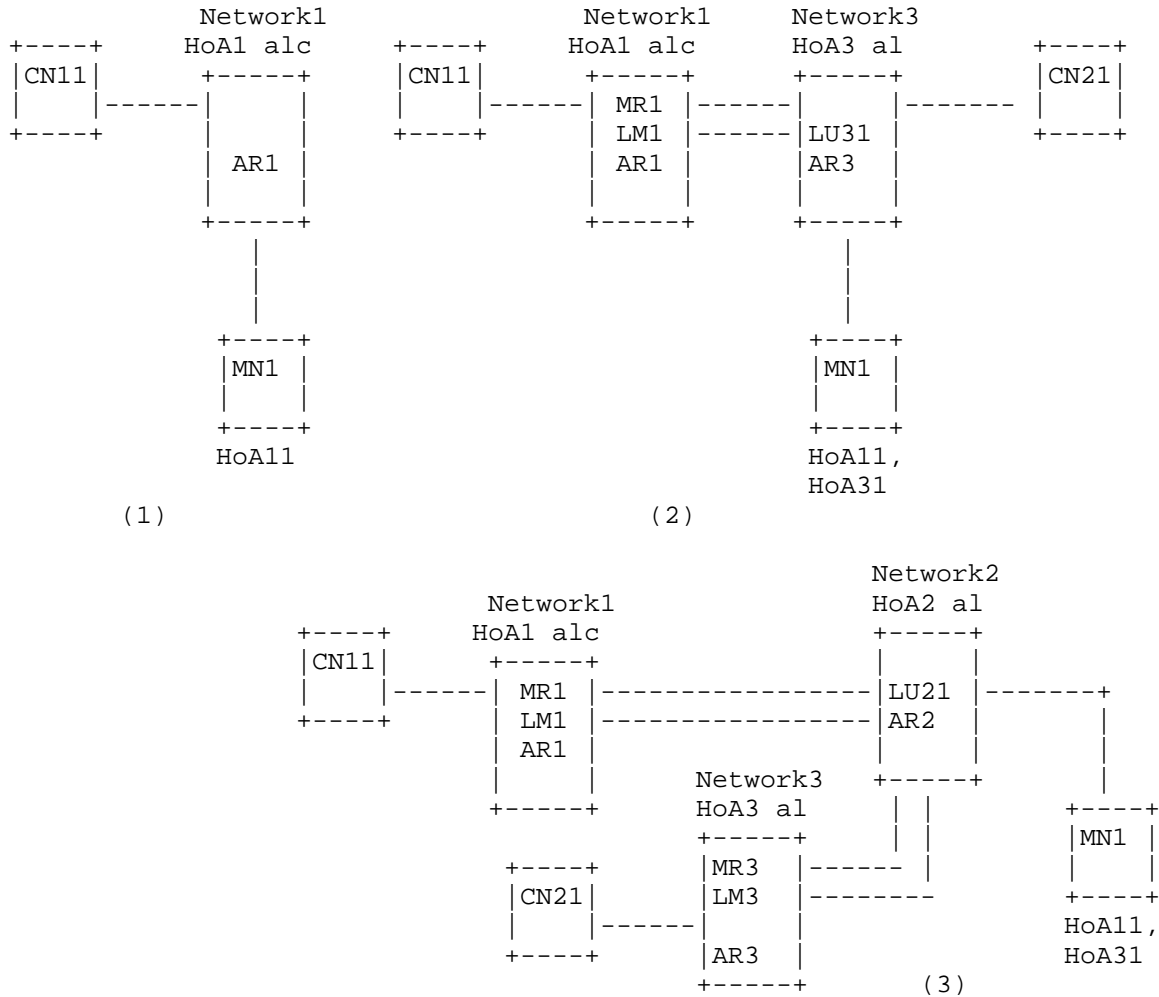


Figure 7. Network-based DMM architecture for a flat network.

5.1.2. Client-based Mobility Management

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

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

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

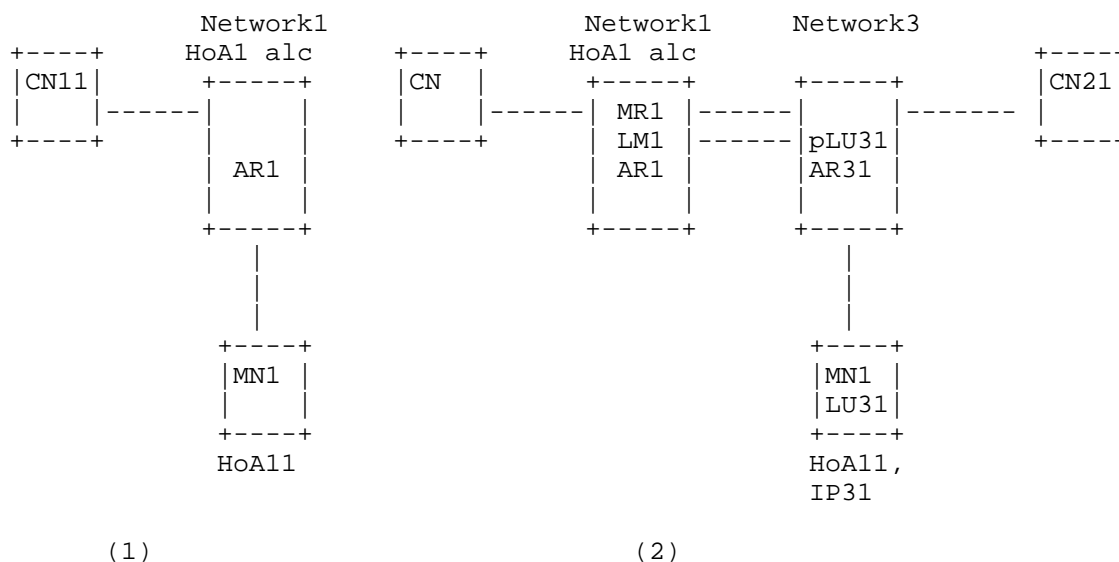


Figure 8. Client-based DMM architecture for a flat network.

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

This scenario considers multiple MRs and a distributed LM database.

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

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

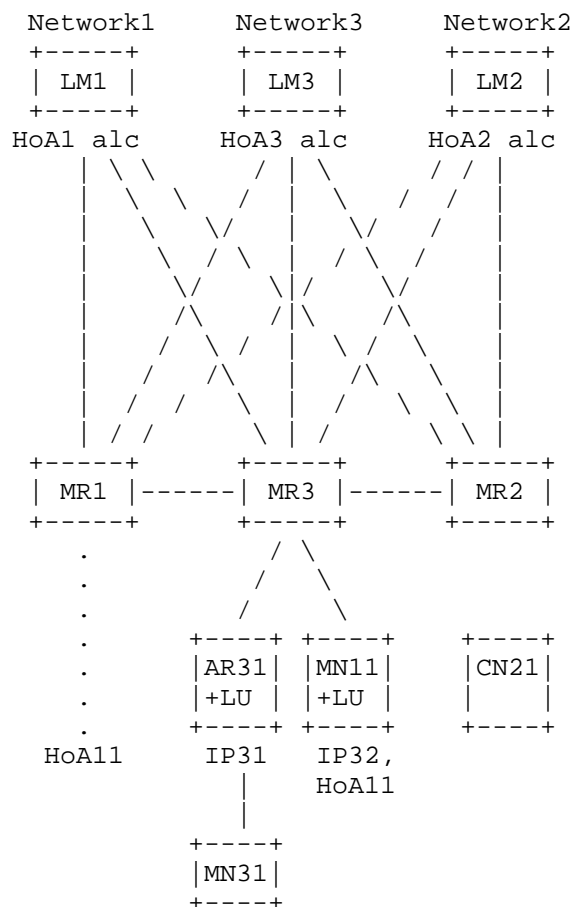


Figure 9. A distributed architecture for mobility management.

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

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

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

6. Gap analysis

6.1. DMM Requirements

6.1.1. Considering existing protocols first

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

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

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

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

6.1.2. Compatibility

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

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

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

6.1.3. IPv6 deployment

The third DMM requirement on IPv6 deployment is the following.

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

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

6.1.4. Security considerations

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

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

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

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

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

6.1.5. Distributed deployment

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

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

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

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

6.1.6. Transparency to Upper Layers when needed

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

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

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

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

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

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

6.1.7. Route optimization

The second part of first requirement is on route optimization.

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

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

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

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

6.2. Mobility Protocols Gap Analysis

6.2.1. Gap analysis with the unified framework

The use of the unified framework meets the following requirements:

REQ4: Considering existing protocols first

REQ5: (first part) compatibility

REQ3: IPv6 deployment

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

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

6.2.2. Gap analysis with MIPv6

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

REQ6: Security consideration

Trust between MN and MR is needed.

6.2.3. Gap analysis with PMIPv6

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

REQ6: Security consideration

Trust between AR and MR is needed.

Trust between MN and MR is needed.

6.2.4. Gap analysis with HMIPv6

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

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

REQ6: Security consideration

Trust between MRs in different networks is needed.

6.2.5. Gap analysis with Distributing Mobility Anchors

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

REQ1: Distributed deployment

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

6.2.6. Gap analysis with HAHA

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

In addition, trust between the LM servers is needed.

REQ6: Security consideration

Trust among the LM servers is needed.

6.2.7. Gap analysis with Dynamic mobility management

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

REQ2: Transparency to upper layers when needed.

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

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

6.2.8. Gap Analysis with Multiple MRs and Distributed LM Database

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

REQ1: (part 2) Distributed deployment

The LMs may generalize into a distributed database.

REQ6: Security considerations

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

6.2.9. Gap Analysis with Route Optimization Mechanisms

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

REQ1: (part 2) Distributed deployment

MR may cache the LM information when needed.

MR function is needed in the CN's network.

REQ6: Security considerations

Trust between the MR and the LM is needed.

6.3. Gap analysis summary

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

Table 1. Summary of Gap Analysis

	Existing proto- cols first	Compati- bility	IPv6 deploy- ment	Security consi- derations	Distri- buted deploy- ment	Upper- layer trans- parency when needed	Route Optimi- zation
Unified framework	Y	Y	Y				
MIPv6	Y	Y	Y	Y	N	N	N
PMIPv6	Y	Y (supports above)	Y	Y (MN-AR)	N	N	N
HMIPv6	Y	Y (supports above)	Y	Y (MN-AR)	N	N	N
Optimize route	Y	Y (supports above)	Y	Y	N	N	locat- ion pr ivacy
Distribute mobility anchors	Y	Y (supports above)	Y	Y	Y	N	N
Multiple MRs and Distri- buted LM database	Y	Y (supports above)	Y	Y (LM-MR in different networks)	Y	Y	
Dynamic mobility	Y	Y (supports above)	Y	Y (LM,MR-MR in different networks)	Y	Y (HoA of appl)	most cases
DMM	Y	Y (supports above)	Y	Y (LM,MR-MR in different networks)	Y	Y (HoA of appl)	except 1st pkts

7. DMM analysis

This section analyses how DMM proposals meet above requirements.

7.1. DMM scenarios and Dynamic mobility management requirement

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

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

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

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

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

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

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

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

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

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

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

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

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

7.2. Route optimization of DMM scenarios

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

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

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

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

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

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

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

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

RS1.CN-MR(CN).gw/ar: Co-locate the MR function at a convenient location to which the packet will always pass. Such locations may be the gateway router or the access router. This approach will be described later.

It is noted here that in a PMIPv6 design with a hierarchical network, the MAG generally is at the access router but LMA can be in the gateway router of a network. Whether a distributed mobility design enhances the MAG or the LMA may involve quite different mechanisms. Yet when looking at the logical function, it is basically the same MR function whether this function co-locates with the access router or the gateway router. This draft therefore put both approaches together. There is however a difference that the access router needs to perform proxy function when using PMIPv6. Yet the logical MR functions are the same. It is again noted that in flattened network, the access router and the gateway router may merge together. With they are merged, the needed function is again the same logical MR function.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Security Considerations

TBD

9. IANA Considerations

None

10. References

10.1. Normative References

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

10.2. Informative References

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

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

- [I-D.jikim-dmm-pmip]
Kim, J., Koh, S., Jung, H., and Y. Han, "Use of Proxy Mobile IPv6 for Distributed Mobility Management", draft-jikim-dmm-pmip-00 (work in progress), March 2012.
- [I-D.liebsch-mext-dmm-nat-phl]
Liebsch, M., "Per-Host Locators for Distributed Mobility Management", draft-liebsch-mext-dmm-nat-phl-02 (work in progress), October 2012.
- [I-D.liu-dmm-dynamic-anchor-discussion]
Liu, D., Deng, H., and W. Luo, "DMM Dynamic Anchor Discussion", draft-liu-dmm-dynamic-anchor-discussion-00 (work in progress), March 2012.
- [I-D.liu-dmm-pmip-based-approach]
Liu, D., Song, J., and W. Luo, "PMIP Based DMM Approaches", draft-liu-dmm-pmip-based-approach-02 (work in progress), March 2012.
- [I-D.luo-dmm-pmip-based-dmm-approach]
Luo, W. and J. Liu, "PMIP Based DMM Approaches", draft-luo-dmm-pmip-based-dmm-approach-01 (work in progress), March 2012.
- [I-D.ma-dmm-armip]
Ma, Z. and X. Zhang, "An AR-level solution support for Distributed Mobility Management", draft-ma-dmm-armip-00 (work in progress), February 2012.
- [I-D.patil-dmm-issues-and-approaches2dmm]
Patil, B., Williams, C., and J. Korhonen, "Approaches to Distributed mobility management using Mobile IPv6 and its extensions", draft-patil-dmm-issues-and-approaches2dmm-00 (work in progress), March 2012.
- [I-D.sarikaya-dmm-dmipv6]
Sarikaya, B., "Distributed Mobile IPv6", draft-sarikaya-dmm-dmipv6-00 (work in progress), February 2012.
- [I-D.seite-dmm-dma]
Seite, P. and P. Bertin, "Distributed Mobility Anchoring", draft-seite-dmm-dma-05 (work in progress), July 2012.
- [I-D.xue-dmm-routing-optimization]
Xue, K., Li, L., Hong, P., and P. McCann, "Routing optimization in DMM",

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

[I-D.yokota-dmm-scenario]

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

[MHA]

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

[Paper-Distributed.Centralized.Mobility]

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

[Paper-Distributed.Dynamic.Mobility]

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

[Paper-Distributed.Mobility.Management]

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

[Paper-Distributed.Mobility.PMIP]

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

[Paper-Distributed.Mobility.Review]

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

[Paper-Host.based.DMM]

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

[Paper-Migrating.Home.Agents]

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

[Paper-Net.based.DMM]

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

[Paper-SMGI]

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

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

[RFC4988] Koodli, R. and C. Perkins, "Mobile IPv4 Fast Handovers", RFC 4988, October 2007.

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

[RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.

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

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

Authors' Addresses

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

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

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

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

V6OPS WG
Internet-Draft
Intended status: Informational
Expires: October 25, 2013

S. Gundavelli
M. Grayson
Cisco
P. Seite
France Telecom - Orange
Y. Lee
Comcast
April 23, 2013

Service Provider Wi-Fi Services Over Residential Architectures
draft-gundavelli-v6ops-community-wifi-svcs-06.txt

Abstract

The tremendous growth in Wi-Fi technology adoption over the last decade has met the ultimate possible goal of 100% adoption rate. All most every new mobile device is now equipped with IEEE 802.11-based wireless interface and with pre-configured policy to prefer Wi-Fi to cellular access. Matching this evolution is every service provider's desire to offer Wi-Fi based broadband services; a new business opportunity even for fixed line operators. Operators are exploring options to monetize their existing networks, most with nation-wide footprint, to build a high-speed Wi-Fi service that can be the basis for offering new wireless broadband services. This document identifies the requirements for supporting these new Wi-Fi community services and the mobility tools which have been standardized in IETF that can be used for enabling these architectures.

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 October 25, 2013.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	4
2. Conventions and Terminology	5
2.1. Conventions	5
2.2. Terminology	5
3. Deployment Models	7
4. Requirements	8
4.1. IPv6 Addressing Model for SP WiFi Architectures	9
4.2. Subscriber Authentication & Service Authorization	9
4.3. Location-based Services	9
4.4. Local Services Access & Internet Traffic Offload	10
4.5. Web-based Authentication Support	10
4.6. Transparent Auto Login (TAL)	10
4.7. Multiple WLAN SSID Support	11
4.8. Multiple Home Network Service (APN) Access	11
4.9. CPE Identity and Authorization	11
4.10. Mobility within the WLAN Access Network	11
4.11. Mobility across WLAN and Macro Access	12
4.12. Differentiated Services for Users behind RG	12
4.13. Lawful Intercept (LI)	12
4.14. Subscriber Management and Charging	13
4.15. Handling the Walk-by Users	14
4.16. Overlapping IPv4 Address Support	14
4.17. Service Provisioning & Monitoring	14
5. Solution Approaches & Considerations	15
5.1. PMIPv6 MAG on the RG: Layer-3 Encapsulation between CPE and Access Gateway	15
5.2. Ethernet-over-IP Support on the RG: Layer-2 Encapsulation between CPE and Access Gateway	15
5.3. Local Aggregation for Subscriber Control and Internet Offload	15
5.4. Mobility Chaining: Integration with Mobile Packet Core	15
6. IANA Considerations	15
7. Security Considerations	15
8. Acknowledgements	16
9. References	16
9.1. Normative References	16
9.2. Informative References	16
Authors' Addresses	17

1. Introduction

The tremendous growth in Wi-Fi technology adoption over the last decade has met the ultimate possible goal of 100% adoption rate. All most every new mobile device is now equipped with IEEE 802.11-based wireless interface and these devices are typically pre-configured with a policy to prefer Wi-Fi to cellular access. This so called, "cheap access based on unlicensed spectrum", is no longer considered an unreliable access, but with all the available protocol tools and with maturity in technology, building a reliable broadband service that can meet the committed service-level agreements is proving to be a non-issue.

Matching this evolution is every service provider's desire to offer Wi-Fi based broadband services; a new business opportunity even for both fixed and mobile operators. The demand for bandwidth is only growing with the availability of new smart devices, new technology applications and with all the content in the Internet. Furthermore, an increasing percentage of mobile consumption is happening in the home and so DSL/Cable operators are exploring options to monetize their existing networks, most with nation-wide footprint, to build a high-speed, nation-wide Wi-Fi service that can be the basis for offering new wireless broadband services and for building roaming agreements with traditional mobile operators, who are unable to meet the mobile subscriber growth due to the finite licensed spectrum available for macro-cell deployments. Every residential CPE device that the operator owns can now be enabled to provide Wi-Fi service and new community Wi-Fi hotspots can be built in any location where there is fixed line coverage. A wireless service based on unlicensed spectrum, and leveraging existing transport is a huge incentive for operators to enter this new market.

To support these business goals, operators are looking at mobility architectures for supporting various requirements. Not all requirements are well understood, and neither are the implications with the chosen solution approaches for each of those requirements. The choice of the architecture has an implication on the CPE evolution and on the core infrastructure feature requirements. Therefore, the sole purpose and the goal of this document is to present all the requirements, identify the protocol tools and any potential gaps. This analysis is important for enabling the network vendors and the mobile operators to make the right design choices and leverage the existing tools that the mobility groups in IETF have already developed and discourage them from adopting proprietary, non-standard mechanisms or developing redundant alternatives.

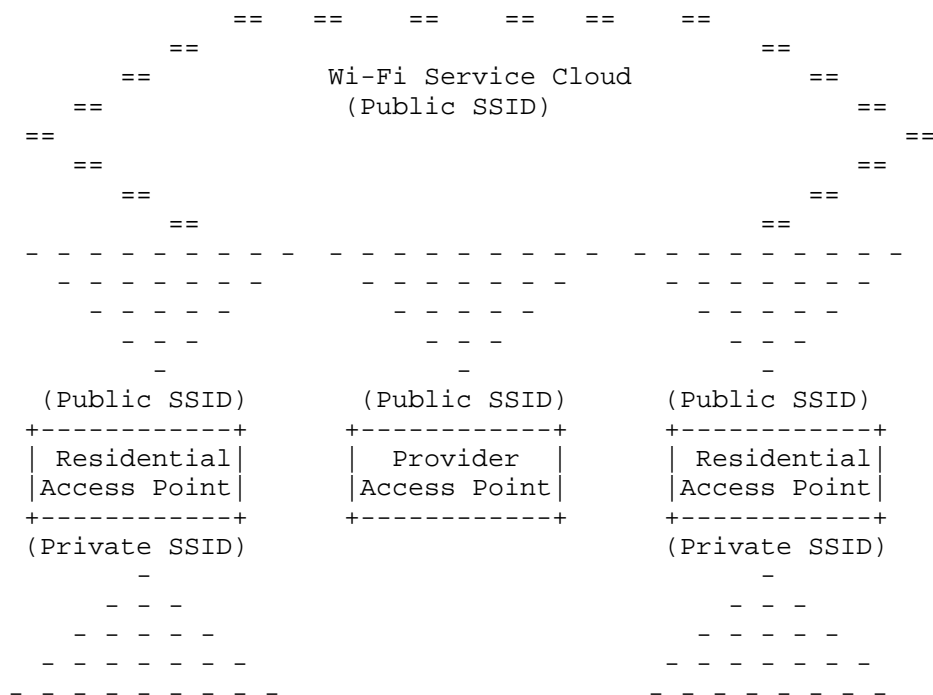


Figure 1: Wi-Fi Cloud Over Residential Gateways

2. Conventions and Terminology

2.1. Conventions

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 RFC 2119 [RFC2119].

2.2. Terminology

This document uses the following abbreviations and definitions:

Community Wi-Fi Service

It is a Wi-Fi based broadband service offered by a service provider. The Wi-Fi Access Points that are part of this service are owned and managed by the operator, and physically located in carrier premises. These operator owned CPE's typically have a large Wi-Fi coverage area, operated on a higher signal power.

There could also be the residential Access Points that are part of this service, located in the subscriber homes, that are part of this service and allowing community access to a public SSID along with a private SSID for their personal access.

Wi-Fi Operator

A service provider that offers Community Wi-Fi services. Wi-Fi operator can be a wireline operator, mobile operator or an operator offering both wireline and mobile services.

Residential Gateway (RG)

It is a network device that is located in the Customer premises and is also referred to as Residential CPE (Customer Premises Equipment). This device is connected to service providers network and defines the demarcation point between the provider and the customer. In the context of this document this is hosting the 802.11 Access Point function.

WLAN controller (WLC)

It is an entity responsible for performing radio resource management (RRM) on the Access Points, system-wide mobility policy enforcement and centralized forwarding function for the user traffic.

Mobile Gateway

It is network entity anchoring IP traffic in the mobile core network. This entity allocates an IP address which is topologically valid in the mobile network and may act as a mobility anchor if handover between mobile and Wi-Fi is supported.

Home/Roaming User

The home user is the owner of the network where the Residential Gateway is located and is paying for the service associated with that Residential Gateway. A Roaming User is a visitor from the operator's home network, or from a partner's network and is allowed to access broadband services using that Residential Gateway and over a Public SSID.

Access Point Name (APN)

Its the name of a packet data network. This APN concept was first introduced in GPRS by 3GPP to enable legacy Intelligent Networking (IN) approaches to be applied to the newly deployed IP packet data services. In roaming deployments, the APN construct was visible to the visited network and allowed legacy IN charging solutions to be supported. Defining an application specific APN then allowed application charging to be supported.

Addressing Models

The term Per-MN-Prefix model [RFC5213] is used to refer to an addressing model where there is a unique network prefix or prefixes assigned for each mobile node. The term Shared-Prefix model [RFC5213] is used to refer to an addressing model where the prefix(es) are shared by more than one node.

3. Deployment Models

Figure 2 illustrates the most common residential and hotspots Wi-Fi deployment models.

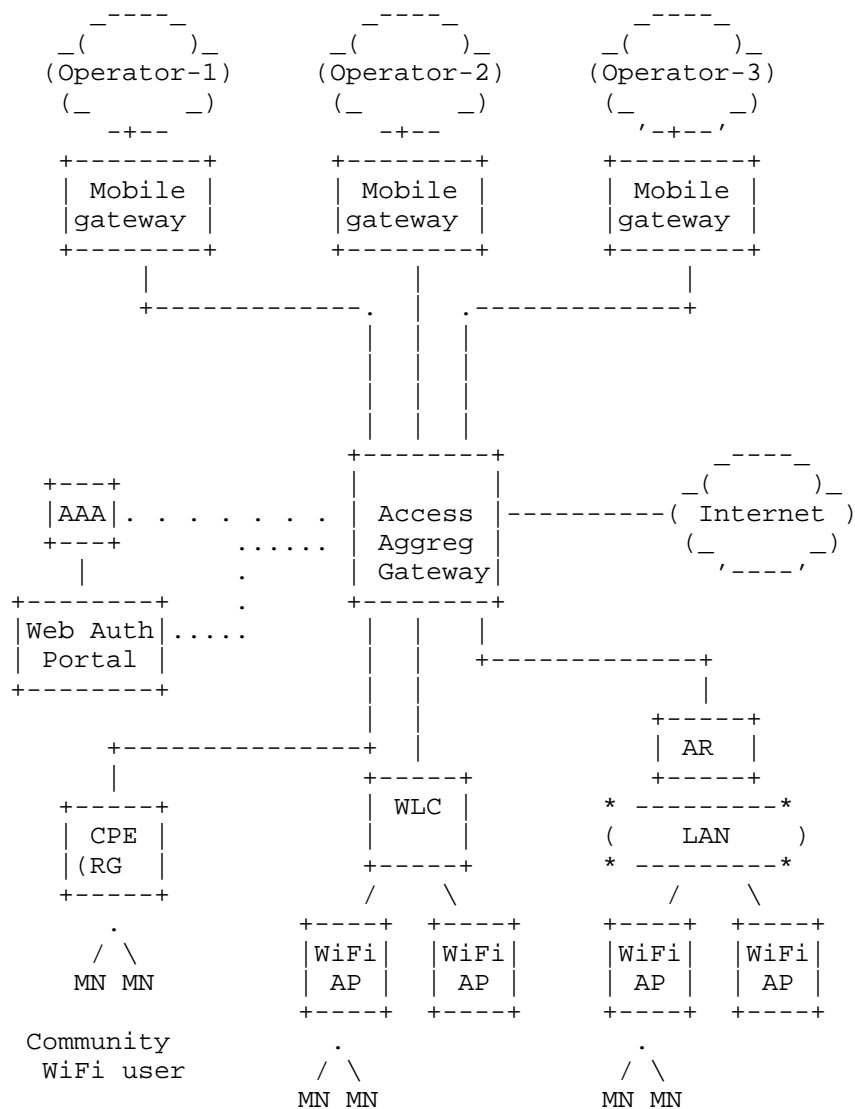


Figure 2: WLAN Service for Retail Model

4. Requirements

4.1. IPv6 Addressing Model for SP WiFi Architectures

The selection of the right IPv6 addressing model for the SP WiFi architectures is an important consideration. There are these two IPv6 addressing models:

- o Unique-Prefix Model - As per this addressing model, home network prefix(es) assigned to a mobile node are for its exclusive use and no other node shares an address from that prefix (other than the Subnet-Router anycast address [RFC4291] that is used by the IPv6 access router hosting that prefix on that link). There could be multiple unique IPv6 prefixes assigned to each mobile node.
- o Shared-Prefix model - The IPv6 prefix that is assigned to the mobile node is a shared prefix. There can be more than one mobile node that can be using IPv6 addresses from that prefix.

3GPP architecture supports Unique-Prefix model for the mobile node's PDN connections. This decision was largely influenced by the IETF recommendation to 3GPP to support this specific addressing model. In the context of SP WiFi, there are clearly scenarios where a mobile node may perform an inter-technology handover from the macro network to the WLAN access network and handoff the session and is important that the addressing model is the same in both the access architectures. Even in deployment models where such handovers are not envisioned, such as an WLAN access aggregation architecture with no mobile packet core integration, there are sufficient reasons for adopting the Unique Prefix model.

4.2. Subscriber Authentication & Service Authorization

Community Wi-Fi service is designed to be available for public access. Wi-Fi operator must authenticate users before offering services to them. Once a user is authenticated, Wi-Fi operator will authorize services based on the user identity. There are many authentication mechanisms, such as 802.1x, Web-authentication, WISPr that the operator may deploy for this purpose.

4.3. Location-based Services

In many deployments, there is a need for the mobile operator to provide differentiated services and policing to the mobile nodes based on the access network to which they are attached. Policy systems in mobility architectures such as PCC and ANDSF in 3GPP system allow configuration of policy rules with conditions based on the access network information. For example, the service treatment for the mobile node's traffic may be different when they are attached to a access network owned by the home operator than when owned by a

roaming partner. The service treatment can also be different based on the configured Service Set Identifiers (SSID) in case of IEEE 802.11 based access networks. Other examples of location services include the operator's ability to display a location specific Web Page, or apply tariff based on the location.

4.4. Local Services Access & Internet Traffic Offload

In the integrated WLAN-EPC architectures, the mobile node's IP traffic is always tunneled back from the access network to the mobile gateway in the home network. However, with the exponential growth in the mobile data traffic, mobile operators are exploring new ways to offload some of the IP traffic flows at the nearest access edge where ever there is an internet peering point, as supposed to carrying it all the way to the mobility anchor in the home network. Not all IP traffic need to be routed back to the home network, some of the non-essential traffic which does not require IP mobility support can be offloaded at the mobile access gateway in the access network. This approach provides greater leverage and efficient usage of the mobile packet core which help lowering transport cost.

4.5. Web-based Authentication Support

Most Public Wireless LAN (PWLAN) deployments today use web-based authentication for authorizing the user for network access. Web-based mode of authentication is considered a legacy mode, for its weak security properties, and there are efforts to replace it with 802.1x-based security mechanisms. However, a very high percentage of the PWLAN deployments are still using using this authentication mode and operators are not willing to move away from this mode any time soon. The reason being, lack of support for 802.1x/EAP support on the 100's of millions of handsets that are out there, and for the lack of client software in the laptops running various operating systems versions. This is forcing the operators to support web-based authentication.

4.6. Transparent Auto Login (TAL)

In many deployments, there is a need to support Transparent Auto Login capability. This is essentially an approach for maintaining Authenticated state for a user, for a duration of time. Once an authenticated user disconnects and re-attaches to the network, the network should allows instant access without forcing the user to re-authenticate.

4.7. Multiple WLAN SSID Support

A Wi-Fi Operator may broadcast multiple SSIDs. In case Residential Wi-Fi hotspots, there can be one set of private SSIDs specific to that home user and there can be another set of public SSIDs for wider community use. In case of public hotspots, the operator can advertise the public SSID for its own subscribers and also public SSID's belonging to other operators with whom the operator has roaming relationships.

4.8. Multiple Home Network Service (APN) Access

The 3GPP system architecture supports the concept of an Access Point Name (APN). An APN can identify a particular routing domain and can be used by 3GPP operators to segment user traffic. APNs are included in the session establishment signaling sent by 3GPP User Equipments (UEs), identifying which routing domain they want to be connected to. Furthermore, 3GPP has defined a system architecture which supports the ability of a single UE to have simultaneous connectivity to a plurality of APNs, and be allocated multiple IPv4 addresses and/or IPv6 prefixes from the network.

There is a need to ensure multiple APN access for a subscriber in the community Wi-Fi network.

4.9. CPE Identity and Authorization

There are two known models with respect to CPE roll out. The consumer may purchase a device off the shelf and plugin to the network, or the operator at the time of service creation may have shipped a new device with the pre-provisioned service configuration. In either case, the operator needs to be able to identify the device based on the IP address and associate that to a given location.

The Wi-Fi network performs access control of UEs, via the CPE acting as AAA supplicant. As a result, the mobile network does not authenticate directly the user but shall trust the CPE performing the authentication.

4.10. Mobility within the WLAN Access Network

The mobile node should have the ability to roam within the Wi-Fi domain. Depending on the deployment model, the mobile node may roam across different IP subnets. To survive to such handover, some applications (e.g. VPN, streaming) need the IP address to be preserved.

A WLAN network may include a large number of Wi-Fi base stations. In

some occasions, two or more Wi-Fi base stations may cover the same area. When a subscriber receives Wi-Fi service in this overlapped area, the device may bounce between different base stations. This is typical Proximity problem. In this scenario, it is important for the WLAN to offer mobility to the subscriber as such the subscriber can continue the services without changing its IP address.

4.11. Mobility across WLAN and Macro Access

A mobile node should have the ability to handover from macro network to the Wi-Fi network and be able to retain IP address configuration and be able to access the home operator services.

4.12. Differentiated Services for Users behind RG

A Wi-Fi operator enabling Hotspot Services on a residential gateway is required to ensure the service levels for the home user is not impacted as a result of opening up the service for public usage. The home user should always have preferred access over public users and the operator may be bound to meet the Service Level Agreements. This essentially requires the operator to be able to differentiate the service flows and apply differentiated service treatment. The operator should be able to enforce QoS policing and labeling of packets to enforce QoS differentiation.

A single operator has deployed both a fixed access network and a mobile access network. In this scenario, the operator may wish a harmonized QoS management on both accesses. However the fixed access network does not implement a QoS control framework. So, the operator may choose to rely on the mobile network, specifying the standard framework to provide a QoS control, to enforce the QoS policy from the mobile gateway to the Wi-Fi Access network.

4.13. Lawful Intercept (LI)

Lawful Intercept [RFC2119] stands for legally authorized interception and monitoring of communications to and from a subscriber under Surveillance by a Law Enforcement Agency. In most of the countries, there are legal obligations for Service Providers to facilitate the intercept of any subscriber's communication if requested by law enforcement agencies. Communications Assistance for Law Enforcement Act (CALEA), the United States wiretapping law passed in 1994 is an example for such legal mandates. This section talks about Lawful Intercept solution requirements that are operators are required to support when offering WLAN services.

The following are the key considerations with respect to supporting Lawful Intercept capability in Wi-Fi architectures.

- o The operator should have the ability to capture IP traffic from any of the mobile nodes for which the operator is offering Wi-Fi services.
- o The ability to identify the Geo-location of the mobile node to the nearest WLAN access point.
- o The ability to track the mobile node's roaming within the network, even when there are no active IP flows.
- o The ability to pre-provision Lawful Intercept for an inactive mobile node so that the capture of IP traffic can be initiated anytime new IP flows associated to that mobile node are detected.
- o Lawful Intercept (LI) should be undetectable by the intercept subject
- o Mechanisms should be in place to limit unauthorized personnel from performing or knowing about lawfully authorized intercepts
- o If the information being intercepted is encrypted by the service provider and the service provider has access to the keys, then the information should be decrypted before delivery to the Law Enforcement Agency (LEA) or the encryption keys should be passed to the Law Enforcement Agency to allow them to decrypt the information.

4.14. Subscriber Management and Charging

It refers to the capability to manage network resources on a per subscriber, and eventually on a per-flow, basis. Subscriber management should be able to maintain a user context associating the user identifier with specific network resource (e.g. IP address, default router, mobility/traffic anchoring point,...), QoS profile, billing context and specific network functions (e.g. legal interception). The user context includes traffic selectors if subscriber management is on a per flow basis. Subscriber management should be done according to the user subscription, the user preferences and/or operator policies.

The ability to charge the subscriber is the fundamental business requirement before an operator can deploy the Wi-Fi service. The operator should have the ability to enforce charge the subscriber by usage and enforce quota policies. This is the basis for keeping the service operational and managing inter-operator roaming agreements.

4.15. Handling the Walk-by Users

In the case of community Wi-Fi, the network is an open network with the SSID visible to any wireless LAN device. This essentially creates a situation where any walk-by user's mobile terminal automatically gets connected to the Wi-Fi network and results in a subscriber session creation. The user may not be having any intention in connecting to the Wi-Fi network and in fact may not be using the mobile device, but the device gets attached to the network and a subscriber session and other network resources get locked up for that user session. The situation is especially worse in public hotspots such as train stations, or Airports where there is high traffic. This is important that this situation is correctly handled.

4.16. Overlapping IPv4 Address Support

The transition from IPv4 to IPv6 is a long process, and during this period of transition, the Wi-Fi operators will have to continue to offer IPv4 services. However, these operators may not have sufficient public IPv4 addresses for all the Wi-Fi devices in their network. For addressing this IPv4 exhaust issue, operators may have to leverage transitioning technologies such as NAT64, Dual-Stack Lite, 6rd or other approaches. These operators may also choose to segment the network into regions and two regions may use overlapped IPv4 address space to provide IPv4 services to users.

In a different scenario, a roaming user from a partner's network, with an established mobility session with her home network, may be using a private IPv4 address and this IPv4 address may be overlapping with the address space that is being used in this access network. Furthermore, the IPv4 address space that is used for assignment to Wi-Fi subscribers should not conflict with the IPv4 addresses used on the Cable/DSL transport network.

The Wi-Fi operator should be able to handle all these scenarios related to overlapping private IPv4 address usage.

4.17. Service Provisioning & Monitoring

Deployment of any community based Wi-Fi access will require additional Wi-Fi specific configuration on a per Residential Gateway basis. In order to support scalable deployment, the Service Providers should be able to provision these configuration options remotely. This remote provisioning framework must support the following:

- o Secure provisioning of the RG with community WiFi parameters to minimize the theft of service
- o Ability to separate the private home subscriber traffic from the community WiFi traffic in the access network
- o Privacy and protection of private Residential subscriber traffic from the community WiFi users
- o Ability to remotely shut down an Residential Gateway which has been hijacked by hackers and is being used for DoS attacks.
- o Ability to temporarily disable services for the community based WiFi support while maintaining service to the Residential fixed broadband subscriber
- o Seamless integration of the WiFi provisioning aspects of the Residential Gateway into the existing RG provisioning infrastructure implemented by the Fixed Broadband Providers
- o Dynamic Service Monitoring Capability for managing the Wi-Fi Service.

5. Solution Approaches & Considerations

The following section identifies the different mobility approaches that Wi-Fi operator can leverage for deploying this Wi-Fi services.

- 5.1. PMIPv6 MAG on the RG: Layer-3 Encapsulation between CPE and Access Gateway
- 5.2. Ethernet-over-IP Support on the RG: Layer-2 Encapsulation between CPE and Access Gateway
- 5.3. Local Aggregation for Subscriber Control and Internet Offload
- 5.4. Mobility Chaining: Integration with Mobile Packet Core

6. IANA Considerations

This document does not require any IANA actions.

7. Security Considerations

This specification identifies the requirements for enabling Community

Wi-Fi Services over Residential architectures and the potential solution approaches for addressing those requirements. The security analysis for each of those requirements are covered in those respective sections.

8. Acknowledgements

The authors would like to thank Bill Choinski, John Coppola and Sangeeta Ramakrishnan for all the discussions related to Service Provider Wi-Fi Service requirements. The authors would also like to thank Byju Pularikkal for all the discussions and text contributions related to Lawful Interception and Service Provisioning.

9. References

9.1. Normative References

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

9.2. Informative References

- [I-D.gundavelli-netext-multiple-apn-pmipv6]
Gundavelli, S., Grayson, M., Lee, Y., Deng, H., and H. Yokota, "Multiple APN Support for Trusted Wireless LAN Access", draft-gundavelli-netext-multiple-apn-pmipv6-01 (work in progress), February 2012.
- [I-D.gundavelli-netext-pmipv6-wlan-applicability]
Gundavelli, S., "Applicability of Proxy Mobile IPv6 Protocol for WLAN Access Networks", draft-gundavelli-netext-pmipv6-wlan-applicability-03 (work in progress), April 2012.
- [I-D.ietf-netext-pmipv6-qos]
Liebsch, M., Seite, P., Yokota, H., Korhonen, J., and S. Gundavelli, "Quality of Service Option for Proxy Mobile IPv6", draft-ietf-netext-pmipv6-qos-00 (work in progress), June 2012.
- [I-D.ietf-netext-pmipv6-sipto-option]
Gundavelli, S., Zhou, X., Korhonen, J., and R. Koodli, "IPv4 Traffic Offload Selector Option for Proxy Mobile IPv6", draft-ietf-netext-pmipv6-sipto-option-07 (work in progress), October 2012.

- [I-D.liebsch-netext-pmip6-authiwb]
Gundavelli, S., Liebsch, M., and P. Seite, "PMIPv6 inter-working with WiFi access authentication", draft-liebsch-netext-pmip6-authiwb-05 (work in progress), September 2012.
- [RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.
- [RFC3924] Baker, F., Foster, B., and C. Sharp, "Cisco Architecture for Lawful Intercept in IP Networks", RFC 3924, October 2004.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.
- [RFC6757] Gundavelli, S., Korhonen, J., Grayson, M., Leung, K., and R. Pazhyannur, "Access Network Identifier (ANI) Option for Proxy Mobile IPv6", RFC 6757, October 2012.
- [TS23402] 3GPP, "Architecture enhancements for non-3GPP accesses", 2010.

Authors' Addresses

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: sgundave@cisco.com

Mark Grayson
Cisco
11 New Square Park
Bedfont Lakes, FELTHAM TW14 8HA
ENGLAND

Email: mgrayson@cisco.com

Pierrick Seite
France Telecom - Orange
4, rue du clos courtel BP 91226
Cesson-Sevigne, 35512
France

Email: pierrick.seite@orange-ftgroup.com

Yiu L. Lee
Comcast
One Comcast Center
Philadelphia, PA 19103
U.S.A.

Email: yiulee@cable.comcast.com
URI: <http://www.comcast.com>

Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 7, 2014

H. Chan (Ed.)
Huawei Technologies
D. Liu
China Mobile
P. Seite
Orange
H. Yokota
KDDI Lab
J. Korhonen
Broadcom Communications
June 5, 2014

Requirements for Distributed Mobility Management
draft-ietf-dmm-requirements-17

Abstract

This document defines the requirements for Distributed Mobility Management (DMM) at the network layer. The hierarchical structure in traditional wireless networks has led primarily to centrally deployed mobility anchors. As some wireless networks are evolving away from the hierarchical structure, it can be useful to have a distributed model for mobility management in which traffic does not need to traverse centrally deployed mobility anchors far from the optimal route. The motivation and the problems addressed by each requirement are also described.

Requirements Language

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 RFC 2119 [RFC2119].

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 December 7, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	4
2. Conventions used in this document	5
2.1. Terminology	5
3. Centralized versus distributed mobility management	7
3.1. Centralized mobility management	7
3.2. Distributed mobility management	8
4. Problem Statement	9
5. Requirements	11
6. Security Considerations	17
7. IANA Considerations	17
8. Contributors	17
9. References	20
9.1. Normative References	20
9.2. Informative References	21
Authors' Addresses	23

1. Introduction

In the past decade a fair number of network-layer mobility protocols have been standardized [RFC6275] [RFC5944] [RFC5380] [RFC6301] [RFC5213]. Although these protocols differ in terms of functions and associated message formats, they all employ a mobility anchor to allow a mobile node to remain reachable after it has moved to a different network. The anchor point, among other tasks, ensures connectivity by forwarding packets destined to, or sent from, the mobile node. It is a centrally deployed mobility anchor in the sense that the deployed architectures today have a small number of these anchors and the traffic of millions of mobile nodes in an operator network are typically managed by the same anchor. Such a mobility anchor may still have to reside in the subscriber's provider network even when the subscriber is roaming to a visited network, in order that certain functions such as charging and billing can be performed more readily by the provider's network. An example provider network is a Third Generation Partnership Project (3GPP) network.

Distributed mobility management (DMM) is an alternative to the above centralized deployment. The background behind the interests to study DMM are primarily in the following.

- (1) Mobile users are, more than ever, consuming Internet content including that of local Content Delivery Networks (CDNs). Such traffic imposes new requirements on mobile core networks for data traffic delivery. To prevent exceeding the available core network capacity, service providers need to implement new strategies such as selective IPv4 traffic offload (e.g., [RFC6909], 3GPP work items Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO) [TS.23.401]) through alternative access networks such as Wireless Local Area Network (WLAN) [Paper-Mobile.Data.Offloading]. In addition, a gateway selection mechanism takes the user proximity into account within the Evolved Packet Core (EPC) [TS.29303]. Yet these mechanisms were not pursued in the past owing to charging and billing considerations which require solutions beyond the mobility protocol. Consequently, assigning a gateway anchor node from a visited network when roaming to the visited network has only recently been done and is limited to voice services.

Both traffic offloading and CDN mechanisms could benefit from the development of mobile architectures with fewer hierarchical levels introduced into the data path by the mobility management system. This trend of "flattening" the mobile networks works best for direct communications among peers in the same geographical area. Distributed mobility management in the flattening mobile networks would anchor the traffic closer to

the point of attachment of the user.

- (2) Today's mobile networks present service providers with new challenges. Mobility patterns indicate that mobile nodes often remain attached to the same point of attachment for considerable periods of time [Paper-Locating.User]. Specific IP mobility management support is not required for applications that launch and complete their sessions while the mobile node is connected to the same point of attachment. However, currently, IP mobility support is designed for always-on operation, maintaining all parameters of the context for each mobile subscriber for as long as they are connected to the network. This can result in a waste of resources and unnecessary costs for the service provider. Infrequent node mobility coupled with application intelligence suggest that mobility support could be provided selectively such as in [I-D.bhandari-dhc-class-based-prefix] and [I-D.korhonen-6man-prefix-properties], thus reducing the amount of context maintained in the network.

DMM may distribute the mobility anchors in the data-plane in flattening the mobility network such that the mobility anchors are positioned closer to the user; ideally, mobility agents could be collocated with the first-hop router. Facilitated by the distribution of mobility anchors, it may be possible to selectively use or not use mobility protocol support depending on whether such support is needed or not. It can thus reduce the amount of state information that must be maintained in various mobility agents of the mobile network. It can then avoid the unnecessary establishment of mechanisms to forward traffic from an old to a new mobility anchor.

This document compares distributed mobility management with centralized mobility management in Section 3. The problems that can be addressed with DMM are summarized in Section 4. The mandatory requirements as well as the optional requirements for network-layer distributed mobility management are given in Section 5. Finally, security considerations are discussed in Section 6.

The problem statement and the use cases [I-D.yokota-dmm-scenario] can be found in [Paper-Distributed.Mobility.Review].

2. Conventions used in this document

2.1. Terminology

All the 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 Mobility Related Terminology [RFC3753]. These terms include the following: mobile node (MN), correspondent node (CN), and home agent (HA) as per [RFC6275]; local mobility anchor (LMA) and mobile access gateway (MAG) as per [RFC5213], and context as per [RFC3753].

In addition, this draft introduces the following terms.

Centrally deployed mobility anchors

refer to the mobility management deployments in which there are very few mobility anchors and the traffic of millions of mobile nodes in an operator network are managed by the same anchor.

Centralized mobility management

makes use of centrally deployed mobility anchors.

Distributed mobility management

is not centralized so that traffic does not need to traverse centrally deployed mobility anchors far from the optimal route.

Hierarchical mobile network

has a hierarchy of network elements arranged into multiple hierarchical levels which are introduced into the data path by the mobility management system.

Flattening mobile network

refers to the hierarchical mobile network which is going through the trend of reducing its number of hierarchical levels.

Flatter mobile network

has fewer hierarchical levels compared to a hierarchical mobile network.

Mobility context

is the collection of information required to provide mobility management support for a given mobile node.

3. Centralized versus distributed mobility management

Mobility management is needed because the IP address of a mobile node may change as the node moves. Mobility management functions may be implemented at different layers of the protocol stack. At the IP (network) layer, mobility management can be client-based or network-based.

An IP-layer mobility management protocol is typically based on the principle of distinguishing between a session identifier and a forwarding address and maintaining a mapping between the two. In Mobile IP, the new IP address of the mobile node after the node has moved is the forwarding address, whereas the original IP address before the mobile node moves serves as the session identifier. The location management (LM) information is kept by associating the forwarding address with the session identifier. Packets addressed to the session identifier will first route to the original network which re-directs them using the forwarding address to deliver to the session. Re-directing packets this way can result in long routes. An existing optimization routes directly using the forwarding address of the host, and such is a host-based solution.

The next two subsections explain centralized and distributed mobility management functions in the network.

3.1. Centralized mobility management

In centralized mobility management, the location information in terms of a mapping between the session identifier and the forwarding address is kept at a single mobility anchor, and packets destined to the session identifier are forwarded via this anchor. In other words, such mobility management systems are centralized in both the control plane and the data plane (mobile node IP traffic).

Many existing mobility management deployments make use of centralized mobility anchoring in a hierarchical network architecture, as shown in Figure 1. Examples are the home agent (HA) and local mobility anchor (LMA) serving as the anchors for the mobile node (MN) and Mobile Access Gateway (MAG) in Mobile IPv6 [RFC6275] and in Proxy Mobile IPv6 [RFC5213] respectively. Cellular networks such as the 3GPP General Packet Radio System (GPRS) networks and 3GPP Evolved Packet System (EPS) networks employ centralized mobility management too. In the 3GPP GPRS network, the Gateway GPRS Support Node (GGSN), Serving GPRS Support Node (SGSN) and Radio Network Controller (RNC) constitute a hierarchy of anchors. In the 3GPP EPS network, the Packet Data Network Gateway (P-GW) and Serving Gateway (S-GW) constitute another hierarchy of anchors.

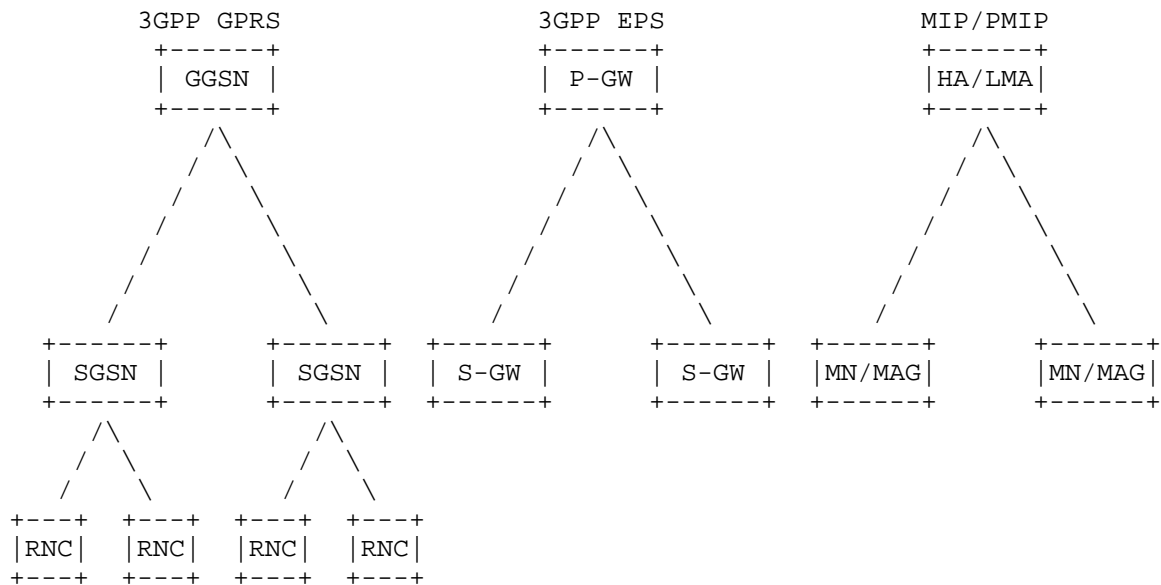


Figure 1. Centralized mobility management.

3.2. Distributed mobility management

Mobility management functions may also be distributed in the data plane to multiple networks as shown in Figure 2, so that a mobile node in any of these networks may be served by a nearby function with appropriate forwarding management (FM) capability.

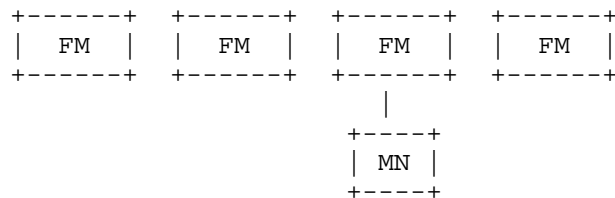


Figure 2. Distributed mobility management.

DMM is distributed in the data plane, whereas the control plane may either be centralized or distributed [I-D.yokota-dmm-scenario]. The former case implicitly assumes separation of data and control planes as described in [I-D.wakikawa-netext-pmip-cp-up-separation]. While mobility management can be distributed, it is not necessary for other functions such as subscription management, subscription database, and network access authentication to be similarly distributed.

A distributed mobility management scheme for a flattening mobile network consisting of access nodes is proposed in [Paper-Distributed.Dynamic.Mobility]. Its benefits over centralized mobility management have been shown through simulations [Paper-Distributed.Centralized.Mobility]. Moreover, the (re)use and extension of existing protocols in the design of both fully distributed mobility management [Paper-Migrating.Home.Agents] [Paper-Distributed.Mobility.SAE] and partially distributed mobility management [Paper-Distributed.Mobility.PMIP] [Paper-Distributed.Mobility.MIP] have been reported in the literature. Therefore, before designing new mobility management protocols for a future distributed architecture, it is recommended to first consider whether existing mobility management protocols can be extended.

4. Problem Statement

The problems that can be addressed with DMM are summarized in the following:

PS1: Non-optimal routes

Forwarding via a centralized anchor often results in non-optimal routes, thereby increasing the end-to-end delay. The problem is manifested, for example, when accessing a nearby server or servers of a Content Delivery Network (CDN), or when receiving locally available IP multicast or sending IP multicast packets. (Existing route optimization is only a host-based solution. On the other hand, localized routing with PMIPv6 [RFC6705] addresses only a part of the problem where both the MN and the correspondent node (CN) are attached to the same MAG, and it is not applicable when the CN does not behave like an MN.)

PS2: Divergence from other evolutionary trends in network architectures such as distribution of content delivery.

Mobile networks have generally been evolving towards a flatter and flatter network. Centralized mobility management, which is non-optimal with a flatter network architecture, does not support this evolution.

PS3: Lack of scalability of centralized tunnel management and mobility context maintenance

Setting up tunnels through a central anchor and maintaining mobility context for each MN usually requires more concentrated resources in a centralized design, thus reducing scalability.

Distributing the tunnel maintenance function and the mobility context maintenance function among different network entities with proper signaling protocol design can avoid increasing the concentrated resources with an increasing number of MNs.

PS4: Single point of failure and attack

Centralized anchoring designs may be more vulnerable to single points of failures and attacks than a distributed system. The impact of a successful attack on a system with centralized mobility management can be far greater as well.

PS5: Unnecessary mobility support to clients that do not need it

IP mobility support is usually provided to all MNs. Yet it is not always required, and not every parameter of mobility context is always used. For example, some applications or nodes do not need a stable IP address during a handover to maintain session continuity. Sometimes, the entire application session runs while the MN does not change the point of attachment. Besides, some sessions, e.g., SIP-based sessions, can handle mobility at the application layer and hence do not need IP mobility support; it is then unnecessary to provide IP mobility support for such sessions.

PS6: Mobility signaling overhead with peer-to-peer communication

Wasting resources when mobility signaling (e.g., maintenance of the tunnel, keep alive signaling, etc.) is not turned off for peer-to-peer communication.

PS7: Deployment with multiple mobility solutions

There are already many variants and extensions of MIP as well mobility solutions at other layers. Deployment of new mobility management solutions can be challenging, and debugging difficult, when they co-exist with solutions already deployed in the field.

PS8: Duplicate multicast traffic

IP multicast distribution over architectures using IP mobility solutions (e.g., [RFC6224]) may lead to convergence of duplicated multicast subscriptions towards the downstream tunnel entity (e.g., MAG in PMIPv6). Concretely, when multicast subscription for individual mobile nodes is coupled with mobility tunnels (e.g., PMIPv6 tunnel), duplicate multicast subscription(s) is prone to be received through

different upstream paths. This problem may also exist or be more severe in a distributed mobility environment.

5. Requirements

After comparing distributed mobility management against centralized deployment in Section 3 and describing the problems in Section 4, this section identifies the following requirements:

REQ1: Distributed mobility management

IP mobility, network access and forwarding solutions provided by DMM MUST enable traffic to avoid traversing single mobility anchor far from the optimal route.

This requirement on distribution is in the data plane only. It does not impose constraints on whether the control plane should be distributed or centralized. However, if the control plane is centralized while the data plane is distributed, it is implicit that the control plane and data plane need to separate (Section 3.2).

Motivation: This requirement is motivated by current trends in network evolution: (a) it is cost- and resource-effective to cache contents, and the caching (e.g., CDN) servers are distributed so that each user in any location can be close to one of the servers; (b) the significantly larger number of mobile nodes and flows call for improved scalability; (c) single points of failure are avoided in a distributed system; (d) threats against centrally deployed anchors, e.g., home agent and local mobility anchor, are mitigated in a distributed system.

This requirement addresses the problems PS1, PS2, PS3, and PS4 described in Section 4.

REQ2: Bypassable network-layer mobility support for each application session

DMM solutions MUST enable network-layer mobility but it MUST be possible for any individual active application session (flow) to not use it. Mobility support is needed, for example, when a mobile host moves and an application cannot cope with a change in the IP address. Mobility support is also needed when a mobile router changes its IP address as it moves together with a host and, in the presence of ingress filtering, an application in the host is interrupted. However

mobility support at the network-layer is not always needed; a mobile node can often be stationary, and mobility support can also be provided at other layers. It is then not always necessary to maintain a stable IP address or prefix for an active application session.

Different active sessions can also differ in whether network-layer mobility support is needed. IP mobility, network access and forwarding solutions provided by DMM **MUST** then enable the possibility of independent handling for each application session of a user or mobile device.

The handling of mobility management to the granularity of an individual session of a user/device **SHOULD** need proper session identification in addition to user/device identification.

Motivation: The motivation of this requirement is to enable more efficient forwarding and more efficient use of network resources by selecting an IP address or prefix according to whether mobility support is needed and by not maintaining context at the mobility anchor when there is no such need.

This requirement addresses the problems PS5 and PS6 described in Section 4.

REQ3: IPv6 deployment

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.

Motivation: This requirement conforms to the general orientation of IETF work. DMM deployment is foreseen in mid- to long-term horizon, when IPv6 is expected to be far more common than today.

This requirement avoids the unnecessarily complexity in solving the problems in Section 4 for IPv4, which will not be able to use some of the IPv6-specific features.

REQ4: Existing mobility protocols

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

Motivation: Reuse of existing IETF work is more efficient and less error-prone.

This requirement attempts to avoid the need of new protocols development and therefore their potential problems of being time-consuming and error-prone.

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

A DMM solution may require loose, tight or no integration into existing mobility protocols and host IP stack. Regardless of the integration level, DMM implementations MUST be able to coexist with existing network deployments, end hosts and routers that may or may not implement existing mobility protocols. Furthermore, a DMM solution SHOULD work across different networks, possibly operated as separate administrative domains, when the needed mobility management signaling, forwarding, and network access are allowed by the trust relationship between them.

Motivation: (a) to preserve backwards compatibility so that existing networks and hosts are not affected and continue to function as usual, and (b) enable inter-domain operation if desired.

This requirement addresses the problem PS7 described in Section 4.

- REQ6: 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. Different management protocols are available. For example:

- (a) SNMP [RFC1157] with definition of standardized management information base MIB objects for DMM, that allows monitoring traffic steering in a consistent manner across different devices,
- (b) NETCONF [RFC6241] with definition of standardized YANG [RFC6020] modules for DMM to achieve a standardized configuration,
- (c) syslog [RFC3164] which is a one-way protocol allowing a device to report significant events to a log analyzer in a network management system.

- (d) IP Flow Information Export (IPFIX) Protocol, which serves as a means for transmitting traffic flow information over the network [RFC7011], with a formal description of IPFIX Information Elements [RFC7012].

It is not the goal of the requirements document to impose which management protocol(s) should be used. An inventory of the management protocols and data models is covered in RFC 6632.

The following lists the operation and management considerations required for a DMM solution; the list may not be exhaustive and may be expanded according to the needs of the solutions:

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

A DMM solution **MUST** support mechanisms to test if the DMM solution is working properly. For example, when a DMM solution employs traffic indirection to support a mobility session, implementations **MUST** support mechanisms to test that the appropriate traffic indirection operations are in place, including the setup of traffic indirection and the subsequent teardown of the indirection to release the associated network resources when the mobility session has closed.

A DMM solution **SHOULD** expose the operational state of DMM to the administrators of the DMM entities. For example, when a DMM solution employs separation between session identifier and forwarding address, it should expose the association between them.

When flow mobility is supported by a DMM solution, the solution **SHOULD** support means to correlate the flow routing policies and the observed forwarding actions.

A DMM solution **SHOULD** support mechanisms to check the liveness of forwarding path. If the DMM solution sends periodic update refresh messages to configure the forwarding path, the refresh period **SHOULD** be configurable and a reasonable default configuration value proposed. Information collected can be logged or made available with protocols such as SNMP [RFC1157], NETCONF [RFC6241], IPFIX [RFC7011], or syslog [RFC3164].

A DMM solution **MUST** provide fault management and monitoring

mechanisms to manage situations where update of the mobility session or the data path fails. The system must also be able to handle situations where a mobility anchor with ongoing mobility sessions fails.

A DMM solution SHOULD be able to monitor usage of DMM protocol. When a DMM solution uses an existing protocol, the techniques already defined for that protocol SHOULD be used to monitor the DMM operation. When these techniques are inadequate, new techniques MUST be developed.

In particular, the DMM solution SHOULD

- (a) be able to monitor the number of mobility sessions per user as well as their average duration.
- (b) provide indication on DMM performance such as
 - 1 the handover delay which includes the time necessary to re-establish the forwarding path when the point of attachment changes,
 - 2 the protocol reactivity which is the time between handover events such as the attachment to a new access point and the completion of the mobility session update.
- (c) provide means to measure the signaling cost of the DMM protocol.
- (d) if tunneling is used for traffic redirection, monitor
 - 1 the number of tunnels,
 - 2 their transmission and reception information,
 - 3 the used encapsulation method and overhead
 - 4 the security used at a node level.

DMM solutions SHOULD support standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules, which SHOULD be created for DMM when needed for such configuration. However, if a DMM solution creates extensions to MIPv6 or PMIPv6, the allowed addition of the definition of management information base (MIB) objects to MIPv6 MIB [RFC4295] or PMIPv6 MIB [RFC6475] needed for the control and monitoring of

the protocol extensions SHOULD be limited to read-only objects.

Motivation: A DMM solution that is designed from the beginning for operability and manageability can avoid difficulty or incompatibility to implement efficient operations and management solutions.

These requirements avoid DMM designs that make operations and management difficult or costly.

REQ7: Security considerations

A DMM solution MUST 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 MUST NOT introduce new security risks, or amplify existing security risks, that cannot be mitigated by existing security protocols and mechanisms.

Motivation: Various attacks such as impersonation, denial of service, man-in-the-middle attacks, and so on, may be launched in a DMM deployment. For instance, an illegitimate node may attempt to access a network providing DMM. Another example is that a malicious node can forge a number of signaling messages thus redirecting traffic from its legitimate path. Consequently, the specific node or nodes to which the traffic is redirected may be under a denial of service attack, whereas other nodes do not receive their traffic. Accordingly, security mechanisms/protocols providing access control, integrity, authentication, authorization, confidentiality, etc. should be used to protect the DMM entities as they are already used to protect against existing networks and existing mobility protocols defined in IETF. Yet if a candidate DMM solution is such that even the proper use of these existing security mechanisms/protocols are unable to provide sufficient security protection, that candidate DMM solution is causing uncontrollable security problems.

This requirement prevents a DMM solution from introducing uncontrollable problems of potentially insecure mobility management protocols which make deployment infeasible because platforms conforming to the protocols are at risk for data loss and numerous other dangers, including financial harm to the users.

REQ8: Multicast considerations

DMM SHOULD enable multicast solutions to be developed to avoid network inefficiency in multicast traffic delivery.

Motivation: Existing multicast deployment have been introduced after completing the design of the reference mobility protocol, often leading to network inefficiency and non-optimal forwarding for the multicast traffic. Instead DMM should consider multicast early so that the multicast solutions can better consider efficiency nature in the multicast traffic delivery (such as duplicate multicast subscriptions towards the downstream tunnel entities). The multicast solutions should then avoid restricting the management of all IP multicast traffic to a single host through a dedicated (tunnel) interface on multicast-capable access routers.

This requirement addresses the problems PS1 and PS8 described in Section 4.

6. Security Considerations

Please refer to the discussion under Security requirement in Section 5.

7. IANA Considerations

None

8. Contributors

This requirements document is a joint effort among numerous participants working in a team. Valuable comments and suggestions in various reviews from the following area directors and IESG members have also contributed to much improvements: Russ Housley, Catherine Meadows, Adrian Farrel, Barry Leiba, Alissa Cooper, Ted Lemon, Brian Haberman, Stephen Farrell, Joel Jaeggli, Alia Atlas, and Benoit Claise. In addition to the authors, each of the following has made very significant and important contributions to the working group draft in this work:

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

Melia Telemaco
Alcatel-Lucent Bell Labs
Email: telemaco.melia@googlemail.com

Elena Demaria
Telecom Italia
via G. Reiss Romoli, 274, TORINO, 10148, Italy
Email: elena.demaria@telecomitalia.it

Jong-Hyouk Lee
Sangmyung University, Korea
Email: jonghyouk@smu.ac.kr

Kostas Pentikousis
EICT GmbH
Email: k.pentikousis@eict.de

Tricci So
ZTE
Email: tso@zteusa.com

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30, Leganes, Madrid 28911, Spain
Email: cjbc@it.uc3m.es

Peter McCann
Huawei Technologies
Email: Peter.McCann@huawei.com

Seok Joo Koh
Kyungpook National University, Korea
Email: sjkoh@knu.ac.kr

Wen Luo
ZTE
No.68, Zijinhua RD,Yuhuatai District, Nanjing, Jiangsu 210012, China
Email: luo.wen@zte.com.cn

Sri Gundavelli
Cisco
sgundave@cisco.com

Hui Deng
China Mobile
Email: denghui@chinamobile.com

Marco Liebsch

NEC Laboratories Europe
Email: liebsch@neclab.eu

Carl Williams
MCSR Labs
Email: carlw@mcsr-labs.org

Seil Jeon
Instituto de Telecomunicacoes, Aveiro
Email: seiljeon@av.it.pt

Sergio Figueiredo
Universidade de Aveiro
Email: sfigueiredo@av.it.pt

Stig Venaas
Email: stig@venaas.com

Luis Miguel Contreras Murillo
Telefonica I+D
Email: lmcm@tid.es

Juan Carlos Zuniga
InterDigital
Email: JuanCarlos.Zuniga@InterDigital.com

Alexandru Petrescu
Email: alexandru.petrescu@gmail.com

Georgios Karagiannis
University of Twente
Email: g.karagiannis@utwente.nl

Julien Laganier
Juniper
Email: julien.ietf@gmail.com

Wassim Michel Haddad
Ericsson
Email: Wassim.Haddad@ericsson.com

Dirk von Hugo
Deutsche Telekom Laboratories
Email: Dirk.von-Hugo@telekom.de

Ahmad Muhanna
Award Solutions
Email: asmuhanna@yahoo.com

Byoung-Jo Kim
ATT Labs
Email: macsbug@research.att.com

Hassan Ali-Ahmad
Orange
Email: hassan.aliahmad@orange.com

Alper Yegin
Samsung
Email: alper.yegin@partner.samsung.com

David Harrington
Effective Software
Email: ietfdbh@comcast.net

9. References

9.1. Normative References

- [RFC1157] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol (SNMP)", STD 15, RFC 1157, May 1990.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3164] Lonvick, C., "The BSD Syslog Protocol", RFC 3164, August 2001.
- [RFC3753] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.
- [RFC4295] Keeni, G., Koide, K., Nagami, K., and S. Gundavelli, "Mobile IPv6 Management Information Base", RFC 4295, April 2006.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC6020] Bjorklund, M., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, October 2010.
- [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.
- [RFC6475] Keeni, G., Koide, K., Gundavelli, S., and R. Wakikawa, "Proxy Mobile IPv6 Management Information Base", RFC 6475, May 2012.
- [RFC6632] Ersue, M. and B. Claise, "An Overview of the IETF Network Management Standards", RFC 6632, June 2012.
- [RFC7011] Claise, B., Trammell, B., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, September 2013.
- [RFC7012] Claise, B. and B. Trammell, "Information Model for IP Flow Information Export (IPFIX)", RFC 7012, September 2013.

9.2. Informative References

- [I-D.bhandari-dhc-class-based-prefix]
Bhandari, S., 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.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.
- [I-D.wakikawa-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-wakikawa-netext-pmip-cp-up-separation-03 (work in progress), April 2014.
- [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.
- [Paper-Distributed.Centralized.Mobility]
Bertin, P., Bonjour, S., and J-M. Bonnin, "A 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.MIP]

Chan, H., "Distributed Mobility Management with Mobile IP", Proceedings of IEEE International Communication Conference (ICC) 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", Journal of Communications, vol. 6, no. 1, pp. 4-15, February 2011.

[Paper-Distributed.Mobility.SAE]

Fisher, M., Anderson, F., Kopsel, A., Schafer, G., and M. Schlager, "A Distributed IP Mobility Approach for 3G SAE", Proceedings of the 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2008.

[Paper-Locating.User]

Kirby, G., "Locating the User", Communication International, 1995.

[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-Mobile.Data.Offloading]

Lee, K., Lee, J., Yi, Y., Rhee, I., and S. Chong, "Mobile Data Offloading: How Much Can WiFi Deliver?", SIGCOMM 2010, 2010.

- [RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.
- [RFC5944] Perkins, C., "IP Mobility Support for IPv4, Revised", RFC 5944, November 2010.
- [RFC6224] Schmidt, T., Waehlich, M., and S. Krishnan, "Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains", RFC 6224, April 2011.
- [RFC6301] Zhu, Z., Wakikawa, R., and L. Zhang, "A Survey of Mobility Support in the Internet", RFC 6301, July 2011.
- [RFC6705] Krishnan, S., Koodli, R., Loureiro, P., Wu, Q., and A. Dutta, "Localized Routing for Proxy Mobile IPv6", RFC 6705, September 2012.
- [RFC6909] Gundavelli, S., Zhou, X., Korhonen, J., Feige, G., and R. Koodli, "IPv4 Traffic Offload Selector Option for Proxy Mobile IPv6", RFC 6909, April 2013.
- [TS.23.401] 3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", 3GPP TR 23.401 10.10.0, March 2013.
- [TS.29303] 3GPP, "Domain Name System Procedures; Stage 3", 3GPP TR 23.303 11.2.0, September 2012.

Authors' Addresses

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

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

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

Hidetoshi Yokota
KDDI Lab
2-1-15 Ohara, Fujimino, Saitama, 356-8502 Japan
Email: yokota@kddilabs.jp

Jouni Korhonen
Broadcom Communications
Porkkalankatu 24, FIN-00180 Helsinki, Finland
Email: jouni.nospam@gmail.com

Distributed Mobility Management (DMM)
Internet-Draft
Updates: 4862 (if approved)
Intended status: Standards Track
Expires: August 28, 2016

J. Korhonen
Broadcom
S. Gundavelli
Cisco
P. Seite
Orange
D. Liu
Alibaba
February 25, 2016

IPv6 Prefix Properties
draft-korhonen-dmm-prefix-properties-05.txt

Abstract

This specification defines an extension to the IPv6 stateless address autoconfiguration procedure. New options with meta data are defined that describe the properties and other prefix class meta data associated with the prefix. The stateless address autoconfiguration procedure and end hosts can make use of the additional properties and class information when selecting source address prefixes for a particular uses and use cases. This specification updates RFC4862.

Requirements Language

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 RFC 2119 [RFC2119].

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 August 28, 2016.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Background and Motivation	3
3. Option Formats	4
3.1. Prefix Meta Data	5
3.2. Meta Data Suboptions	6
4. Host Considerations	7
4.1. Stateless Address Autoconfiguration Enhancements	7
4.2. Internal Data Structures	8
4.3. Default Address Selection	8
5. Router Considerations	8
6. Multiple Provisioning Domain Considerations	9
7. Security Considerations	9
8. IANA Considerations	10
9. Acknowledgements	10
10. References	10
10.1. Normative References	10
10.2. Informational References	11
Authors' Addresses	12

1. Introduction

This specification defines a new neighbor discovery protocol message option, the Prefix Information Option with Meta Data (PIOMD), that indicate, for example, the mobility management properties associated to the prefix, and a class value that conveys metadata associated to the prefix with a local administrative domain wide importance. The solution may use of Multiple Provisioning Domains (MPVD) framework [RFC7556] [I-D.ietf-mif-mpvd-ndp-support]. Furthermore, the specification discusses corresponding source address selection hint issues with the IPv6 Socket API and applications in general [I-D.ietf-dmm-ondemand-mobility].

For example, the IPv6 Socket API for Source Address Selection [RFC5014] already covers Mobile IPv6 [RFC6275] and allows selecting between a home address (HoA) and a care-of address (CoA). A mobile node (MN) with a client based mobility IP stack is supposed to know which prefixes are CoA(s) and/or HoA(s). However, this is not the case with network based mobility management where the MN is expected to be agnostic of the mobility support.

The extensions are minimal in a sense that they do not define new functionality, for example, to any existing mobility protocol but instead add an explicit indication of network based mobility knowledge into the IPv6 stateless address autoconfiguration (SLAAC) [RFC4862]. The heavy lifting is mostly on the applications side and on the IP stack providing interface for applications, since they need to make use of the new functionality. The new functionality is achieved by defining a new, backward compatible, IPv6 neighbor discovery protocol options that convey the required prefix related meta data information the SLAAC procedure may take use of.

This would allow for network based mobility solutions, such as Proxy Mobile IPv6 [RFC5213] or GTP [TS.29274] to explicitly indicate that their prefixes have mobility, and therefore, the MN IP stack or specifically applications can make an educated selection between prefixes that have mobility and those that do not. There is also a potential need to extend both [RFC3493] and [RFC5014] in order to provide required hooks into socket APIs.

The underlying assumption is that a MN has multiple prefixes to choose from. Typically this means either the MN has multiple interfaces or an interface has been configured with multiple prefixes. This specification does not make a distinction between these alternatives and does not either make any assumptions how the possible transfer of a prefix is done between interfaces in the case a network based mobility solution is used.

2. Background and Motivation

This section discusses the motivations behind adding metadata and other address selection decision making affecting information into IPv6 prefixes. The additional information is conveyed from the network to a end host during the IPv6 address configuration phase. The motivation example taken from and discussed below is from the mobile networks.

IP mobility and its centralized topological anchoring of IP addresses has known issues. For instance, non-optimal routing is a classical example. Another concerns include excessive tunneling, increased signaling due the maintenance of mobility related bindings,

aggregation of traffic to centralized mobility anchor gateways and unnecessary IP mobility related state management for IP traffic that does not as such benefit from mobility. In general, it is observed that most applications do not need IP level mobility, and work just fine with "temporary" IP addresses that come and go. However, IP mobility still has its virtues making the applications unaware of mobility, and certain wireless mobile networking architecture make extensive use of network based IP mobility.

In order to overcome some of the above issues, use of local resources and topologically local addressing could be enhanced. In many cases this would lead to use of multiple addresses of which some provide mobility and some do not. However, an end host has to have means to distinguish between addresses that provide mobility, and those that are short lived and usable only within a limited topological area.

[RFC7333] discussed the requirements for distributed mobility management and [RFC7429] describes the gaps from current best practices and the desired approaches for de-centralized mobility management. One approach is using the dynamic anchoring for distributed de-centralized mobility management. The idea is to use the local allocated prefix for any newly initiated 'IP session' and use the previously allocated prefix for the ongoing sessions. This specification can be used to implement the prefix selection for dynamic anchoring. For example, both the locally allocated and the remotely allocated/anchored prefixes can be identified by the prefix property option as described in Section 3.2.

The solution described in this document also shares similar motivations for classifying the prefix as described in [I-D.bhandari-dhc-class-based-prefix]. Some service providers may wish to allocate specific prefixes for some services or type of traffic. In this situation, the end host must be able to classify prefixes according to type of service.

This specification provides tools for extending the IPv6 address management and source address selection so that end hosts (and their applications) can select a proper address for their needs. This specification complements [I-D.bhandari-dhc-class-based-prefix] by providing the SLAAC version of the additional prefix related meta data information delivery compared to the DHCPv6 stateful approach.

3. Option Formats

3.1. Prefix Meta Data

This specification defines a new neighbor discovery protocol message option, the Prefix Information Option with Meta Data (PIOMD), to be used in router advertisement messages. The PIOMD is treated as the same as [RFC4861] Prefix Information Option (PIO) except with an addition of new meta data suboptions.

The PIOMD can coexist with RFC4861 PIO. The prefixes advertised in both PIOMD and PIO can even be the same. It is up to the receiving end host to select the appropriate prefix(es) for configuring its IPv6 addresses. In a case the PIO and the PIOMD share the same prefix, then all the other parameter (like flags and lifetimes) MUST be the same.

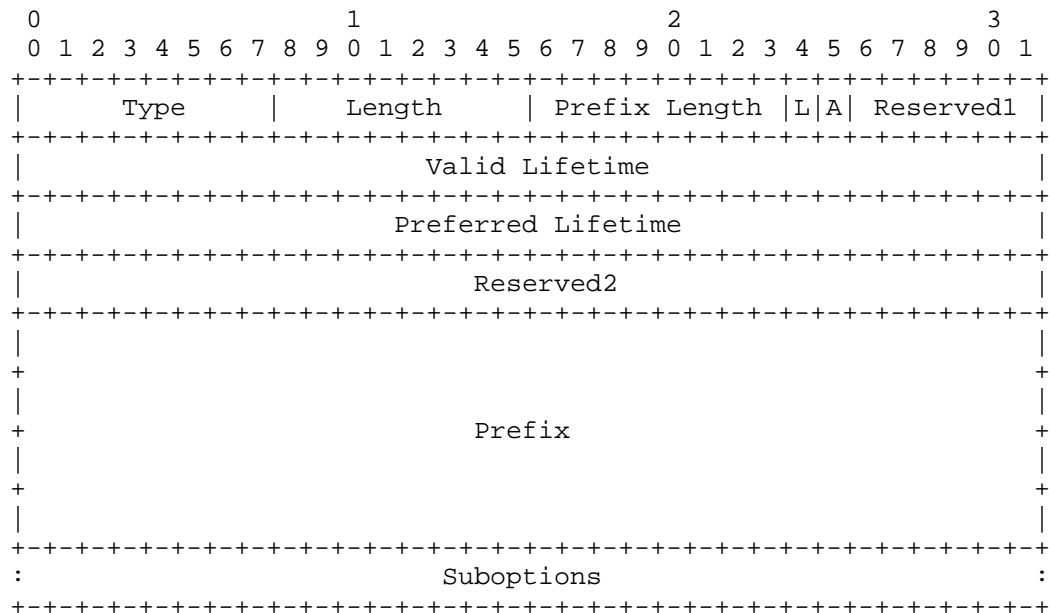


Figure 1: Prefix Information Option with additional meta data

Type

Set to TBD1.

Length

4 if no suboptions are present. Greater than 4 if one or more suboptions are present.

Suboptions

Zero or more suboptions that describe properties and other meta data attached to the advertised prefix. See Section 3.2 for description of the meta data suboption format and suboptions already defined in this specification. The existence of suboptions can be determined from the length field. If the length is greater than 4, then at least one suboption MUST be present.

Rest of the fields are handled exactly as described in Section 4.6.2. of RFC4861 [RFC4861].

3.2. Meta Data Suboptions

The generic suboption format for the PIO with meta data (PIOMD) is shown in Figure 2. The suboption follows the alignment and length rules familiar from [RFC4861]. On a particular note, the flag 'C' describes whether the suboption is mandatory to understand by the receiver or not. If 'C' is set to zero (0), the receiver can silently discard an unknown suboption and skip to the next suboption. If 'C' is set to one (1), then an unknown suboption causes the receiver to silently discard the entire PIOMT and no further suboptions need to be parsed. There can be multiple instances of the same suboption type in one PIOMD option.

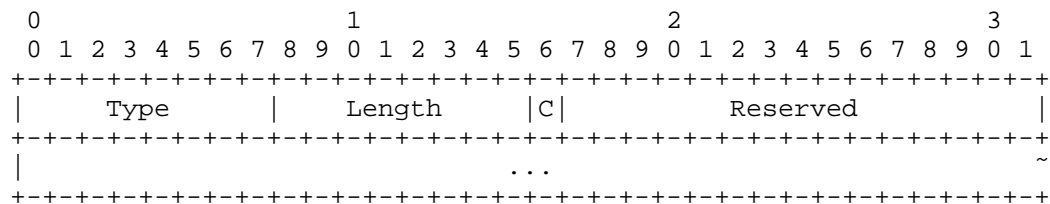


Figure 2: Generic meta data suboption format

Figure 3 shows the Prefix Properties suboption. The prefix properties values are defined in Section 6.1. of [I-D.bhandari-dhc-class-based-prefix]. When an end host receives a router advertisement message with a PIOMD and the prefix properties suboption, it can use the suboption information as an additional hint for selecting the prefix for a desired purpose and use case. The prefix properties have global meaning i.e., they have the same treatment and handling cross administrative domains. The value for the 'C' flag SHOULD be one (1). This also implies that if the prefix properties bit vector has a flag bit set, which the receiving end host does not understand and the 'C' flag is also set, then the whole PIOMD option MUST be discarded.

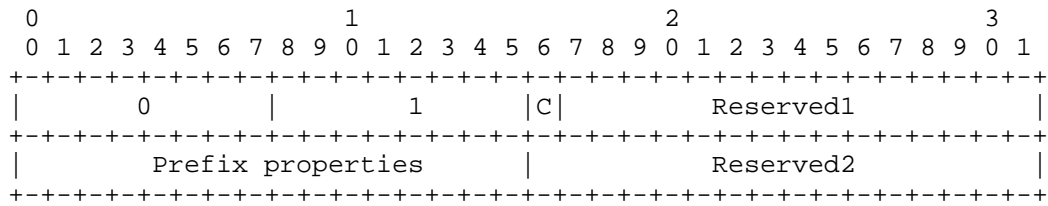


Figure 3: Prefix Properties suboption

Figure 4 shows the Prefix Class suboption. The prefix class values and usage follow what has been defined in Section 2.3. of [I-D.bhandari-dhc-class-based-prefix]. When an end host receives a router advertisement message with a PIOMD and the prefix class suboption, it can use the suboption information as an additional hint for selecting the prefix for a desired purpose and use case. The prefix class has only local administrative meaning i.e., they are local to the access network and may overlap both semantically and registry wise across different administrative domains. How the boundaries of an administrative domain are determined is outside the scope of this specification. The value for the 'C' flag SHOULD be zero (0).

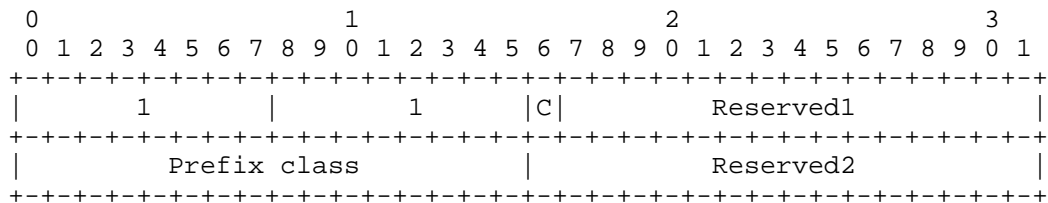


Figure 4: Prefix Class suboption

Future specifications MAY define new suboptions. One potential example could be a suboption to identify the provisioning domain where the configuration information originates.

4. Host Considerations

4.1. Stateless Address Autoconfiguration Enhancements

This specification extends to the [RFC4862] Stateless Address Autoconfiguration (SLAAC). As described in Section 3.1, a new [RFC4861] PIO like option PIOMD can be used to either complement or entirely replace the PIO in a router advertisement. An end host that understands the PIOMD option MUST always prefer a prefix found in the PIOMD over the same prefix found in the PIO option.

4.2. Internal Data Structures

The host internal data structures need to be extended with the 'prefix property' and the 'prefix class' information associated to the learned prefix and configured addresses. How this is accomplished is host implementation specific. It is also a host implementation issue how an application can learn or query both properties or class of an address or a prefix. One possibility is to provide such information through the socket API extensions (see discussion in [I-D.ietf-dmm-ondemand-mobility]). Other possibilities include the use of e.g., `ioctl()` or NetLink [RFC3549] extensions.

4.3. Default Address Selection

The 'prefix property' is only used as a hint. It does not affect the existing [RFC6724] automatically. A specific rule to host's policy table has to be inserted by an application or some daemon process. Alternatively, an application can express its address mobility property preferences through the socket API extensions (see discussion in [I-D.ietf-dmm-ondemand-mobility]), which means the socket library or middleware has to modify [RFC6724] policy table or algorithm.

The 'prefix properties' flags MAY define the prefix preference for an IP stack that understands the extensions defined in this specification. The IP stack SHOULD use the properties preferences to supersede [RFC6724] Source Address Selection Rule 8 when selecting a default source address among multiple choices and an application has not explicitly indicate what kind of source address it prefers.

The 'prefix class' defines an application 'class' the advertised prefix is intended to be used for. The class has only local administrative domain significance. The 'prefix class' can be used, for example, to identify prefixes that are meant to be used reach a voice over IP (VoIP) service or a video streaming application within the local administrative network. A specific application in the end host MAY use this additional class information when enumerating through multiple available addresses and then select a specific address to be used for its purposes.

5. Router Considerations

A network administrator MAY configure routers complying to this specification also send router advertisements with the PIOMD option into every router advertisement that also contains the [RFC4861] PIO option. Since the PIOMD sending router has no prior knowledge whether the end hosts on the link support the PIOMD option, it is strongly RECOMMENDED that both [RFC4861] PIO and the PIOMD are always

included in the router advertisement, even if the advertised prefixes were the same. Alternatively (or in addition) multiple provisioning domains [I-D.ietf-mif-mpvd-ndp-support] can be used to separate prefixes advertised using PIOMD options. See Section 6 for further details.

A router can also make use of the 'C' flag handling in the PIOMD suboptions when introducing new functionality into the network. Since it is possible to include multiple suboptions of the same type into the PIOMD option, the router can easily make a difference between e.g., prefix properties that must be understood by the receiver and those that can safely be ignored.

6. Multiple Provisioning Domain Considerations

Multiple Provisioning Domains (MPVD) framework [RFC7556] allows grouping network configuration information under an explicitly named provisioning domain [I-D.ietf-mif-mpvd-id]. This would allow network operators to place mobility related configuration information (including prefixes) under a specific explicit provisioning domain and non-mobile configuration information into other explicit domain or implicit provisioning domain.

MPVDs are the RECOMMENDED way to deliver PIOMD options. This allows mobile network operators selectively advertise mobility related network configurations. MPVDs also provide adequate security features for mobile hosts to verify the authenticity of the configuration information.

7. Security Considerations

Existing Prefix Information Option related security considerations apply as described in [RFC4861] and [RFC4191]. A malicious node on the shared link could include stale metadata in a PIOMD causing the host to learn wrong information regarding the prefix and thus make misguided selection of prefixes on the link. Similarly a malicious middleman on the link could modify or remove metadata in the PIOMD causing misguided selection of prefixes. In order to avoid on-link attacks, SeND [RFC3971] can be used to reject Router Advertisements from potentially malicious nodes and guarantee integrity protection of the Router Advertisements.

If MPVD support for NDP [I-D.ietf-mif-mpvd-ndp-support] is used, then the mobile host can use its security features to verify the authenticity and correctness of the received PIOMD information.

8. IANA Considerations

Section 3.1 defines a new IPv6 Neighbor Discovery protocol option type TBD1 for the Prefix Information Option with Meta Data. The type value is defined in the existing 'IPv6 Neighbor Discovery Option Formats' IANA registry.

Section 3.2 defines a new IANA registry for the Prefix Information Option with Meta Data suboptions. The registry allocation policy is Standards Action [RFC5226]. The initial allocations for the prefix properties and prefix class suboptions are listed in Section 3.2.

9. Acknowledgements

The authors thank Ole Troan for his feedback and suggestions on this document (the Classed PIO).

10. References

10.1. Normative References

- [I-D.ietf-mif-mpvd-id]
Krishnan, S., Korhonen, J., Bhandari, S., and S. Gundavelli, "Identification of provisioning domains", draft-ietf-mif-mpvd-id-02 (work in progress), October 2015.
- [I-D.ietf-mif-mpvd-ndp-support]
Korhonen, J., Krishnan, S., and S. Gundavelli, "Support for multiple provisioning domains in IPv6 Neighbor Discovery Protocol", draft-ietf-mif-mpvd-ndp-support-02 (work in progress), October 2015.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <<http://www.rfc-editor.org/info/rfc4861>>.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <<http://www.rfc-editor.org/info/rfc4862>>.

- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <<http://www.rfc-editor.org/info/rfc5226>>.
- [RFC6724] Thaler, D., Ed., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, DOI 10.17487/RFC6724, September 2012, <<http://www.rfc-editor.org/info/rfc6724>>.

10.2. Informational References

- [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.ietf-dmm-ondemand-mobility]
Yegin, A., Kweon, K., Lee, J., Park, J., and D. Moses, "On Demand Mobility Management", draft-ietf-dmm-ondemand-mobility-02 (work in progress), February 2016.
- [RFC3493] Gilligan, R., Thomson, S., Bound, J., McCann, J., and W. Stevens, "Basic Socket Interface Extensions for IPv6", RFC 3493, DOI 10.17487/RFC3493, February 2003, <<http://www.rfc-editor.org/info/rfc3493>>.
- [RFC3549] Salim, J., Khosravi, H., Kleen, A., and A. Kuznetsov, "Linux Netlink as an IP Services Protocol", RFC 3549, DOI 10.17487/RFC3549, July 2003, <<http://www.rfc-editor.org/info/rfc3549>>.
- [RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <<http://www.rfc-editor.org/info/rfc3971>>.
- [RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191, November 2005, <<http://www.rfc-editor.org/info/rfc4191>>.
- [RFC5014] Nordmark, E., Chakrabarti, S., and J. Laganier, "IPv6 Socket API for Source Address Selection", RFC 5014, DOI 10.17487/RFC5014, September 2007, <<http://www.rfc-editor.org/info/rfc5014>>.

- [RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, DOI 10.17487/RFC5213, August 2008, <<http://www.rfc-editor.org/info/rfc5213>>.
- [RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <<http://www.rfc-editor.org/info/rfc6275>>.
- [RFC7333] Chan, H., Ed., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", RFC 7333, DOI 10.17487/RFC7333, August 2014, <<http://www.rfc-editor.org/info/rfc7333>>.
- [RFC7429] Liu, D., Ed., Zuniga, JC., Ed., Seite, P., Chan, H., and CJ. Bernardos, "Distributed Mobility Management: Current Practices and Gap Analysis", RFC 7429, DOI 10.17487/RFC7429, January 2015, <<http://www.rfc-editor.org/info/rfc7429>>.
- [RFC7556] Anipko, D., Ed., "Multiple Provisioning Domain Architecture", RFC 7556, DOI 10.17487/RFC7556, June 2015, <<http://www.rfc-editor.org/info/rfc7556>>.
- [TS.29274] 3GPP, "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)", 3GPP TS 29.060 8.11.0, December 2010.

Authors' Addresses

Jouni Korhonen
Broadcom
3151 Zanker Rd.
CA San Jose
USA

Email: jouni.nospam@gmail.com

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: sgundave@cisco.com

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

Email: pierrick.seite@orange.com

Dapeng Liu
Alibaba

Email: max.ldap@alibaba-inc.com

DMM Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 18, 2014

M. Liebsch
NEC
P. Seite
Orange-France Telecom
G. Karagiannis
University of Twente
S. Gundavelli
Cisco
February 14, 2014

Distributed Mobility Management - Framework & Analysis
draft-liebsch-dmm-framework-analysis-03.txt

Abstract

Mobile operators consider the distribution of mobility anchors to enable offloading some traffic from their core network. The Distributed Mobility Management (DMM) Working Group is investigating the impact of decentralized mobility management to existing protocol solutions, while taking into account well defined requirements, which are to be met by a future solution. This document discusses DMM using a functional framework. Functional Entities to support DMM as well as reference points between these Functional Entities are introduced and described. The described functional framework allows distribution and co-location of Functional Entities and build a DMM architecture that matches the architecture of available protocols. Such methodology eases the analysis of best current practices with regard to functional and protocol gaps.

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 August 18, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	3
2. Conventions and Terminology	5
3. Functional Architecture for DMM Support	6
4. Different Constellations of Functional Entities	11
4.1. Condensed Deployment: Mobility Protocol Centric Solutions	11
4.2. Cooperative Deployment: Distributed Architecture	12
5. Security Considerations	14
6. IANA Considerations	15
7. References	16
7.1. Normative References	16
7.2. Informative References	16
Appendix A. How the framework can support a gap analysis! Some examples.. . . .	17
A.1. Condensed Deployment using Mobile IPv6	17
A.2. Condensed Deployment using Proxy Mobile IPv6	17
A.3. Cooperative Deployment using LISP	17
A.4. Cooperative Deployment using iBGP	18
Appendix B. Functional Architecture for Multicast DMM Support . .	21
Appendix C. Change Notes	25
Authors' Addresses	26

1. Introduction

The concept of Distributed Mobility Management (DMM) is based on the distribution of mobility anchors towards the access networks to provide mobile nodes with local anchors and enable optimized routing of traffic above anchor level to any kind of serving point, e.g. distributed content caches. The closer mobility anchors are located to mobile nodes, the more a mobile node's handover may necessitate the assignment of a new mobility anchor. Continuity of a mobile node's IP address or IP address prefix enables IP session continuity, but creates the problem of routing downlink packets to the mobile node's current mobility anchor. Different solutions and associated extensions to IP mobility management protocols are being discussed to maintain a mobile node's IP session after mobility anchor relocation, including solutions that are based on existing protocols.

This document defines a functional framework for DMM and describes an initial set of well defined functional entities (FE), which are required to support IP address continuity in a network with distributed mobility anchors. Having identified the function of each FE as well as required interfaces between FEs allows different constellations of FEs, either by co-locating or distributing them. Functional frameworks have been successfully used within and outside of the IETF, such as the ITU-T [ITU-TY2018][ITU-TY2804], to support the thorough analysis of protocols gaps with existing protocols and to enable the design of suitable solutions. Due to the complexity of the DMM problem and solutions space, we consider such framework of particular importance for performing a Gap Analysis while assigning the defined FEs to architecture components of existing protocols and to build suitable solutions for DMM based on extensions to a single or multiple existing protocols and architecture components.

This version of the draft introduces a basic set of FEs and interfaces between these FEs to support IP address continuity in DMM, without being specific to the used mobility management protocol, which operates below the mobility anchor. The functional framework as per this draft is protocol agnostic, such that it can apply to (1) solutions that are solely based on existing IP mobility protocols and to (2) solutions which get support from non-mobility protocols.

The framework enables the analysis of existing protocols' suitability to support DMM and allows building optimized solutions for DMM without being limited to the mobility protocol suites. In particular, the framework can be used to build solutions on the following challenges that are currently being discussed in the context of DMM rechartering:

- o Support of different deployment models, where the mobility anchors can be located in the access networks or in the core/backbone network
- o Anchor selection mechanisms
- o Control- and Data-plane separation techniques for mobility components
- o Enhancements to mobile node for operating in a DMM-enabled network
- o Policy extensions for supporting DMM
- o Optimized traffic steering approaches for DMM used to ensure IP address continuity
- o Exposing mobility states (incl. binding state, access network parameters, etc.) to inter-work, for example, with SDN technology

Some examples how the framework can support the identification of required protocol extensions to existing mobility management protocol or alternatively the support from non-mobility protocols to design suitable DMM solutions on system level are described in Appendix A.

Appendix B defines an additional set of functional entities, which enables multicast support in DMM and can complement the framework for DMM unicast support.

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Functional Architecture for DMM Support

The framework introduces four additional functional entities (FE) which are relevant complement existing mobility- and transport networks to enable DMM support for unicast traffic and to meet essential DMM requirements as per [I-D.ietf-dmm-requirements], such as enabling temporary IP address continuity after a mobile node got assigned a new mobility anchor. Further FEs may be needed to enable advanced features, such as simultaneous use of an imported mobile node HoA or HNP to maintain ongoing data sessions and a new HoA or HNP, which is allocated by the mobile node's new mobility anchor after handover. Additional FEs are not considered in this revision of the draft, but can be introduced easily in future versions of the draft and considered for the BCP discussion and gap analysis.

The following FEs are currently considered as existing functional entities to build the mobility- and transport network:

- o FE_R: Functional Entity of a standard IP Router / Switch
- o FE_MA_C: Functional Entity Mobility Anchor, Control Plane
- o FE_MA_U: Functional Entity Mobility Anchor, User Plane
- o FE_MU_C: Functional Entity Mobile User Client, Control Plane
- o FE_MU_U: Functional Entity Mobile User Client, User Plane

The list comprises a generic router/switch function FE_R that's supposed to build the transport network. It has no particular function that's specific to DMM, but performs routing according to a longest prefix match. Deployment specific aspects, such as the use of IP/MPLS, are not (yet) considered in this draft.

The entities FE_MA_C and FE_MA_U represent the unmodified functions of the mobility architecture's mobility anchor. In Mobile IPv6, these function would be co-located with the Home Agent, in Proxy Mobile IPv6, these functions would be co-located with the Local Mobility Anchor (LMA). In a cellular IP (CIP) enabled domain, these functions would be co-located with the domain's CIP Gateway.

The entities FE_MU_C and FE_MU_U represent the existing user client functions, that send location updates to the mobility anchor. In Mobile IPv6, these functions are co-located with the Mobile Node, whereas in Proxy Mobile IPv6, these functions are co-located with the Mobile Access Gateway.

So far, this draft defines four DMM-specific FEs, which can be either

distributed or co-located with existing FEs of the mobility- or routing plane. One or more of the following FEs are currently assumed to add to an existing mobility- and transport network to enable DMM support for IP address continuity:

- o FE_MCTX: Functional Entity Mobility Context Transfer
- o FE_I: Functional Entity Ingress to DMM plane
- o FE_E: Functional Entity Egress of DMM plane
- o FE_IEC: Functional Entity for Ingress/Egress Control

Note: No all FEs or reference points between FEs may be relevant for a DMM-enabled solution that is based on existing protocols and the associated architecture. Which functions are relevant to complement an existing protocol and architecture depends on the identified gaps.

The task of the FE_MCTX is to export relevant binding cache information, such as the mobile node's HoA or HNP, from the mobile node's previous mobility anchor (pMA) during mobility anchor relocation to enable IP address continuity after mobility anchor relocation. Furthermore, the function allows importing mobility context on the mobile node's new mobility anchor. Imported HoA/HNP of a mobile node will be treated as identifier and non-routable IP address (prefix), as it probably does not match the new mobility anchor's location in the topology. Furthermore, the FE_MCTX can provide mobility context to the FE_IEC to allow keeping these policies updated, which allow forwarding of packets to the MN's currently used mobility anchor.

The function FE_I enables the ingress level of indirection by means of deviating from the standard routing path of the mobile node's downlink packets, which carry the mobile node's HoA/HNP in the destination IP address field of their IP header. The FE_I can retrieve information from a control function (FE_IEC) to establish forwarding of the mobile node's packets to the appropriate DMM egress function (FE_E). Forwarding can be for example accomplished by an IP tunnel to the egress function, address translation to a routable IP address or other means.

The function FE_E receives downlink packets being forwarded by the DMM ingress function FE_I, e.g. by terminating a forwarding tunnel. The state on the FE_I can be established through the DMM ingress/egress control function (FE_IEC) and is used to identify an MN's received packets and deliver them to the MN's current mobility anchor (FE_MA). If the FE_E is co-located with the FE_MA, the delivery is a local operation. If the FE_E is not co-located with the FE_MA, other

techniques, such as host-routes or technology such as OpenFlow may be used to deliver the packets to the mobile node's current mobility anchor. If not co-located with the FE_MA, the FE_E is supposed to be located close to the mobile node's current FE_MA.

The function FE_IEC represents a control function, that establishes, updates and removes policies (per-host or grouped) in the FE_I and the FE_E to allow forwarding of a mobile node's downlink packets towards the mobile node's current mobility anchor.

The mobile node's IP address (prefix) is carried in the source address field of the uplink packet. This source address is thus topologically incorrect after mobile node's handover. When IP routers of the mobility domain do not apply filtering according to the source addresses, uplink packets can be assumed to be routable and no specific operation is required.

If source address filtering is used, relevant routers need to be reconfigured to exclude the mobile node's IP address from filtering rules. If such filtering is performed by a mobility anchor or a Proxy Mobile IPv6 Mobile Access Gateway (MAG), local mobility functions on these routers should perform the task to reconfigure the local filter rules for uplink traffic.

When traffic indirection also applies to the uplink, e.g. to enable bidirectional tunneling to ensure that downlink and uplink data packets always traverse the same ingress/egress functions, FE_E and FE_I functions come into play on the uplink path. Downlink FE_I and FE_E become respectively FE_E and FE_I on the uplink. The uplink FE_I forwards a mobile node's packets to the FE_E corresponding to the downlink FE_I that has sent packets with the mobile node's address in the destination address field. The FE_I can also retrieve the information from the FE_IEC.

Figure 1 illustrates how the four DMM-specific FEs complement existing FEs of the mobility architecture. These DMM-specific FEs and associated operation on the interfaces between them can be realized by existing protocols, extensions to them or new protocols. Figure 1 separates the data plane from the control plane.

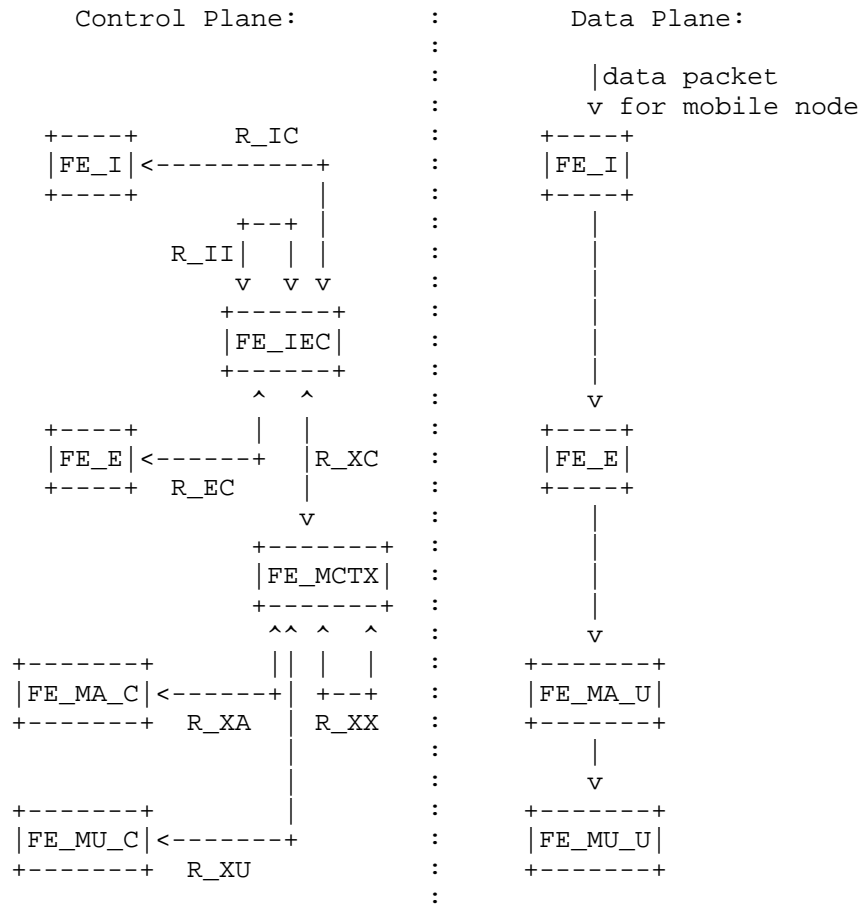


Figure 1: Basic set of functional entities (FE) and interfaces to enable IP-address continuity in DMM

The reference points between FEs comprise the following features:

- o R_XA: Enables the FE_MCTX to retrieve mobility context information from the FE_MA of the MN's mobility anchor. Such information includes for example the MN's Home Address (HoA) or Home Network Prefix (HNP). In the network of the MN's new mobility anchor, the reference point enables the FE_MCTX to provide the MN's mobility context to the associated FE_MA, that imports the MN's mobility context to enable IP address continuity.
- o R_XU: Enables the FE_MCTX to retrieve mobility context information from the mobile user client control function, the FE_MU_C. In host

mobility management, this function is located on the Mobile Node, who could support DMM operation by notifying the FE_MCTX through this reference point.

- o R_XX: Enables the direct transfer of an MN's mobility context between two functions FE_MCTX, which are typically located in the network of the MN's previous and new mobility anchor respectively.
- o R_IC: Enables the FE_IEC to provide policies to the FE_I, which are used to forward the MN's downlink packets towards the MN's new mobility anchor and the associated FE_E. These policies can be provided to the FE_I in an unsolicited manner or on request by the FE_I.
- o R_EC: Enables the FE_IEC to provide policies to the FE_E, which are used at the FE_E to identify received packets that belong to a particular MN and deliver these packets to the MN's new mobility anchor. Such policies could include, for example, tunnel endpoint information, flow identification rules or other identification and addressing rules.
- o R_XC: Enables initialization and update of the FE_IEC about the MN's mobility context as well as about its current location as represented by the FE_E in the network of the MN's current mobility anchor.
- o R_II: Multiple instances of an FE_IEC can be deployed to build a DMM architecture, e.g. to distribute load and scale better, or distribute tasks associated with the FE_IEC to enable cooperative solutions.

4. Different Constellations of Functional Entities

The defined FEs can be grouped or distributed to build a DMM architecture that considers new architecture components or that is based on components of existing protocols. As a starting point, this section depicts and describes two deployment variants, which reflect the current understanding of the WG how DMM could be accomplished using existing protocol specifications as base. Variants of these two deployment models or entirely new models are possible and can be added to future versions of this document.

Note: This section is incomplete and needs further input on different deployment models and variants.

4.1. Condensed Deployment: Mobility Protocol Centric Solutions

Mobility protocol centric solutions aim at extensions to available mobility protocols to enable DMM, without being dependent on any external, non-mobility component and protocol. IP address continuity is typically established on the control plane by extensions to the mobility protocol to convey an MN's mobility context to a new mobility anchor, and on the data plane by the establishment of a forwarding tunnel between mobility anchors to deliver downlink packets from the originally assigned mobility anchor to the MN's currently used mobility anchor after anchor relocation. Alternatively, IP address continuity is enabled by using multiple mobility anchors simultaneously, whereas the mobile node's IP address(es) remain anchored at the topologically correct anchor point. These approaches differ in the level of extensions to the mobility protocols and in the support of certain features on the mobile node, such as the simultaneous use of multiple mobility anchors and associated Home Addresses. They have in common the sub-optimal routing path, as the mobile node's downlink traffic needs to traverse the location of the IP addresses topologically correct mobility anchor.

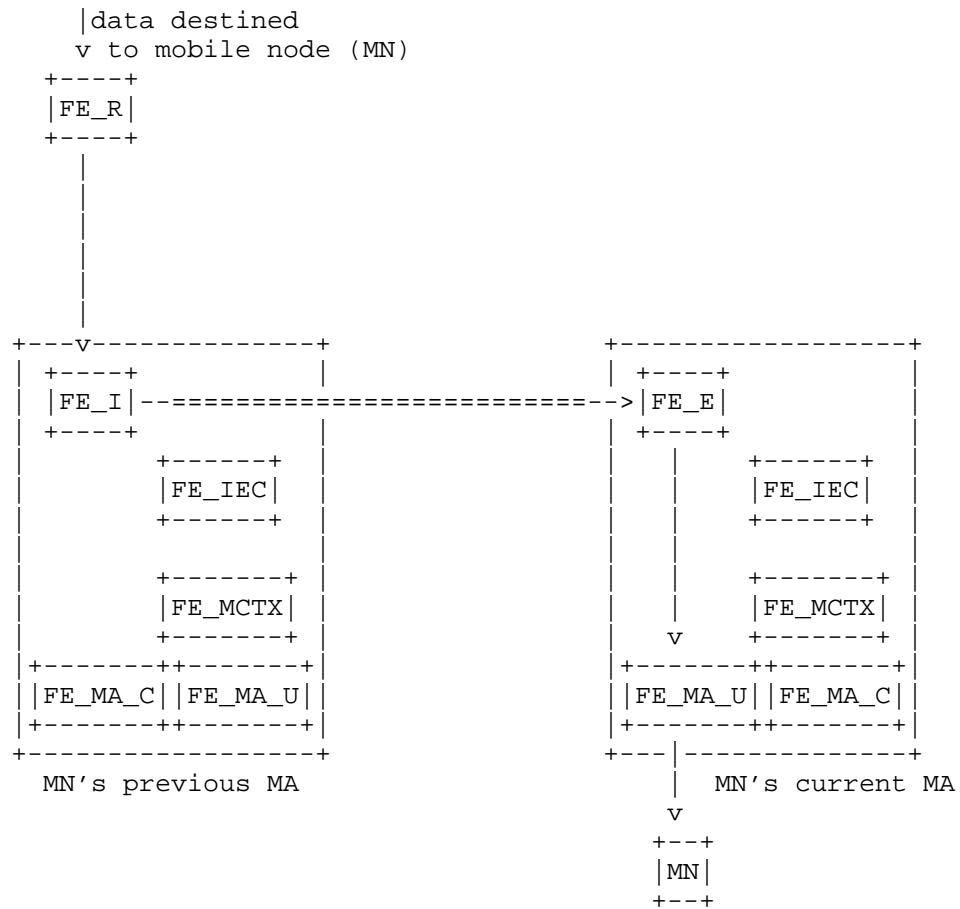


Figure 2: Condensed Deployment: Mobility Protocol Centric Solutions

4.2. Cooperative Deployment: Distributed Architecture

A distributed architecture considers protocol operation between distributed FEs, aiming at a DMM solution that's to a large extent independent of the mobility architecture and protocol. A further goal is to establish optimal routing paths for the MN's traffic after the MN's mobility anchor has been relocated and IP address continuity must be provided.

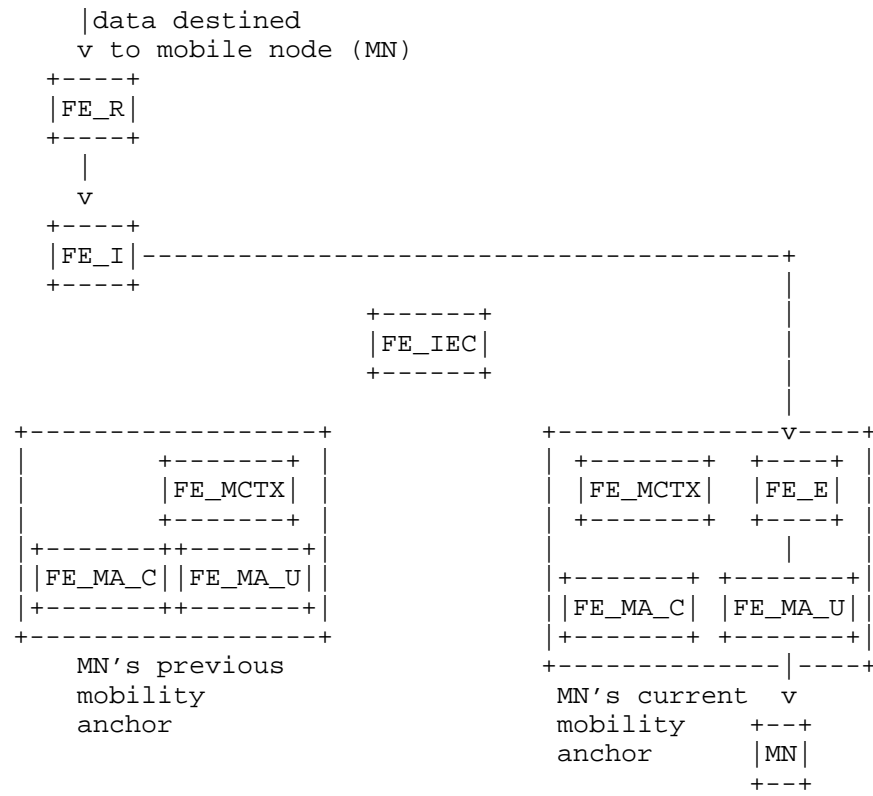


Figure 3: Cooperative Deployment: Distributed Architecture

5. Security Considerations

Different constellations of Functional Entities may allow re-use of existing protocols' security mechanisms to protect DMM protocol operation. In particular in a distributed model, new interfaces must be protected, e.g. to counteract unauthorized packet redirection to a different, possibly malicious mobility anchor. Details about security threats will be studied when the placement of Functional Entities for a selected set of preferred deployment models becomes mature.

6. IANA Considerations

As this document represents a framework and no protocol specification, there is no need for IANA actions.

7. References

7.1. Normative References

- [I-D.ietf-dmm-requirements]
Chan, A., Liu, D., Seite, P., Yokota, H., and J. Korhonen,
"Requirements for Distributed Mobility Management",
draft-ietf-dmm-requirements-14 (work in progress),
February 2014.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas,
"Protocol Independent Multicast - Sparse Mode (PIM-SM):
Protocol Specification (Revised)", RFC 4601, August 2006.
- [RFC4605] Fenner, B., He, H., Haberman, B., and H. Sandick,
"Internet Group Management Protocol (IGMP) / Multicast
Listener Discovery (MLD)-Based Multicast Forwarding
("IGMP/MLD Proxying")", RFC 4605, August 2006.
- [RFC6224] Schmidt, T., Waehlich, M., and S. Krishnan, "Base
Deployment for Multicast Listener Support in Proxy Mobile
IPv6 (PMIPv6) Domains", RFC 6224, April 2011.

7.2. Informative References

- [ITU-TY2018]
"ITU-T Y.2018, Mobility management and control framework
and architecture within the NGN transport stratum".
- [ITU-TY2804]
"ITU-T Q.1707/Y.2804, Generic framework of mobility
management for next generation networks".

Appendix A. How the framework can support a gap analysis! Some examples..

A Gap analysis can be performed according to different deployment models and variants as summarized in Section 4. A suitable set of DMM FEs can be mapped to the architecture of existing protocols from within or beyond the IP mobility protocol solution space to analyze and identify gaps in the chosen protocols to support and optimize DMM operations. This section provides a few examples about the mapping of DMM FEs to mobility protocol FEs and non-mobility protocol FEs. Common goal is to enable DMM support, either in a mobility protocol centric manner or by means of a distributed architecture, relying on the support and associated collaboration with non-mobility protocol functions, such as routing. As examples for the distributed architecture, the Locator-Identifier Split Protocol (LISP) and the iBGP have been used to enable traffic indirection in the routing plane above the topological level of distributed mobility anchors.

A.1. Condensed Deployment using Mobile IPv6

Note: A detailed example needs to be added in a next revision.

Description: Framework mapping to existing Mobile IPv6 architecture. Technical approach is the establishment of a forwarding tunnel between previous HA and new HA to enable IP address continuity after anchor relocation. Approach is the identification of missing protocol functions in Mobile IPv6 as expected from DMM functional entities as per this specification to enable full DMM support.

A.2. Condensed Deployment using Proxy Mobile IPv6

Note: A detailed example needs to be added in a next revision.

Description: Framework mapping to existing Proxy Mobile IPv6 architecture. Technical approach is the establishment of a forwarding tunnel between previous LMA and new LMA to enable IP address continuity after anchor relocation. Approach is the identification of missing protocol functions in Proxy Mobile IPv6 as expected from DMM functional entities as per this specification to enable full DMM support.

A.3. Cooperative Deployment using LISP

This example utilizes LISP Tunnel Ingress Routers (TIR) to perform the LISP map and encap procedure and tunnel packets to the mobile node's current mobility anchor (Figure 4). The mobile node's IP address is assumed routable above TIR level. TIRs can be for example deployed close to a mobile operator's IXP or close to operator-owned

traffic sources, such as a mobile Content Delivery Network (CDN). A TIR, which receives data packets destined to the mobile node, can consult the LISP Mapping Database (DB) to resolve the mobile node's IP address into its current locator, which is the mobile node's currently used mobility anchor. The mobility anchor has to terminate the LISP tunnel at the Tunnel Egress Router (TER) function and forward the data packets to the mobile node's current location according to the utilized mobility management protocol. An identified gap in a setup with LISP is the dynamic update of the Mapping Database and the update of already established states in TIRs in case the mobile node's location has changed from one mobility anchor to another mobility anchor.

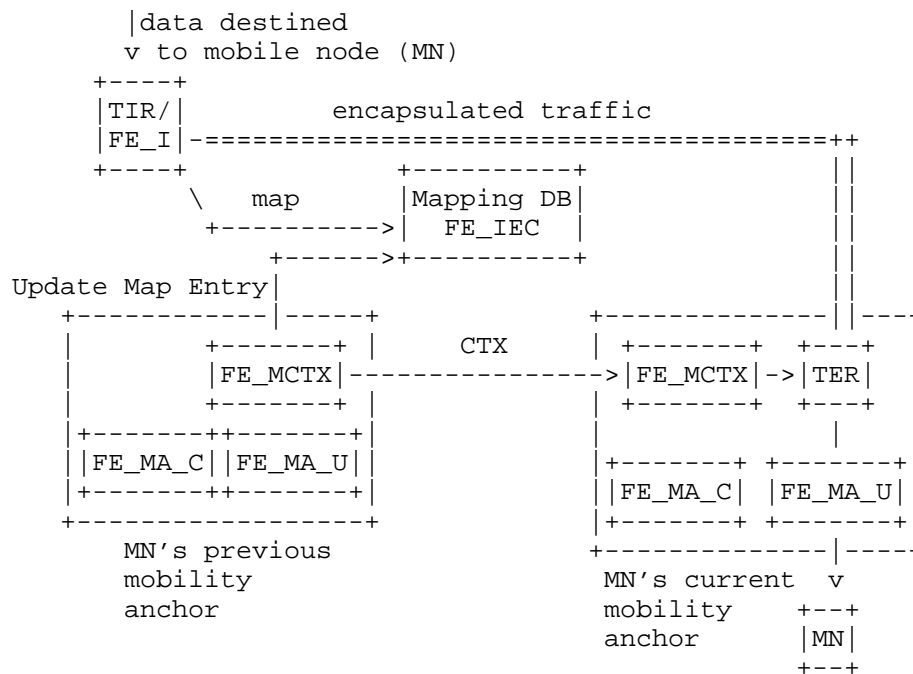


Figure 4: Example: DMM indirection at LISP TIRs

A.4. Cooperative Deployment using iBGP

This example utilizes the iBGP to establish per-host or group states in iBGP routers and forward a mobile node's packets hop-by-hop to its currently used mobility anchor. Figure 5 depicts an iBGP router with co-located FE_E and FE_I to receive data packets and to forward these packets to the next hop according to the routing state as per iBGP

update. The FE_IEC can be represented by the iBGP component to enable the setup of distributed routing states in distributed iBGP routers to direct the mobile node's data packets to its current mobility anchor. Hence, the FE_IEC is distributed in all iBGP routers to collaborate in the setup of host routes. The mobility anchor itself must implement iBGP to contribute to the distribution and update of host routes, e.g. after the mobile node changed its mobility anchor while IP address continuity must be supported. Since iBGP has been designed to propagate routing states to distributed routers, only minor protocol gaps may be identified in a detailed analysis. Beyond protocol gaps, further aspects need to be analyzed in such setup, which include limitations in scalability and route update latency.

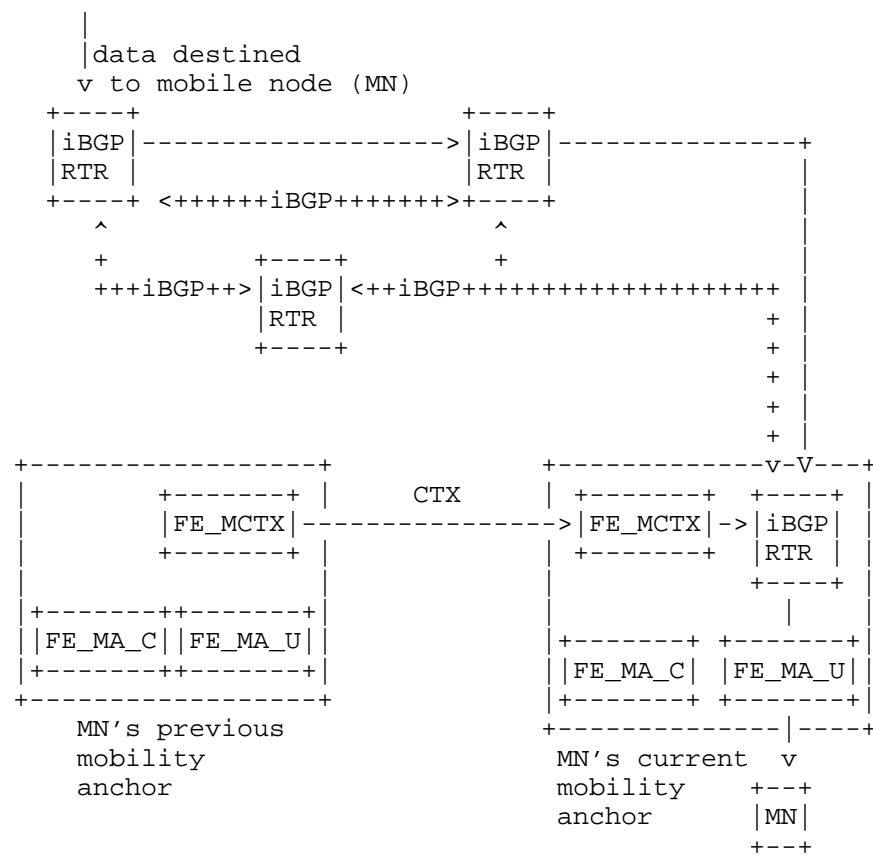
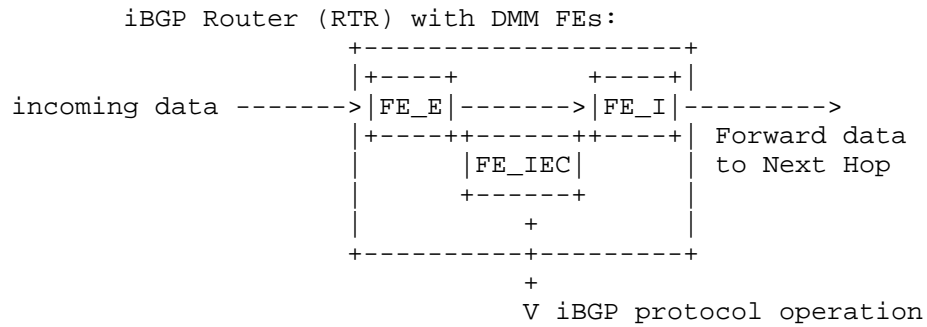


Figure 5: Example: DMM indirection at iBGP routers

Appendix B. Functional Architecture for Multicast DMM Support

The framework for multicast DMM support is similar to the framework for unicast DMM support introduced in Section 3 with the main difference that the additional introduced features are needed to support the multicast control and user plane. This framework, similar to the one introduced in Section 3, introduces four DMM-specific, with the main difference that these FEs are able to support multicast traffic, instead of unicast traffic. Additional FEs might be needed but are not considered in this revision of the draft, but can be introduced easily in future versions of the draft and considered for the BCP discussion and gap analysis.

The following FEs are currently considered as existing multicast based Functional entities to build the mobility- and transport network:

- o FE_MR: Functional Entity of a standard Multicast IP Router / Switch. This FE can be incorporated to support the functionality of a Rendezvous Point (RP) and of a Designated Router (DR), see e.g., [RFC4601].
- o FE_MLD-P: Functional Entity of a standard Multicast Listener Discovery Proxy (MLSD-P) used to provide MLD based forwarding, following the operation defined in e.g., [RFC4605] and [RFC6224].
- o FE_MA_C_M: Functional Entity Mobility Anchor, Control Plane, for the support of multicast traffic
- o FE_MA_U_M: Functional Entity Mobility Anchor, User Plane, for the support of multicast traffic
- o FE_MU_C: Functional Entity Mobile User Client, Control Plane, for the support of unicast and multicast traffic. In case of multicast traffic the FE_MU_C can operate as multicast sender and multicast listener.
- o FE_MU_U: Functional Entity Mobile User Client, User Plane, for the support of unicast and multicast traffic. In case of multicast traffic the FE_MU_U can operate as multicast sender and multicast listener.

The four DMM-specific FEs used to support multicast traffic are listed below.

- o FE_MCTX_M: Functional Entity Mobility Context Transfer, used for the support of multicast traffic.

- o FE_I_M: Functional Entity Ingress to DMM plane, used for the support of multicast traffic.
- o FE_E_M: Functional Entity Egress of DMM plane, used for the support of multicast traffic.
- o FE_IEC_M: Functional Entity for Ingress/Egress Control, used for the support of multicast traffic.

These FEs support similar features as the ones supported by the FE_MCTX, FE_I, FE_E, FE_IEC FEs, respectively, described in Section 3, with the main difference that they are used for the support of the multicast control and user planes, instead of the unicast control and user planes.

Figure 6 depicts the basic set of functional entities (FE) and interfaces to enable IP-address continuity in multicast based DMM. The four DMM-specific FEs and their associated operation on the interfaces between them can be realized by existing protocols, extensions to them or new protocols.

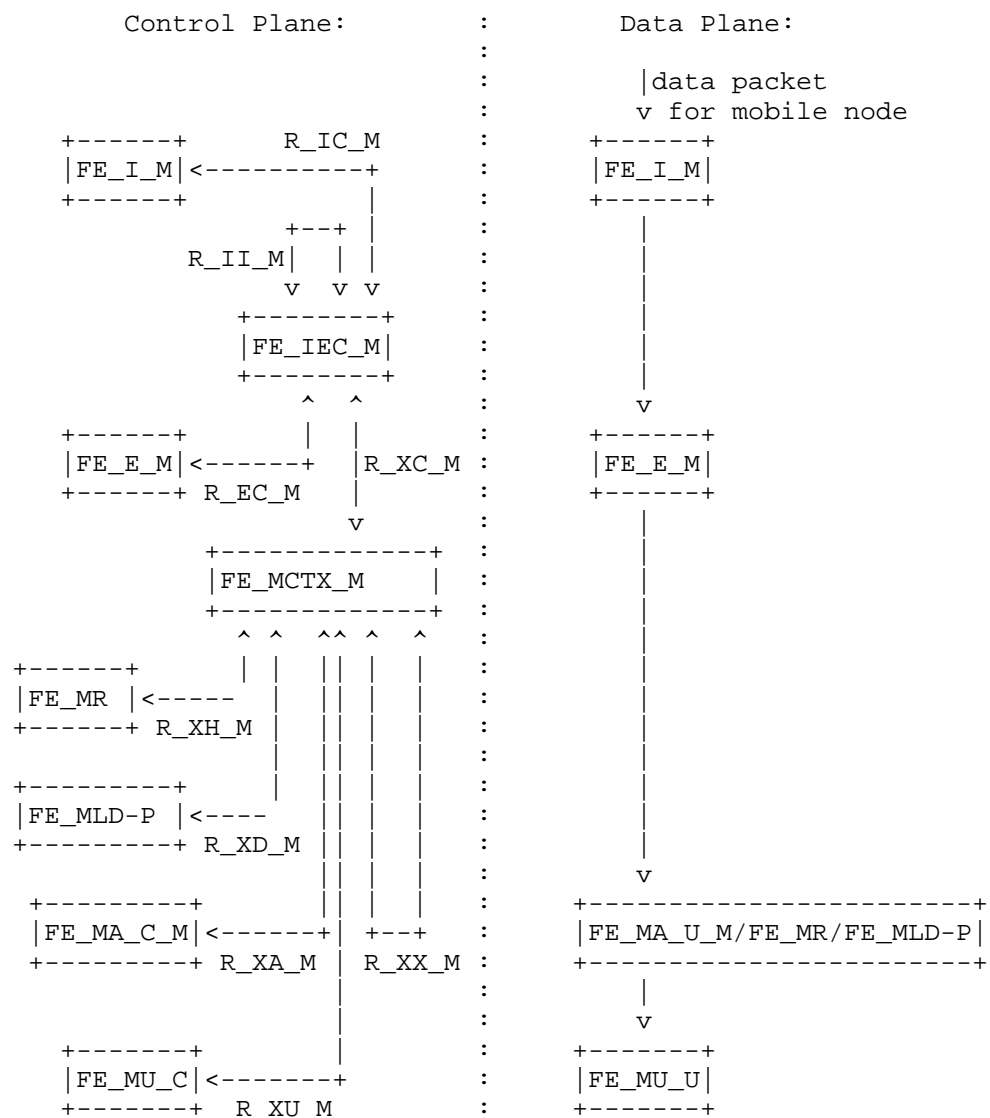


Figure 6: Basic set of functional entities (FE) and interfaces to enable IP-address continuity in multicast based DMM

The reference points between FEs are shown in Figure 6. In particular the features comprised by the reference points R_XA_M, R_XU_M, R_XX_M, R_IC_M, R_EC_M, R_XC_M, R_II_M, are similar to the ones supported by the reference points R_XA, R_XU, R_XX, R_IC, R_EC, R_XC, R_II, respectively, described in Section 3, with the difference that they are used to support the multicast based control plane,

instead of supporting the unicast based control plane.

Two additional reference points are added that are comprising the following features:

- o R_XH_M: Enables the FE_MCTX_M to retrieve MR routing based information from FE_MR following the operation defined in e.g., [RFC4601].
- o R_XD_M: Enables the FE_MCTX_M to retrieve Multicast Listener Discovery forwarding information from FE_MLD-P following the operation defined in e.g., [RFC4605] and [RFC6224].

Appendix C. Change Notes

Changes in version 01:

- o Introduced functional split between existing Mobility Anchor Control- and User-Plane
- o Introduced functional split of existing mobile user client Control- and User-Plane
- o Added uplink routing considerations in DMM architecture
- o Description of a first DMM Multicast framework in the Appendix
- o Added examples to the appendix about how to use the framework for a gap analysis and for the design of optimized DMM solutions

Authors' Addresses

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

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

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

Phone:
Email: pierrick.seite@orange-ftgroup.com

Georgios Karagiannis
University of Twente
AE Enschede, 7500
Netherlands

Phone: +31 53 4894099
Email: karagian@cs.utwente.nl

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: sgundave@cisco.com

DMM
Internet-Draft
Intended status: Standards Track
Expires: April 17, 2013

D. Liu
China Mobile
October 14, 2012

Deployment of existing mobility protocols in DMM Scenario.
draft-liu-dmm-of-deployment-00

Abstract

Distributed Mobility Managment(DMM) aims to eliminate the centralized anchor point of current IP mobility solutions to get better scalability and optimize the data plane routing. Many soulutions have been proposed in DMM working group but before defining any new DMM protocol, it is a good approach to investigate first whether it is feasible to deploy current IP mobility protocol in DMM scenario in a way that can meet all the requirment of DMM.This document discusses the way of the deployment of current IP mobility protocol in DMM scenario and analyses the gaps between this approach and the DMM requirment.

Requirements Language

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 RFC 2119 [RFC2119].

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 17, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the

document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	3
2. Distributed Mobility Management Use Cases	3
3. Deployment of current IP mobility protocol in DMM scenario	4
3.1. Client-based mobility solution in DMM scenario	4
3.2. Network based mobility solution in DMM scenario	5
4. Gap analysis	6
5. IANA Considerations	6
6. Security Considerations	6
7. Co-authors and Contributors	7
8. Acknowledgements	8
9. References	8
9.1. Normative References	8
9.2. Informative References	8
Author's Address	8

1. Introduction

Most existing IP mobility solutions are derived from Mobile IP [RFC3775] principles where a given mobility anchor (e.g. the Home Agent (HA) in Mobile IP or the Local Mobility Agent (LMA) in Proxy Mobile IPv6 [RFC5213] maintains Mobile Nodes (MNs) bindings. Data traffic is then encapsulated between the MN or its Access Router (e.g. the Mobile Access Gateway (MAG) in PMIPv6) and its mobility agent. These approaches lead to the implementation of centralised architectures where both MN context and traffic encapsulation need to be maintained at a central network entity, the mobility anchor. Such centralised approach provides the ability to route MN traffic whatever MN's localisation while maintaining IP session continuity during handovers. However, when hundreds of thousands of MNs are communicating in a given cellular network, a centralized mobility anchoring point causes well-known bottlenecks and single point of failure issues, which requires costly network dimensioning and engineering to be fixed. In addition, tunnelling encapsulations impact the overall network efficiency since they require the maintenance of MN's specific contexts in each tunnel end nodes and they incur delays in packet processing and transport functions.

2. Distributed Mobility Management Use Cases

Distributed Mobility Management can be used in the following use cases:

1. Local break out scenario

The fast increase of data traffic gives operators much pressure on their core network, operators have to extend their core network capacity and thence increase the cost. To deal with this problem, operators tend to offload their traffic in the network edge to decrease the pressure of their core network. This kind of solution usually called "local break out". In 3GPP, LIPA/SIPTO architecture is such kind of offload solutions for mobile operators. In the local break out scenario, the traffic is routed near the access point, but current IP mobility solution's anchor point usually located in the core network level. To solve this problem we can deploy the mobility anchor in the network edge, it will be discussed in detail in the following section.

2. CDN/Cache scenario

Similar to the local break out scenario, CDN/Cache usually been deployed in the network edge. In this scenario if all the data traffic still need to go back to a centralized mobility anchor in the core network it will cancel out the effect of CDN/cache. So the

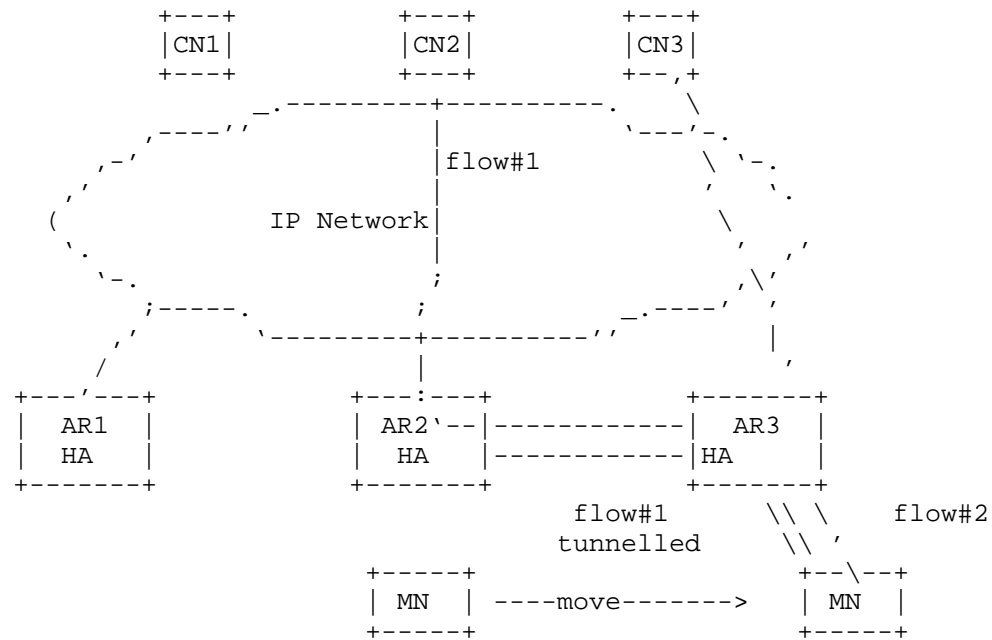
solution is also to deploy the mobility anchor point near the access network.

3. Deployment of current IP mobility protocol in DMM scenario

Current IP mobility protocol can be classified into client-based solution and network based solution. The basic idea is to deploy the mobility anchor near the access network and in this scenario, the MN may have more than one mobility anchors.

3.1. Client-based mobility solution in DMM scenario

One solution to deploy Mobile IP in DMM scenario is to implement the HA functionalities in the access routers, as shown on Figure 1. Any given IP flow can be considered as implicitly anchored on the current host's access router when set up. In addition, dynamic mobility anchoring [I-D.kassi-mobileip-dmi] could avoid data encapsulation for motionless nodes: until the host does not move, the IP flow is delivered as for any standard IPv6 node. The anchoring function at the access router is acting only to manage traffic indirection while the host moves to a new access router. So, when the MN handoff, its current traffic is still attached to the anchor access router which is responsible for forwarding the IP flows to the MN. For example, let's consider an IP flow, flow#1, initiated by the mobile node, MN, when attached to AR2. Flow#1 will be routed in a standard way as long as the MN remains attached to AR2. If the MN moves to AR3, flow#1 remains anchored to AR2, which plays the role of HA. If MN starts a new IP communication, flow#2, while attached to AR3; flow#2 will be routed in a standard way as long as the MN remains attached to AR3. Then, if the MN moves to AR1, flow#1 and flow#2 will be respectively anchored to AR2/HA and AR3/HA.

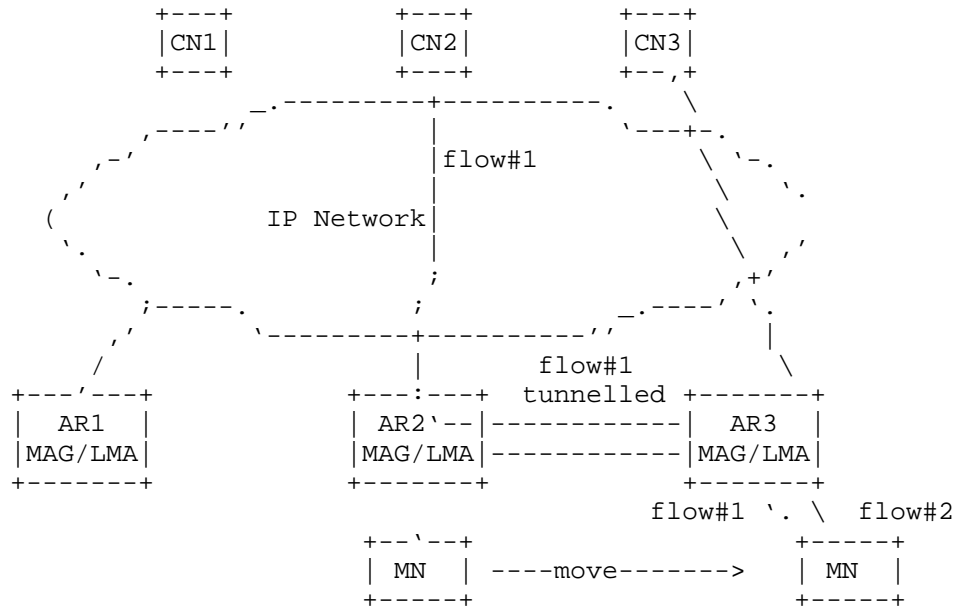


Distributed Client Based Mobility

3.2. Network based mobility solution in DMM scenario

Figure 2 shows the deployment of PMIP [RFC5213] in DMM scenario. The basic is to distribute mobility traffic management with dynamic user's traffic anchoring in the access network nodes. Each AR supports both the MAG and LMA functionalities. Any given IP flow can be considered as implicitly anchored on the current host's access router when set up. Until the host does not move, the IP flow is delivered as for any standard IPv6 node. The anchoring function at the access router is thus acting only to manage traffic indirection while the host moves to a new access router. So, when the MN handoff, its current traffic is still attached to the anchor access router which is responsible for forwarding its anchored MN's IP flows to the new MN's location (i.e. to the AR the MN is attached to). For example, let's consider an IP flow, flow#1, initiated by the mobile node, MN, when attached to AR2. Flow#1 will be routed in a standard way as long as the MN remains attached to AR2. If the MN moves to AR3, flow#1 remains anchored to AR2, which plays the role of LMA. AR3 plays the role of MAG for MN/flow#1. If MN starts a new IP communication, flow#2, while attached to AR3; flow#2 will be routed in a standard way as long as the MN remains attached to AR3. Then, if the MN moves to AR1, flow#1 and flow#2 will be respectively anchored to AR2/LMA and AR3/LMA and AR1 will provide MAG

functionalities for MN.



Distributed Network Based Mobility

4. Gap analysis

There are several problems need to consider in the above solutions.
 draft draft-liu-dmm-dynamic-anchor-discussion-00 ,
 draft-liu-dmm-address-selection-00 and draft-liu-dmm-mobility-api-00
 has discussed those problems in detail.

5. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

6. Security Considerations

TBD

7. Co-authors and Contributors

Many content of this document comes from DMM barbof and draft-liu-distributed-mobility-02, the original authors was list here as co-authors and contributors:

Pierrick Seite: pierrick.seite@orange-ftgroup.com

Hidetoshi Yokota: yokota@kddilabs.jp

Charles E. Perkins: charliep@computer.org

Hui Deng: denghui@chinamobile.com

Melia Telemaco: telemaco.melia@alcatel-lucent.com

Elena Demaria: elena.demaria@telecomitalia.it

Peter McCann: Peter.McCann@huawei.com

Kostas Pentikousis: k.pentikousis@huawei.com

Tricci So: tso@zteusa.com

Jong-Hyouk Lee: jh.lee@telecom-bretagne.eu

Jouni Korhonen: jouni.korhonen@nsn.com

Sri Gundavelli: sgundave@cisco.com

Carlos J. Bernardos: cjbc@it.uc3m.es

Marco Liebsch: Marco.Liebsch@neclab.eu

Wen Luo: luo.wen@zte.com.cn

Georgios Karagiannis: g.karagiannis@utwente.nl

Julien Laganier: jlaganier@juniper.net

Wassim Michel Haddad: Wassam.Haddad@ericsson.com

Alexandru Petrescu: alexandru.petrescu@gmail.com

Seok Joo Koh: sjkoh@knu.ac.kr

Dirk von Hugo: Dirk.von-Hugo@telekom.de

Ahmad Muhanna: amuhanna@awardsolutions.com

8. Acknowledgements

TBD

9. References

9.1. Normative References

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

9.2. Informative References

[I-D.draft-seite-dmm-dma-00]
Seite, P. and P. Bertin, "Distributed Mobility Anchoring, draft-seite-dmm-dma-00", February 2012.

Author's Address

Dapeng Liu
China Mobile
32 Xuanwumen West Street
Beijing, Xicheng District, 100053
China

Phone: +86-13911788933
Email: liudapeng@chinamobile.com

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 18, 2013

W. Luo
ZTE
S. Tricci
ZTE USA
October 15, 2012

Distributed Mobility Management Approach with Mobile IP and Proxy Mobile
IP
draft-luo-dmm-with-mip-and-pmip-00

Abstract

Based on the analysis of current centralized mobility management approaches, three main functions of current centralized mobility anchor are identified, which are Mobility Routing (MR), Home Address Allocation (HAA), and Location Management (LM), in this draft.

Based on the proposal of decoupling those functions, this draft provides a concept of architecture for Distributed Mobility Management (DMM) with some key approaches for DMM. Those approaches are compatible with both current MIP and PMIP protocols.

Requirements Language

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 RFC 2119 [RFC2119].

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 18, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	3
2. Conventions and Terminology	3
2.1. Conventions used in this document	3
2.2. Terminology	3
3. Solution Overview	4
3.1. Functional Decomposition	4
3.2. An Example of Networking Model	4
3.3. Concept Architecture of Distributed Mobility Management . .	5
4. Overview of the Distributed Mobility Management Approaches . .	7
4.1. Initial Attachment	7
4.2. Dynamic Mobility Management	7
4.3. Distributed Routing	8
4.4. Handover with Active Session	11
5. Supporting Client Based and Network Based Mobile IP	13
6. Considerations of the Optimized Routing	13
7. Security Consideration	14
8. Gaps with the Distributed Mobility Management Requirement . .	15
9. IANA Considerations	15
10. References	15
10.1. Normative References	15
10.2. References	15
Authors' Addresses	16

1. Introduction

Centralized mobility anchoring has several drawbacks such as single point of failure, routing in a non optimal route and etc. which are discussed in [I-D.liu-mext-distributed-mobile-ip].

Based on the analysis of current centralized mobility management approaches, three main functions of current centralized mobility anchor are identified, which are Mobility Routing (MR), Home Address Allocation (HAA), and Location Management (LM), in this draft.

Based on the proposal of decoupling those functions, this draft provides a concept of architecture for Distributed Mobility Management (DMM) with some key approaches for DMM. Those approaches are compatible with both current MIP and PMIP protocols.

This is an initial version, and not aimed to solve all issues which are defined in [I-D.liu-mext-distributed-mobile-ip]. Further, whether the architecture and approaches proposed in this draft can meet the DMM requirements defined in [I-D.ietf-dmm-requirements] is not examined carefully yet. The gap analysis will be provided in the future.

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

This draft introduces following terms which are very similar with terms defined in [I-D.chan-dmm-framework-gap-analysis].

Mobility Routing (MR), which is a logical function used for intercepting packets to/from the HoA of a mobile node and forwarding the packets, based on the corresponding location information to perform distributed routing.

Home Address Allocation (HAA), which is a logical function used for allocating home network prefix or home address to a mobile node.

Location Management (LM), which is a logical function, used for managing and keeping track of the internetwork location information of a mobile node, which includes a mapping of the HoA of the MN to

the routing address of the MN (i.e. routing location) or another network element that knows how to forward packets towards the MN.

3. Solution Overview

3.1. Functional Decomposition

The existing mobility management technology, such as MIP, PMIP and etc., bundles all the mobility management functions into one centralized Home Agent (HA) or Local Mobility Anchor (LMA).

Sharing similar view with [I-D.chan-dmm-framework-gap-analysis], this draft decomposes those centralized anchor into the following logical functions to allow a more flexible design to achieve distributed mobility management (DMM):

- a. Home Address Allocation (HAA) function
- b. Mobility Routing (MR) function
- c. Location Management (LM) function

Assuming for any given administrative domain, it consists of one or more so called local network (as illustrated in figure 1). Further, each those local networks most likely consists of several routers which are deployed with mobility routing (MR) function, and one home address allocation (HAA) function and one location management (LM) function.

The HAA and LM, depended on the operating policy, could be deployed as a combined entity or be deployed separately.

3.2. An Example of Networking Model

Figure 1 illustrates a possible deployment of distribute mobility management specified by this draft, which contains 3 local networks.

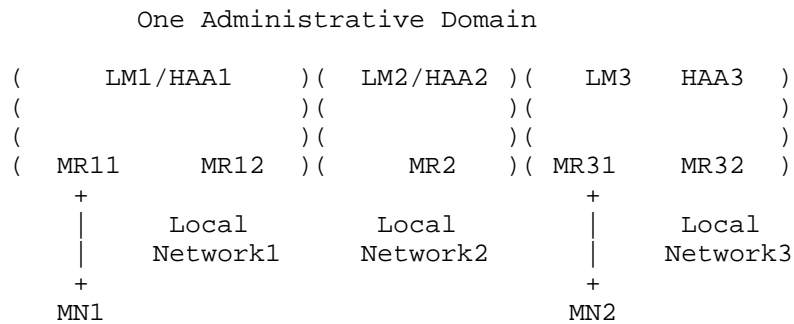


Figure 1. An example of DMM deployment

Both local network 1 and local network 3 contain multiple MRS (e.g. two MRs), while local network 2 includes one MR. The LM and the HAA are co-located as a single entity in local network 1 and 2, while are deployed separately in local network 3.

One should be noticed that, the above figure is only an example. In actual deployment, for one single local network, multiple LMs and HAAs could also be deployed.

One should also be noticed that, in this draft, assuming all local networks belong to a same administrative domain (e.g. one operator). Otherwise, out of the scope of this draft.

3.3. Concept Architecture of Distributed Mobility Management

For supporting distributed mobility management, signaling interactions are needed between those MR, LM and HAA. This section tries to illustrate architecture of the DMM approaches specified in this draft.

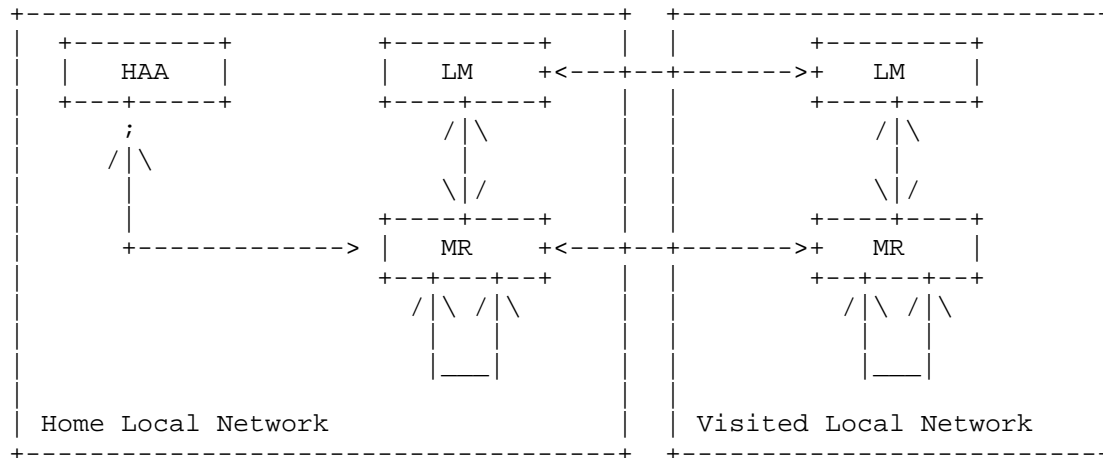


Figure 2. Architecture

The local network to which the MN is initially attached is known as its home local network. The HAA function of mobile node's home local network is responsible for IP address\prefix (i.e. HoA\HNP) assignment for the mobile node. During the movement, the mobile node could leave its home and enter one another local network which is known as visited local network in this draft.

Interfaces among HAA, LM and MR are needed, and are described as following

- Interface between HAA and MR, which supports signaling for IP prefix or address assignment, during the attachment of a mobile node to a MR
- Interface between LM and MR, which supports signaling for maintaining the routing location of mobile node, and the set up of an optimized routing for mobile node
- Interface between MR and MR, which supports the signaling for the handover of a mobile node from previous MR (pMR) to new MR (nMR) in control plane, and supports delivering traffic between mobile node and its correspondent node in a distributed manner in data plane.

An administrative domain may have a large amount of mobile nodes; therefore the LM may need to maintain a large amount of information (i.e. tracing the routing location of those mobile nodes).

It is better for an administrative domain to deploy multiple LMs.

Those LMs could be deployed in a form of distributed database, and interfaces between them are necessary for information interactive.

4. Overview of the Distributed Mobility Management Approaches

4.1. Initial Attachment

The initial attachment for distributed mobility management specified in this draft is triggered when a mobile node is initialized and attached to an access link on which the mobile node is connected to a MR.

When determining that mobile node is authorized for the DMM service, MR interacts with HAA, which is in the same local network, by signaling, over the interface between them, for the purpose of HoA\HNP assignment. The HoA\HNP assignment mechanism could be based on stateful or stateless mechanism.

After configuring HoA\HNP for the mobile node, that local network becomes mobile node's home local network. The MR, depends on the local policy, may interact with a LM which is also in mobile node's home local network (i.e. MN's home LM) to update the mobile node's routing location.

Updating mobile node's routing location during initial attachment is not a mandatory step. Since the mobile node is currently attached to its home local network and the assigned HoA\HNP is anchored at mobile node's currently attached MR. The traffic, which is designated to mobile node's HoA\HNP, should be routed to that MR by regular IPv6 routing mechanism automatically.

4.2. Dynamic Mobility Management

Mobile node may change its point of attachment from pMR to nMR when it moves. The nMR may locate at mobile node's home local network, or may at a different local network (i.e. visited local network).

Based on the attachment event, the nMR should try to retrieve mobile node's HoA\HNP configuration status first (e.g. from mobile node's HAA in home local network), and update mobile node's LM with its new routing location (e.g. IP address of nMR).

Depend on the configuration of the network, new HoA\HNP which is anchored at nMR could be assigned to mobile node when the mobile node is attached to the nMR. In this case, both HoAs\HNPs which are anchored at pMR and nMR respectively are available for the mobile node.

In this case, newly initiated session after the handover is preferred to use new HoA\HNP as source IP. Meantime, old session which has already initiated before handover could still use the old HoA\HNP as source IP for the purpose of keeping session continuity. The similar idea is also proposed in [I-D.seite-dmm-dma], [I-D.bernardos-dmm-distributed-anchoring] and [I-D.korhonen-dmm-local-prefix].

But, one should note that, in the above configuration, mobile node should have ability to manage multiple HoAs\HNPs, and should have ability to decide to return which one of those multiple HoAs when applications on the mobile node ask for an IP address to bind.

4.3. Distributed Routing

To perform optimized routing, the MRs need the location information which is maintained at the LMs. Use the scenario illustrated in figure 1 as an example.

The assumptions are as following:

- o MN1 and MN2 are currently attached to MR11 and MR 31 respectively
- o The destination IP address of the traffic (from MN2 to MN1) is set to the HoA of MN1
- o The MN1's HoA above is anchor at MR12 (which means the regular IPv6 routing mechanism will deliver any packet whose destination IP address is set to MN1's HoA to MR12), not the MR to which the MN1 is currently attached (i.e. MR11).

Then, upon receiving the initial few packets of the traffic, MR31 should determine how to forward the traffic optimally.

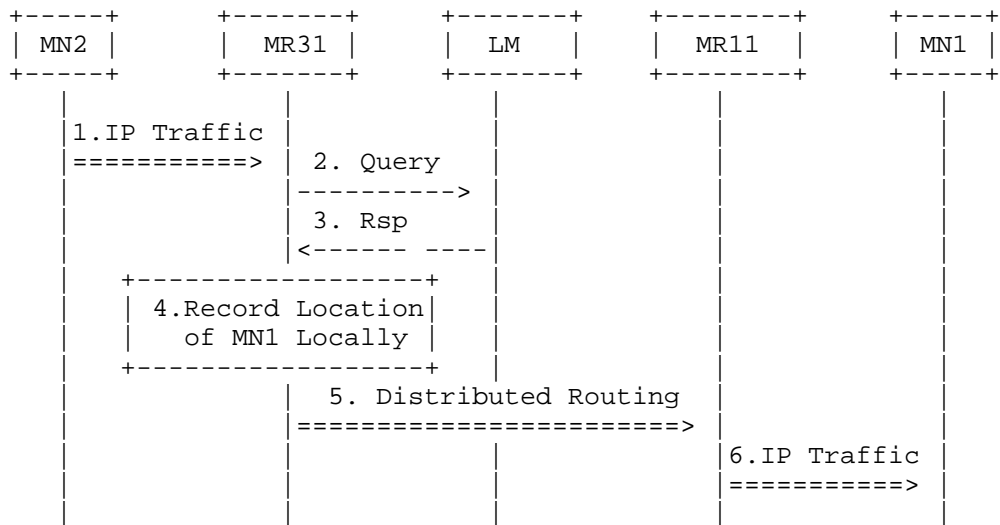


Figure 3. Optimized routing based on location query

Figure 3 illustrates one possible behavior the MR31 could take for the purpose of determining how to forward the traffic in an optimized manner.

MR31 first determines whether it holds the routing location information of MN1 locally. If not, MR31 will initiate a query to a LM (e.g. MN1's home LM), who holds such information, by sending a query message via the interface between MR and LM.

When receiving the response, MR31 should save the queried routing location information of MN1 locally.

Based on the routing location information retrieved, MR31 could perform so called distributed routing for delivering the traffic.

- o One of distributed routing mechanism: MR31 could set up its endpoint of a tunnel (e.g. IP in IP tunnel) to MR11 based on MN1's routing location, encapsulate all IP packets of the traffic and send those encapsulated IP packets to MR11 in the established tunnel directly.
- o Another one of distributed routing mechanism: as specified in [I-D.liebsch-mext-dmm-nat-phl], per-host-locator mechanism can be used by MR31 to perform distributed routing, in which, the locator is MN1's routing location.

Only two example distributed routing mechanisms are list above. Some

better mechanisms can be developed in the future.

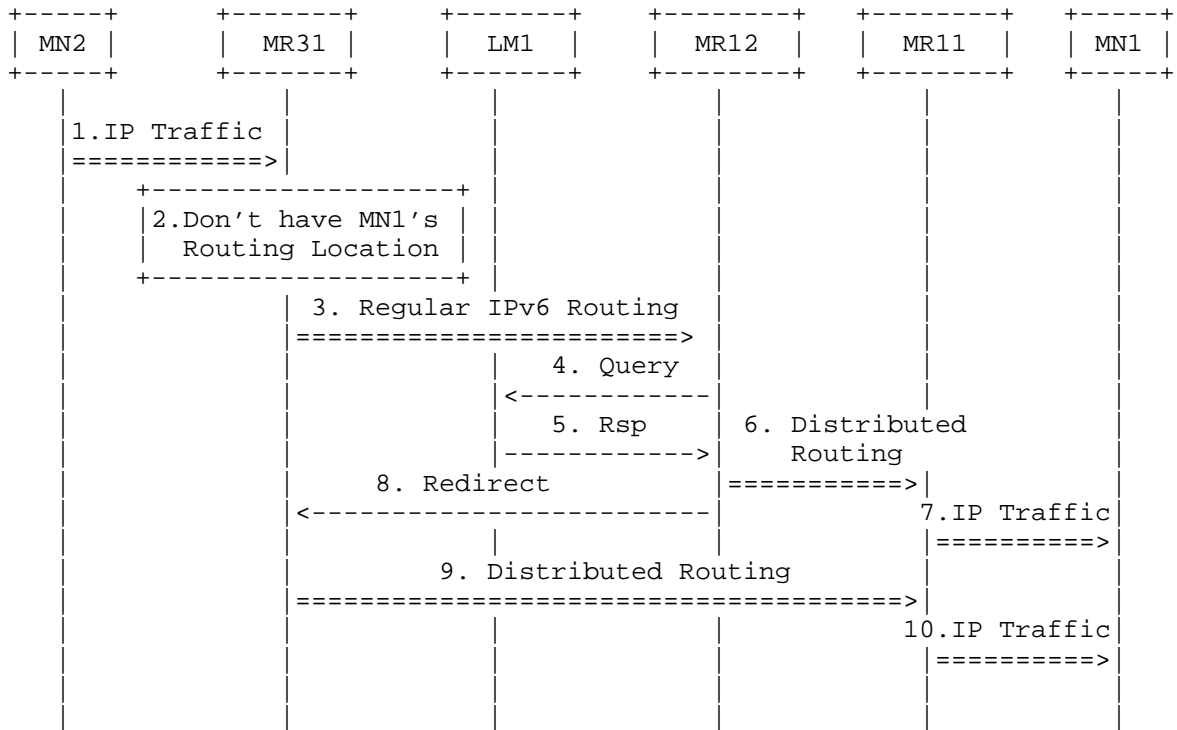


Figure 4. Another approach for optimized routing

As indicated in [I-D.chan-dmm-framework-gap-analysis], multiple mechanisms can be used for setting up optimized routing for DMM. Figure 4 illustrates another possible behavior the MR31 could take for the purpose of determining how to forward the traffic in an optimized manner.

MR31 first determine whether it holds the routing location information of MN1 locally. And if MR31 determines it doesn't hold such information, it will forward the traffic received by regular IPv6 routing mechanism.

The traffic will be forwarded to MR12, based on the assumption that the destination IP address of the traffic (i.e. HoA of MN1) is anchored at MR12. Upon receiving the traffic, MR12 will determine that the MN1 is not attached to itself. As a result, MR12 will query with LM for MN1's routing location.

When MN1's routing location information is determined, MR12 could

perform distributed routing for delivering the traffic, as described above, to MR11 to which the MN1 is currently attached and then forwarded to MN1 by MR11.

MR12 is further preferred to send another message to MR31 via interface between MRs to inform MR31 with MN1 current routing location to trigger the direction. The MR31, based on the received routing location information, will perform distributed routing for delivering the rest IP packets of traffic, first to MR11, then to MN1, as described above.

One can note that, for both behaviors described above, when the routing between MN1 and MN2 is established, the routing is optimized: MN2=>MR31=>MR11=>MN1.

For the latter behavior, one can also note that, if the MN1 is currently attached to the MR12, the routing for traffic from MN2 to MN1 will be identical with regular IPv6. But, how the MR12 can determine MR31 (i.e. the MR to which the MN2 is attached) is a challenge.

4.4. Handover with Active Session

Section 4.2 has already discussed scenarios the mobile node changes its point of attachment, but without discussing how to maintain the continuity of sessions which are initiated before the handover.

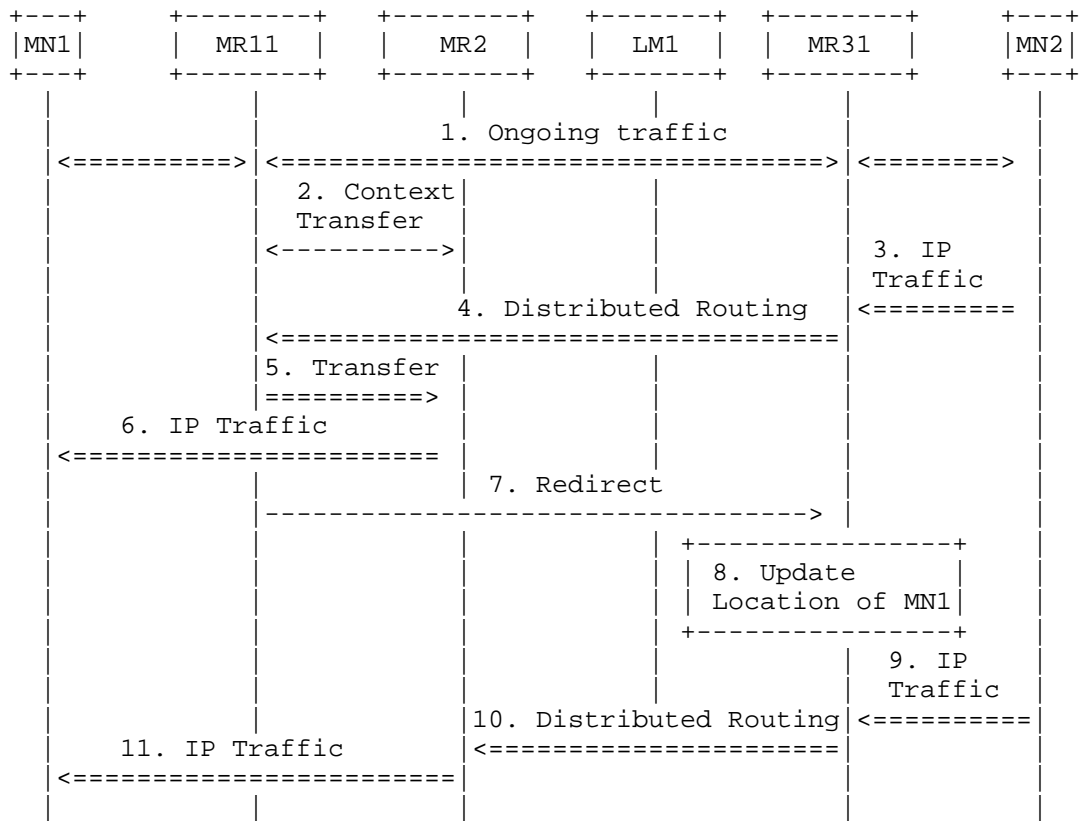


Figure 5. Handover with Active Session

Figure 5 illustrates approaches for handover of MN1 from pMR (MR11) to nMR (MR2). During the handover, the nMR need to update MN1's new routing location to the LM.

Context transfer between nMR and pMR is always necessary, e.g. security context. The nMR could inform the pMR with MN1's new routing location information during the context transfer.

Based on the received information, pMR sets up mobility context for MN1 locally to at least record MN1's new routing location. It should be noted that, the mobility context for a specific mobile node which is performing handover is just a temporarily information. When the handover is finished, the correspondent mobility context need to be deleted.

MR31 to which the MN2 is attached isn't aware of the handover event of MN1. Thus, the traffic from MN2 to MN1 will still be forwarded by

MR31 to the pMR (MR11) in a distributed routing manner (which is described in section 4.3 above).

For reducing packet loss, the pMR is preferred to establish a directional tunnel to nMR and forward the received packets from MR31 to nMR via the tunnel. The key is that, the pMR needs to send a message to MR31 to update MN1's routing location stored in MR31 locally. Based on the updated routing location information of MN1, MR31 will forward the upcoming traffic from MN2 to MN1 to the nMR directly.

5. Supporting Client Based and Network Based Mobile IP

Figure 2 in [I-D.chan-dmm-framework-gap-analysis] analyzes MIP and PMIP by comparing the destination IP address in the network-layer header as a packet traverses from a CN to an MN. According to the comparison, as far as the data-plane traffic is concerned, the route from CN to MN in MIP is similar to the route from CN to MAG in PMIP. The difference is only in replacing the MN in MIP with the MAG-MN combination in PMIP. Therefore, the architecture using MIP can be adapted to the architecture using PMIP by replacing the MN with the MAG-MN combination.

Based on the above analysis which is provided [I-D.chan-dmm-framework-gap-analysis], the idea of DMM solution proposed in this draft applied to both MIP and PMIP supported clients.

- o If applying MIP to the deployment scenario illustrated in figure 1, the MR could be implemented with part of HA function
- o If applying PMIP to the deployment scenario illustrated in figure 1, the MR could be implemented with part of LMA function, and put MAGs between MRs and MNs. Otherwise, the MR could be implemented with part of both LMA and MAG functions.

6. Considerations of the Optimized Routing

One can note that, the routing between MN and CN is optimized based on the mechanism described in section 4.2. And in section 4.2, the CN is assumed to be a mobile node. That means CN must be attached to a certain MR, and that MR will keep track of the location of CN and interpreted any packet sent from CN to MN. But, when CN is a fixed node, there may be no such MR which servers the CN.

In real world, most of such fixed nodes (CN) are deployed in a

centralized manner, e.g. CDN/IDC/Web Servers and etc. Those fixed nodes are generally converged by a couple of access routers, although the topology within those fixed nodes may be very complicating, to access operator's IP bearer network. Figure 6 is an example.

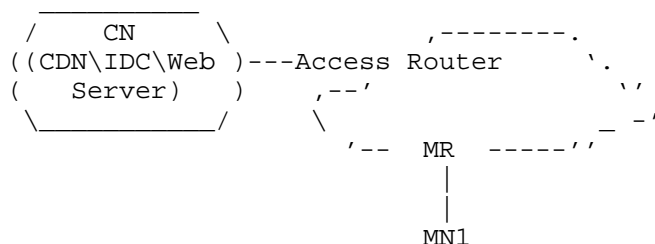


Figure 6. CNs are fixed nodes

For the scenario described in figure 6, a direct solution is to implement MR function with that so called convergence access router or gateway router (i.e. the access router illustrated in the above figure).

Another alternative is to use anycast mechanism described in [I-D.chan-dmm-framework-gap-analysis] and [I-D.wakikawa-mext-global-haha-spec]. Anycast mechanism could guarantee the traffic sent from CN to MN to reach a nearest MR which anycast the HNP aggregation of the mobile node.

7. Security Consideration

This draft proposes signaling messages interaction over interfaces among MRs, LMs and HAAs for supporting Distributed Mobility Management (figure 2). The security issues should be considered for those messages.

Since, this draft assumes all local networks belong to a same administrative domain (e.g. one operator), then signaling interfaces among those MRs, LMs and HAAs can be established directly. Security association mechanism which is used for protecting PBU\PBA messages defined in [RFC5213] can be reused for protecting signaling messages (such as IP address allocation, routing location information update\query) between MR and LM\HAA.

Signaling between MRs (such as signaling for distributed mobility support) in this draft is preferred to be protected by using end-to-end security association(s) offering integrity and data origin authentication. The MR is proposed to implement IPsec [RFC4301] or

other equivalents for protecting the messages. E.g. IPsec Encapsulating Security Payload (ESP, [RFC4303]) in transport mode with mandatory integrity protection could be used for protecting those signaling messages.

8. Gaps with the Distributed Mobility Management Requirement

TBD

9. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

10. References

10.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.
- [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

10.2. References

- [I-D.bernardos-dmm-distributed-anchoring]
Bernardos, CJ. and JC. Zuniga, "PMIPv6-based distributed anchoring", September 2012.
- [I-D.chan-dmm-framework-gap-analysis]
Chan, H., "A unified mobility management protocol framework and DMM gap analysis", July 2012.

- [I-D.ietf-dmm-requirements]
Chan, H., "Requirements for Distributed Mobility Management", September 2012.
- [I-D.korhonen-dmm-local-prefix]
Korhonen , J. and T. Savolainen , "Local Prefix Lifetime Management for Proxy Mobile IPv6", March 2012.
- [I-D.liebsch-mext-dmm-nat-phl]
Liebsch , M., "Per-Host Locators for Distributed Mobility Management", March 2012.
- [I-D.liu-mext-distributed-mobile-ip]
Liu, D., "Distributed Deployment of Mobile IPv6", March 2010.
- [I-D.seite-dmm-dma]
Seite , P. and P. Bertin , "Distributed Mobility Anchoring", July 2012.
- [I-D.wakikawa-mext-global-haha-spec]
Wakikawa , R., "Global HA to HA Protocol Specification", September 2011.

Authors' Addresses

Wen Luo
ZTE
No.68, Zijinhua RD,Yuhuatai District
Nanjing, Jiangsu 210012
China
Email: luo.wen@zte.com.cn

Tricci So
ZTE USA
Email: tso@zteusa.com

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 18, 2013

B. Sarikaya
Huawei USA
October 15, 2012

Mobility Management Protocols for Cloud-Like Architectures
draft-sarikaya-dmm-cloud-mm-00.txt

Abstract

Telecommunication networks are being virtualized and are moving into the cloud networks. This brings the need to redesign the mobility protocols of Mobile and Proxy Mobile IPv6. This document defines mobility management protocols for virtualized networks. Control and data plane separation is achieved by separating Home Agent and Mobile Access Gateway functionalities into the control and data planes.

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 18, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as

described in the Simplified BSD License.

Table of Contents

1. Introduction	3
2. Terminology	4
3. Control and Data Plane Separation for MIPv6	5
4. Authentication in Control and Data Plane Separation	6
5. Control and Data Plane Separation for PMIPv6	7
6. Security Considerations	8
7. IANA Considerations	8
8. Acknowledgements	9
9. References	9
9.1. Normative References	9
9.2. Informative references	10
Author's Address	11

1. Introduction

Mobile IPv6 defines client based mobility support to the mobile nodes and is defined in [RFC6275]. There are several extensions to Mobile IPv6 such as multiple Care-of Address registration for multi-homed mobile nodes [RFC5648], flow mobility [RFC6089] and Dual Stack Mobile IPv6 [RFC5555]. Mobile IPv6 is based on a centralized mobility anchoring architecture at the home agent (HA).

Proxy Mobile IPv6 defines network based mobility support to the mobile nodes and is defined in [RFC5213]. PMIPv6 operation involves a Mobile Access Gateway handling mobility of the mobile node and registering the mobile node with the Local Mobility Anchor (LMA) which receives and sends MN traffic into the Internet. LMA operation is compatible with the home agent of MIPv6. IPv4 support for PMIPv6 is defined in [RFC5844] and flow mobility extensions in [I-D.ietf-netext-pmipv6-flowmob].

Centralized mobility anchoring has several drawbacks such as single point of failure, routing in a non optimal route, overloading of the centralized data anchor point due to the data traffic increase, low scalability of the centralized route and context management [I-D.ietf-dmm-requirements].

Architecture of a cloud network is shown in Figure 1, see also [I-D.rekhter-nvo3-vm-mobility-issues]. Top of Rack Switch (ToR) is a switch in a cloud network that is connected to the servers. The servers host virtual machines. A cloud network has one or more Data Center Border Routers (BR) or edge routers that connects the cloud network to the Internet including other cloud network or storage networks. Storage network is usually part of the same cloud network and it is connected to the BR using Fiber Channel (fc) links.

Control and data plane separation is stated as a requirement for the distributed mobility management. Mobile IPv6 control plane is used for registration and handover signaling and for establishing security association, e.g. IPSec SAs. Data plane is used for data transfer from the corresponding nodes (CN) to MN and from MN to CNs. Typically control plane traffic is much lighter than the data plane traffic and control plane traffic has stronger latency requirements. Control plane data plane separation requires signaling between the control and data plane functional entities.

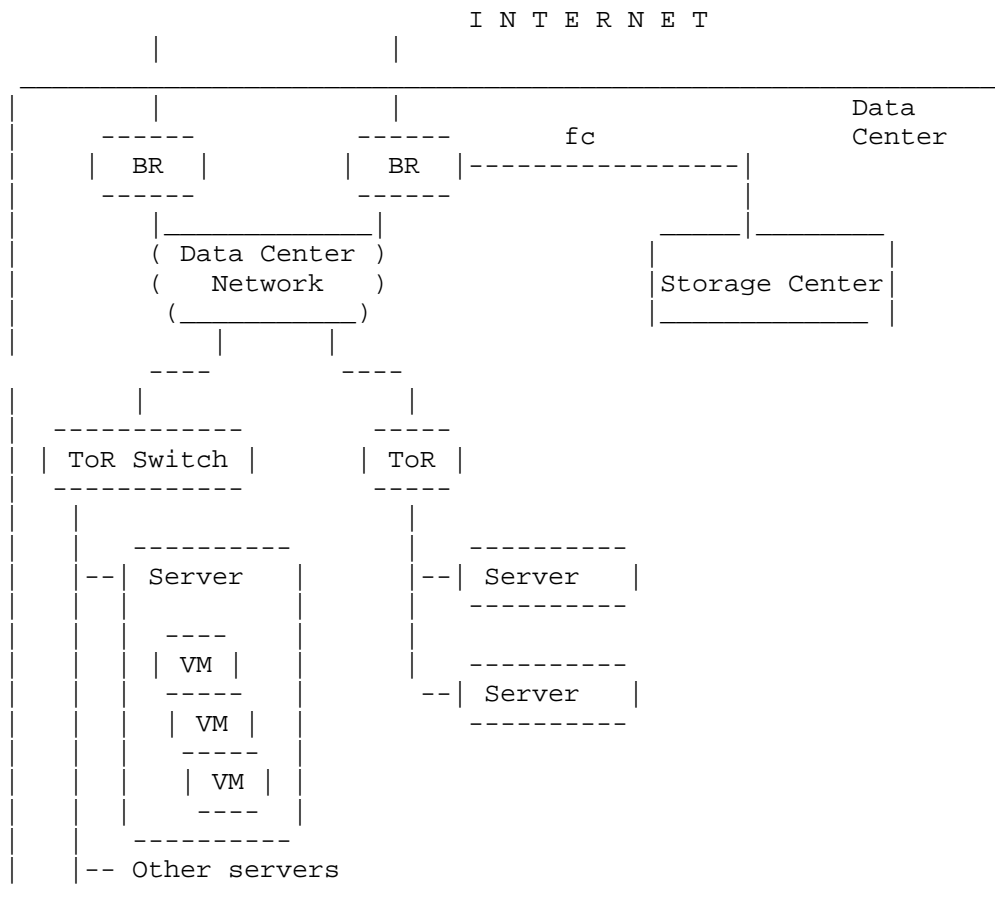


Figure 1: Architecture of Cloud

2. Terminology

This document uses the terminology defined in [RFC6275] and [RFC5213].

3. Control and Data Plane Separation for MIPv6

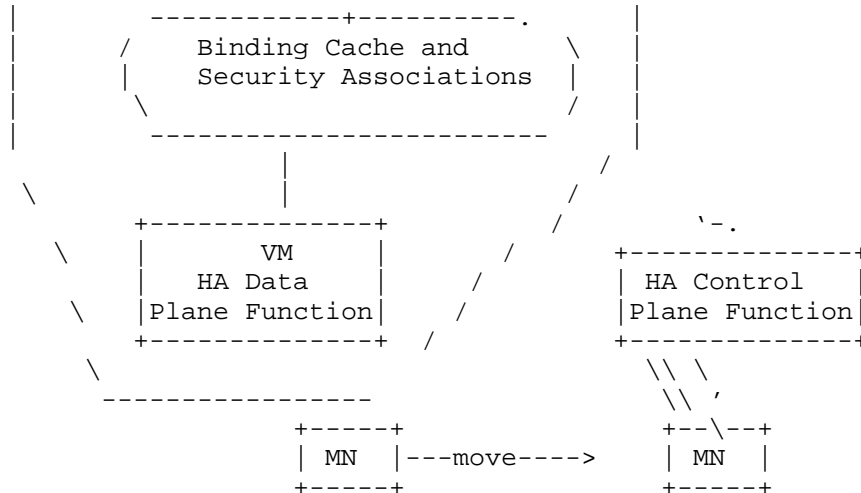


Figure 2: Architecture of MIPv6 Control and Data Planes

Control and data plane separation can be achieved by dividing HA into two functional entities: control plane functional entity and data plane functional entity as shown in Figure 2. These functional entities can be hosted on different physical entities. These two entities must share a common database. The database contains the binding cache and the security association information such as IPSec keys.

HA Data Plane function can be implemented as virtual machine (VM) in a cloud network. Binding cache and security associations will be stored in the storage center of the cloud network that VMs can easily access. HA Control Plane function is geographically more distributed than HA data Plane function and is placed closer to the mobile nodes in order to meet the latency requirements.

MN first communicates with the control plane function to establish security association. Address configuration and binding registration follows. Next MN receives/sends data packets using the data plane function closest to the link MN is attached.

When MN moves MN does handover signaling with the control plane function which updates the binding cache based on this move. Control plane function informs the new data plane function of this binding cache update and then MN starts to receive and send data to the new data plane function. MN MUST keep HA control plane function address in cache so that it can conduct handover signaling with it.

When MN boots, it goes through authentication and security association establishment. Next MN sends a binding update. MN does these steps with HA control plane function. MN sends Binding Update message to HA control plane function and receives a Binding Acknowledgement message and in this message MN MUST receive HA data plane function address.

HA data plane function address can be provided by HA control plane function to MN in Alternate Home Agent Tunnel Address option defined in [I-D.perkins-netext-hatunaddr] of BA message [RFC6275]. MN starts tunneling data packets and sends them to Alternate Home Agent Tunnel Address. Also MN receives data packets tunneled from Alternate Home Agent Tunnel Address.

Control and data plane separation does not require protocol extensions except the sharing of binding cache and security associations database. How this sharing can be accomplished is left out of scope with this specification.

4. Authentication in Control and Data Plane Separation

Currently, MN and HA create security associations (SA) based on the home address using IKEv2 as the key exchange protocol. When MN moves SAs are reestablished when MN gets a new care-of address. After SA is established, MN and HA use Encapsulating Security Payload (ESP) encapsulation for Binding Updates and Binding Acknowledgements [RFC4877].

IKEv2 enables the use of EAP authentication and provides EAP transport between MN as the peer and HA as the authenticator. EAP authentication is done using one of the EAP methods such as EAP-AKA [RFC4187].

MN is authorized as a valid user using EAP authentication. IKEv2 public key signature authentication with certificates is used to authenticate the home agent and derive keys to be used in exchanging BU/BA securely. MN can use the same identity, e.g. MN-NAI during both EAP and IKEv2 authentication.

On the other hand MN goes through the access authentication when it first connects to the network. A typical access authentication protocol is AKA. MSK derived from this authentication serves as the session key in accessing the air interface.

There is an overlap between the access and user authentications sometimes done using the same protocol, e.g. AKA. Full EAP method execution may take several round trips, some times five or more round

trips and slow down the user access to the Internet. This is especially an important consideration in Distributed Mobility Management since MN may connect to several home agents instead of staying anchored at one home agent.

In order to reduce the number of round trips EAP authentication can be combined with reauthentication. Reauthentication is EAP method dependent. EAP-AKA reauthentication takes only one round trip [RFC4187]. MN must go through an EAP-AKA reauthentication before when MN was connected to the previous HA. During reauthentication reauthentication ID is generated. MN MUST use its reauthentication ID during IKEv2 EAP authentication with the new home agent. This ensures that EAP-AKA authentication takes only one round trip. MN continues to use its reauthentication ID in subsequent reauthentication runs with the same HA.

5. Control and Data Plane Separation for PMIPv6

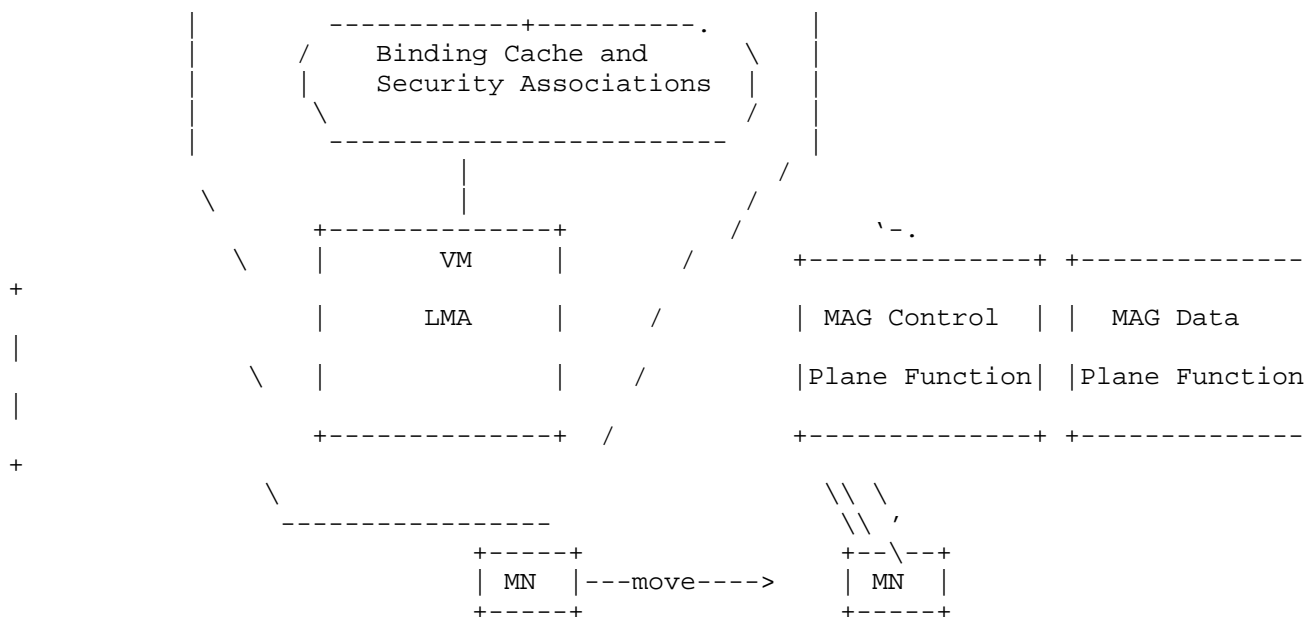


Figure 3: Architecture of PMIPv6 Control and Data Planes

Control and data plane separation can be achieved by dividing MAG into two functional entities: MAG control plane functional entity and MAG data plane functional entity as shown in Figure 3. LMA stays the same. LMA can be implemented as virtual machine (VM) in a cloud network. Binding cache and security associations will be stored in the storage center of the cloud network that VMs can easily access.

MAG Control Plane function together with MAG Data Plane function is geographically distributed and is placed closer to the mobile nodes

in order to meet the latency requirements.

MN first communicates with the MAG control plane function to establish security association. Address configuration follows. Next MN receives/sends data packets using the LMA closest to the link MN is attached from MAG Data Plane function.

When MN moves MN does handover signaling with the control plane function which MAG control plane function updates the binding cache based on this move. MAG control plane function informs the MAG data plane function of this binding cache update and then MN starts to receive and send data to the new data plane function. MN MUST keep MAG control plane function address which is the same in the domain for all MNs in its cache.

When MN boots, it goes through authentication and security association establishment. Next MAG control plane function sends a proxy binding update to the LMA. MAG control plane function sends Proxy Binding Update message to the LMA and receives a Proxy Binding Acknowledgement message and in this message MAG control plane function MUST receive (possibly new) LMA address.

LMA address can be provided to MAG control plane function in Alternate Home Agent Tunnel Address option defined in [I-D.perkins-netext-hatunaddr] of PBA message [RFC5213]. MAG control plane function passes the LMA address to MAG data plane function. When MAG data plane function receives data packets from MN, it encapsulates the packets and sends them to Alternate Home Agent Tunnel Address. Also when packets are received from Alternate Home Agent Tunnel Address MAG data plane function decapsulates the packet and then send it to the MN.

Alternate Home Agent Tunnel Address option in Proxy Mobile IPv6 is much less useful because MAG data plane function could be preconfigured with the LMA address value that happens to be topologically closest LMA.

6. Security Considerations

TBD.

7. IANA Considerations

TBD.

8. Acknowledgements

TBD.

9. References

9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC2136] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
- [RFC5026] Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.
- [RFC5555] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.
- [RFC5648] Wakikawa, R., Devarapalli, V., Tsirtsis, G., Ernst, T., and K. Nagami, "Multiple Care-of Addresses Registration", RFC 5648, October 2009.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.
- [I-D.ietf-netext-pmipv6-flowmob] Bernardos, C., "Proxy Mobile IPv6 Extensions to Support Flow Mobility", draft-ietf-netext-pmipv6-flowmob-04 (work in progress), July 2012.
- [RFC6089] Tsirtsis, G., Soliman, H., Montavont, N., Giaretta, G., and K. Kuladinithi, "Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support", RFC 6089, January 2011.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC4877] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.

- [RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, January 2006.

9.2. Informative references

- [I-D.ietf-dmm-requirements]
Chan, A., "Requirements for Distributed Mobility Management", draft-ietf-dmm-requirements-02 (work in progress), September 2012.
- [I-D.rekhter-nvo3-vm-mobility-issues]
Rekhter, Y., Henderickx, W., Shekhar, R., Fang, L., Dunbar, L., and A. Sajassi, "Network-related VM Mobility Issues", draft-rekhter-nvo3-vm-mobility-issues-03 (work in progress), October 2012.
- [I-D.perkins-netext-hatunaddr]
Perkins, C., "Alternate Tunnel Source Address for LMA and Home Agent", draft-perkins-netext-hatunaddr-00 (work in progress), May 2012.

Author's Address

Behcet Sarikaya
Huawei USA
5340 Legacy Dr. Building 175
Plano, TX 75074

Phone: +1 469 277 5839
Email: sarikaya@ieee.org

Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 10, 2014

P. Seite
P. Bertin
France Telecom - Orange
JH. Lee
Telecom Bretagne
February 6, 2014

Distributed Mobility Anchoring
draft-seite-dmm-dma-07.txt

Abstract

Most existing IP mobility solutions are derived from Mobile IP principles where a given mobility anchor maintains Mobile Nodes (MNs) binding up-to-date. Data traffic is then encapsulated between the mobility anchor and the MN or its Access Router. These approaches are usually implemented on a centralised architectures where both MN context and traffic encapsulation need to be processed at a central network entity, i.e. the mobility anchor. However, one of the trend in mobile network evolution is to "flatten" mobility architecture by confining mobility support in the access network, e.g. at the access routers level, keeping the rest of the network unaware of the mobility events and their support. This document discusses the deployment of legacy Proxy Mobile IP approach in such a flat architecture. The solution allows to dynamically distribute mobility functions among access routers for an optimal routing management. The goal is also to dynamically adapt the mobility support of the MN's needs by applying traffic redirection only to MNs' flows when an IP handover occurs.

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 August 10, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Terminology	3
2. Introduction	3
3. Basics of Distributed Mobility Management	5
3.1. Fundamentals	5
3.2. Considerations on Client based mobility management	6
3.3. Considerations on Network based mobility management	8
4. Solution Overview for network based DMM	8
4.1. Distributed and Dynamic Mobility Anchoring	8
4.2. Protocol sequence for handover management	11
4.3. Multiple Interfaces support	12
5. Difference with Proxy Mobile IPv6	14
6. Security Considerations	14
7. IANA Considerations	14
8. Acknowledgements	14
9. References	15
9.1. Normative References	15
9.2. Informative References	15
Authors' Addresses	15

1. Terminology

Proxy Mobile IPv6 inherited terminology

The following terms used in this document are to be interpreted as defined in the Proxy Mobile IPv6 specification [RFC5213]: Mobile Node (MN), home Network Prefix (HNP), Mobile Node Identifier (MN-Identifier), Proxy Binding Update (PBU), and Proxy Binding Acknowledgement (PBA).

Mobility capable Access Router (MAR)

The Mobility capable Access Router is an access router which provides mobility management functions. It has both mobility anchoring and location update functional capabilities. A Mobility capable Access Router can act as a Home or as a Visited Mobility capable Access Router (respectively H-MAR and V-MAR). Any given MAR could act both as H-MAR and V-MAR for a given mobile node having different HNPs, either allocated by this MAR (H-MAR role) or another MAR on which the mobile node was previously attached (V-MAR role).

- * H-MAR: it allocates HNP for mobile nodes. Similarly to [RFC5213], the H-MAR is the topological anchor point for the mobile node's home network prefix(es) it has allocated. The H-MAR acts as a regular IPv6 router for HNPs it has allocated, and when a mobile node has moved away and attached to a V-MAR, the H-MAR is responsible for: tracking the mobile node location (i.e. the V-MAR where the mobile node is currently attached), and forwarding packets to the V-MAR where the mobile node is attached.
- * V-MAR: it manages the mobility-related signaling for a mobile node, using a HNP allocated by a MAR previously visited by the mobile node, that is attached to its access link.

2. Introduction

Most existing IP mobility solutions are derived from Mobile IP [RFC3775] principles where a given mobility agent (e.g. the Home Agent (HA) in Mobile IP or the Local Mobility Agent (LMA) in Proxy Mobile IPv6 [RFC5213]) maintains Mobile Nodes (MNs) bindings. Data traffic is then encapsulated between the MN or its Access Router (e.g. the Mobile Access Gateway (MAG) in PMIPv6) and its mobility agent. In other words, these approaches rely on a centralised architecture where both MN mobility context and traffic encapsulation features need to be maintained at a central network entity, the mobility agent. Such centralised approach provides the ability to

route MN traffic whatever its localisation is, as well as to support handovers when it moves from access router to access router; however, when millions of MNs are communicating in a given cellular network, such a centralised network entity may cause bottlenecks and single point of failure issues, which requires costly network dimensioning and engineering to be fixed. In addition, tunnelling encapsulations impact the global network efficiency since they require the maintenance of MN's specific contexts in each tunnel end nodes and they incur delays in packet processing and transport functions. Besides, centralized mobility management might not take into account current network evolution where the trend is to cache and distribute content (e.g. CDN architecture) closer to the end-user. As a consequence, alternative mobility approaches are currently being discussed and a potential solution is the distribution of mobility anchors, as stated by requirement "REQ1" in [I-D.ietf-dmm-requirements].

Moreover, it is well established that a huge amount of mobile communications are set up while the MN remains attached to the same access router. For example, the user is being communicating at home, in his office, at a cafe, etc. and the mobility support is thus not required. Applying the aforementioned centralised principles leads then to maintain user's mobility contexts, whereas the MN remains motionless. So, to avoid such a waste of resources, mobility management should come into play only when the mobile node changes the point of attachment (i.e. performs a handover) and when it needs the conservation of the current IP address. Actually, this is the requirement "REQ2" from [I-D.ietf-dmm-requirements].

The DMM working group has been chartered to address above issues by exploring the distribution of mobility management functions and, for the sake of pragmatism, it has been agreed to firstly focus on existing mobility protocols. The goal of this document is to address this concern and, thus, has no other ambition than to discuss the use of legacy IP mobility protocols in distributed anchoring architecture. Besides, it must be noted this document aims only to meet basic [I-D.ietf-dmm-requirements] requirements, namely:

- o confining the mobility support at the access routers level, keeping the rest of the network unaware of mobility events and their support (REQ1);
- o dynamically adapting mobility support to each of the MN's needs by applying traffic redirection only to MNs' flows that are already established when an IP handover occurs (REQ2).

3. Basics of Distributed Mobility Management

3.1. Fundamentals

As stated in [I-D.ietf-dmm-requirements], mobility anchoring may be distributed to multiple locations in the access network. For example, mobility anchoring (MA) function could be co-located with the access router (AR) as shown on Figure 1. This architecture allows the traffic to be anchored closer to the mobile node and, for example, to provide optimal mobility support to distributed content (e.g. CDN based delivery architecture).

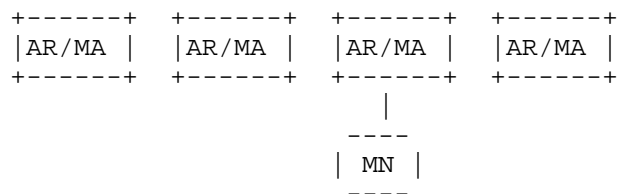


Figure 1: Distributed Mobility Management

Mobility management may be partially distributed, i.e. only the data plane is distributed, or fully distributed, i.e. both the data plane and control plane are distributed [I-D.yokota-dmm-scenario]. If conceptual differences exist, these two approaches share common fundamentals and it is possible to describe the generic behavior of a DMM deployment. Note that the following focuses only on the two first requirements of [I-D.ietf-dmm-requirements] (i.e. distribution of mobile anchoring and dynamic mobility management)

In a standard IPv6 network without specific mobility support, any host is able to set up communications flows using a global IPv6 address acquired with the support of its current access router [RFC4862]. When the host moves from this access router to a new one, its ongoing IP sessions cannot be maintained without leveraging on IP mobility mechanisms. However, once attached to the new access router, the host can again acquire a routable global IPv6 address to be used for any new communication flow it sets up. Hence, a flow based mobility support may be restricted to provide traffic indirection to host's flows that are already ongoing during host's handovers between access routers. Any new flow being set up uses the new host's global address acquired on the new link available after the handover.

When a multiple-interface host moves between access routers of different access technologies, such a simple approach can also be applied, considering that each network interface provides dynamically global IPv6 addresses acquired on current access routers.

Hence, any given IP flow can be considered as implicitly anchored on the current MN's access router when being set up. Meaning that, if the MN moves across more than one access router and initiates IP communications while being attached to different access routers, the MN might be served simultaneously by more than one mobility anchor. While the MN is attached to its initial access router, the IP flow is delivered as for any standard IPv6 node. The anchoring function at the access router is thus needed only to manage traffic indirection if the MN moves to a new access router and for subsequent movements while the IP flow remains active), maintaining the flow communication until it ends up.

Any packet sent to the MN is routed in a standard way to the access router anchoring the flow as the packet contains the destination IP address issued from router prefix. Then, if the MN is currently attached to the initial anchor access router, the incoming packet is directly delivered over the access link. Otherwise, the anchoring access router needs to redirect the packet to the current (or one of the current) MN's access router(s).

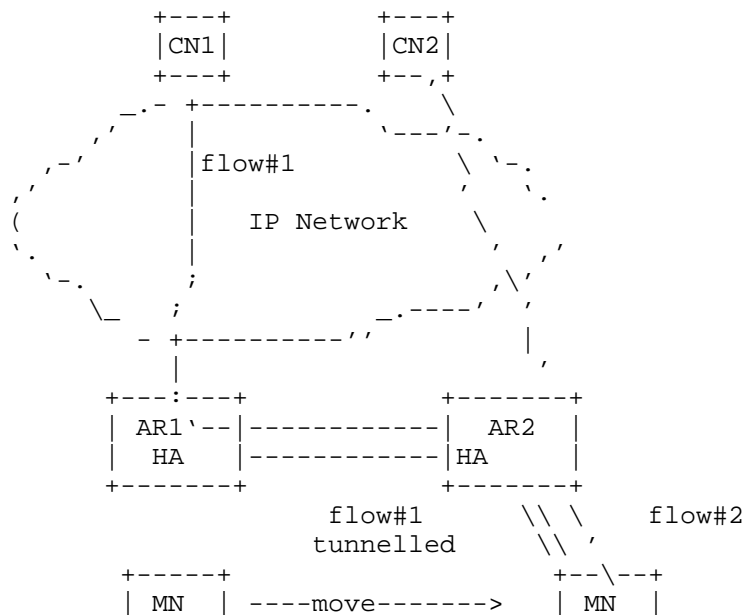
Any outgoing packet from the MN is sent over either the initial anchor access router link or another access router link it is currently using. In the first case, the packet can be routed in a standard way, i.e., without requiring network mobility support functions. In the second case, we consider its redirection to the initial flows' anchor router, but it may be noticed that direct routing by the current access router may be also allowed (yet this may lead to more stringent security and policy considerations).

3.2. Considerations on Client based mobility management

Actually, there is no issue to implement a basic DMM (as described in previous section) with vanilla Mobile IP protocol, e.g. [RFC3775], as long as the MN can manage simultaneously different bindings to different Home Agents (HA), i.e. manage simultaneously more than one tunnel to the mobile anchors. Basically, nothing prevents to implement the HA functionalities in the access routers, so that any given IP flow can be considered as implicitly anchored on the current host's access router when set up. The anchoring function at the access router is acting only to manage traffic indirection while the host moves to a new access router. When the MN moves to a new access router, the MN implicitly considers the previous access router as the HA for IP addresses allocated by this access router. Then, the MN

can perform the binding update to the previous access router for IP session initiated on it. So, MN's current traffic remains attached to the previous access router which is responsible for forwarding the IP flows to the MN.

Figure 2 illustrates the use of Mobile IP in a distributed architecture. For example, let's consider an IP flow, flow#1, initiated by the mobile node, MN, when attached to AR1. Flow#1 is routed in a standard way as long as the MN remains attached to AR1. If the MN moves to AR2, the MN proceeds to the binding update to AR1, which plays the role of HA, so that flow#1 remains anchored to AR1. The home address is the IP address obtained from AR1 and the Care-of-Address is the IP address obtained from AR2. If MN starts a new IP communication, flow#2, while attached to AR2; flow#2 is routed in a standard way as long as the MN remains attached to AR2. In this situation, applications can use either the Home Address or the Care-of-Address and the IP stack is supposed to make the source address selection depending on the need for mobility support; in the example of Figure 2, the Home Address shall be used as the source address for flow#1 and the Care-of-Addresses for flow#2. Then, if the MN moves to another access router, flow#1 and flow#2 will be respectively anchored to AR1/HA and AR2/HA. Mobile IP resources (mobility context and tunneling in both ARx/HA and MN) are released after IP communication stopped.



+-----+

+-----+

Figure 2: Distributed Client Based Mobility

3.3. Considerations on Network based mobility management

It is also possible to go for DMM with Proxy Mobile IPv6 [RFC5213]. For example, mobility functions, i.e. MAG and LMA, can be co-located with the access routers. The anchoring behavior might be similar to the client based solution; however there is an issue with the binding update management. In a network based solution, the MN is not supposed to participate to mobility signalling and the MAG is expected to know the mobility anchor serving the MN. This problem can be tricky in distributed mobility architecture because 1) the MN can be served by more than one LMA (see fundamentals in Section 3.1) and 2) the mobility anchor depends on point of attachment when the IP communication has been initiated. There are basically two ways to address the issue without modifying proxy mobile IP:

1. Involve the MN in the mobility management process: during the attachment process to a new access router, the MN could communicate its ongoing mobility sessions (i.e. list of current HNP with associated mobility anchors) to the MAG. For example, this information could be provided in a dedicated router solicitation option.
2. Rely on centralized part of the control plane: when the MN attaches to a new access router, the MAG function retrieves the mobility sessions, for that MN, from a centralized database. This database is expected to be updated each time a new prefix is allocated to the MN, and also when the prefix is released.

Even if the first option does not introduce a new piece of protocol, it can be seen as a violation of the basic of the network based mobility approach where the MN must remain agnostic of the mobility support. So, this document only goes for the second option.

4. Solution Overview for network based DMM

4.1. Distributed and Dynamic Mobility Anchoring

The basic idea is to distribute mobility traffic management with dynamic user's traffic anchoring in access network nodes. The solution relies on a very simple flat architecture outlined in Figure 3 where the Mobility capable Access Router (MAR) supports both traffic anchoring and MN's location management functionalities. The

architecture relies on a centralized database storing ongoing mobility sessions for the MNs (see Section 4.2 for details). This database stores the HNPs currently allocated to the MN and their respective anchoring point. This database is typically the PMIPv6 policy store [RFC5213]. However, the detailed specification of the interaction between MAGs and this database is currently out of the scope of this document.

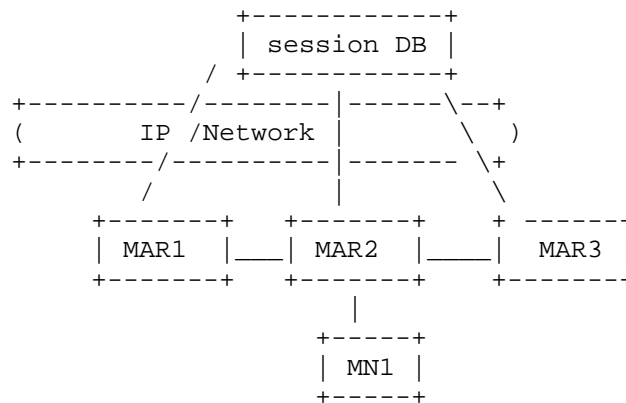


Figure 3: Architecture for Distributed Mobility Anchoring

Regular IPv6 routing applies when an IP communication is initiated. For instance, if the mobile node (e.g. MN1), being attached to MAR1, initiates a communication: flow#1; the traffic will be routed through MAR1 without requiring any specific mobility operation. When MN1 moves away from MAR1 and attaches to MAR2, the traffic remains anchored to MAR1 and is tunnelled between MAR1 and MAR2. MAR1 becomes the mobility anchor, for IP sessions initiated by MN1 when it was attached to MAR1, and MAR2 plays the role of MAG for these sessions.

Communications newly initiated, e.g. flow#2, while the mobile node is attached to MAR2 will be routed in a standard way via MAR2. But, if the mobile node moves away from MAR2 (e.g. attaches to MAR3), while maintaining both flow#1 and flow#2, two mobility anchors come into play: flow#1 and flow#2 will be respectively anchored in MAR1 and MAR2.

Summarizing, it is proposed to dynamically locate mobility anchoring depending on where the flow is initially created. Accordingly,

communications are expected to be initiated without requiring mobility anchoring and tunnelling. Note that, even if a mobile node is moving across several MARs, the tunnel endpoints are always on the initial H-MAR and on the current V-MAR. In the case the mobile node moves from MAR1 to MAR2 then to MAR3, a tunnel will be firstly established between MAR1 and MAR2; then the tunnel will be moved between MAR1 and MAR3.

However such architecture leads to new requirement on the HNP prefix model. Actually, because the HNP is anchored to its mobility anchor (i.e. H-MAR), a dynamic mobility anchoring requires that each MAR must advertise different per-MN prefixes set.

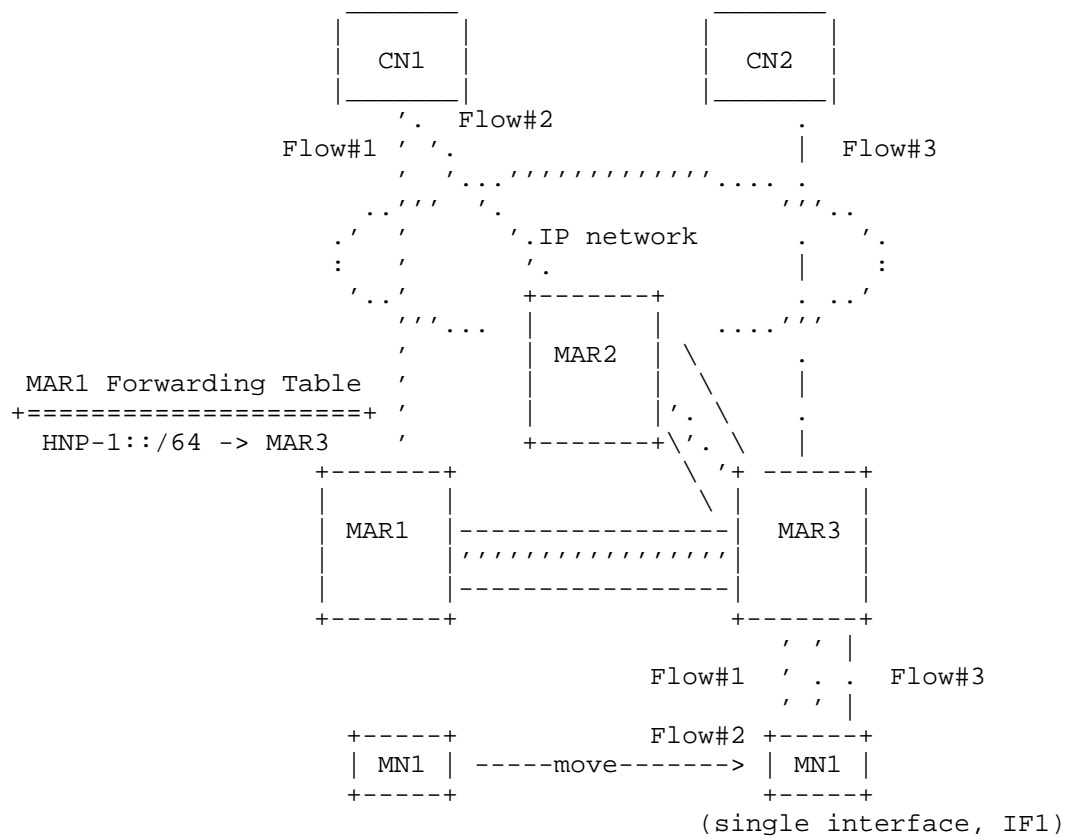


Figure 4: Distributed Mobility Anchoring

4.2. Protocol sequence for handover management

Handover management for a single interface mobile node is depicted on Figure 5 where the mobile node, MN1, is assumed to move from MAR1 to MAR2.

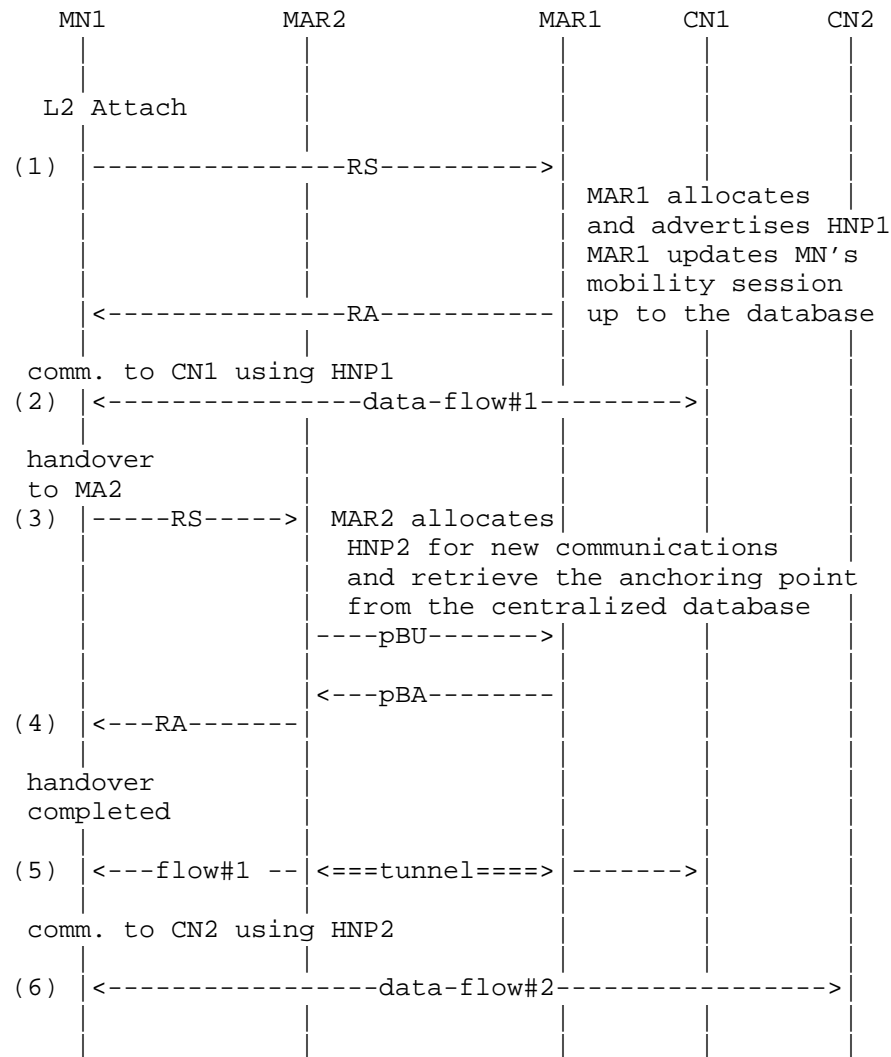


Figure 5: Handover management with Distributed Mobility Anchoring

Following are the main steps of the handover management process:

1. The mobile node, MN1, attaches to MAR1 which is responsible for allocating the MN-HNP, e.g. HNP1 for MN1.
2. Hence, the mobile node can initiate and maintain data transport sessions (with CN1 in the picture), using IP addresses derived from HNP1, in a standard way while it remains attached to MAR1, i.e. mobility functions do not come into play.
3. The MN attaches to MAR2 which will thus acts as V-MAR for HNP1. Firstly, MAR2 retrieves the ongoing MN's mobility sessions from the centralized sessions database; here only one mobility session is ongoing: (MN::HNP1,MAR1). Then MAR2 proceeds to location update for HNP1 with MAR1, which plays the LMA role, i.e., PBU/PBA exchange between MAR2 and MAR1. MAR2 also allocates new prefix (HNP2) for MN1; this prefix is meant to be used by application flows initiated after the handover.
4. In response to MN's router solicitation, MAR2 is expected to advertise both HNP1 and HNP2 to the MN, for respectively, the IP communications initiated when the MN was attached to MAR1 and the IP communications which will be initiated while attached to MAR2. An IP address derived from HNP1 must not be used for new IP communications; so, prefix HNP1 is announced as deprecated. The MN could also make the prefix selection relying on prefix properties [I-D.korhonen-dmm-prefix-properties] if supported.
5. MAR1, playing the LMA role for HNP1, encapsulates MN1's traffic and tunnels it to the V-MAR, i.e. MAR2, where packets are decapsulated and delivered to the MN.
6. The mobile node initiates and maintains new data transport sessions, e.g. with CN2, using IP addresses derived from HNP2. This traffic is routed in a standard way while the mobile node remains attached to MAR2.

4.3. Multiple Interfaces support

The distribution of mobility functions can also apply in the context of multiple-interfaces terminals. In such a case, any given IP flow can be considered as implicitly anchored on the current host's access router when set up. Until the host does not move from the initial access router (H-MAR), the IP flow is delivered as for any standard IPv6 node. The anchoring function at the H-MAR is thus managing traffic indirection only if one, or several, IP flow(s) are moved to another interface, and for subsequent movements while the initial anchored flows remain active. This anchoring is performed on a per-flow basis and each H-MAR needs to track all possible V-MARs for a given host on the move. The H-MAR must also manage different tunnels for a given mobile node providing that the node is multihomed and it

simultaneously processes different IP flows on its interfaces.

Lets consider a simple example to illustrate the dynamic per-flow mobility anchoring. Figure 6 depicts the IP flow mobility management for a mobile node with two interfaces. The IP data flows, Flow#1 and Flow#2, have been initiated on if1. Thus, Flow#1 and Flow#2, using respectively prefixes HNP1 and HNP2, are anchored to MAR1. Referring to the picture, Flow#1 has not been moved; so Flow#1 is delivered in a standard IPv6 way. Flow#2 has been transferred from If1 to If2, so Flow#2 packets, corresponding to HNP2, are tunnelled from MAR1 to MAR2. In other words, MAR1 and MAR2 are respectively the H-MAR anchor and the V-MAR for flow#2.

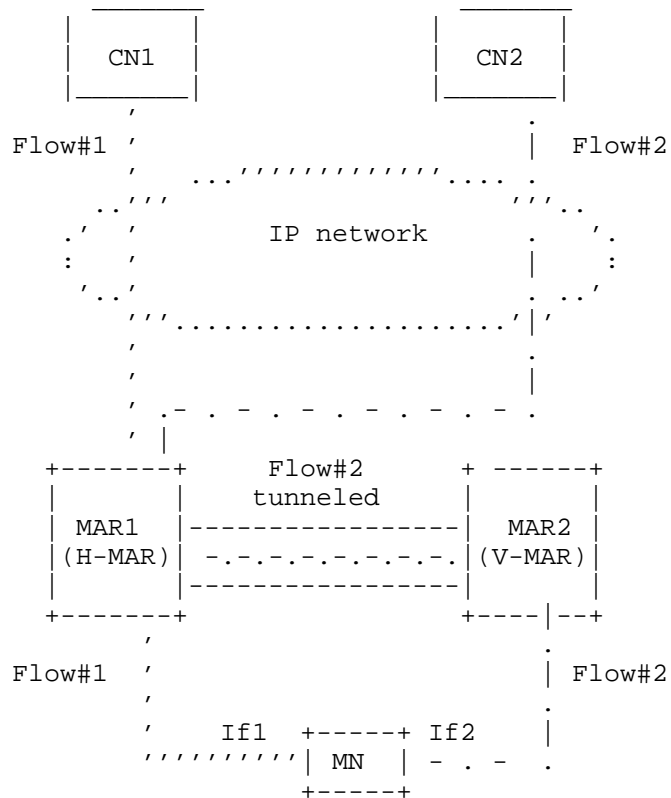


Figure 6: Distributed IF flow Mobility Anchoring

In case of the handover of an IP flow between interfaces, the mobile

node must rely on the logical interface support, as per [I-D.ietf-netext-logical-interface-support].

5. Difference with Proxy Mobile IPv6

The DMM solution that described in this document can be implemented with current Proxy Mobile IPv6 protocol [RFC5213]; neither protocol operations nor messages semantic are changed. The session database, used in this document, is a remote policy store, as defined in [RFC5213]. However, in [RFC5213], the mobile node's IPv6 home network prefix(es) assigned to the mobile node is an optional field of the policy store; now, with distribution of mobility anchors, this field becomes mandatory.

So, the mandatory fields of the policy profile are now:

- o The mobile node's identifier (MN-Identifier)
- o The IPv6 address of the local mobility anchor (LMAA)
- o The mobile node's IPv6 home network prefix(es) assigned to the mobile node's connected interface.

6. Security Considerations

TBD.

7. IANA Considerations

This document has no actions for IANA.

8. Acknowledgements

The authors would also like to express their gratitude to Hidetoshi Yokota, Telemaco Melia, Dapeng Liu, Anthony Chan, Julien Laganier, Lucian Suci and many others for having shared thoughts on the concept of distributed mobility.

This document inherits from concepts introduced in [NTMS2008], co-signed by Philippe Bertin, Servane Bonjour, Jean-Marie Bonnin, Karine Guillouard.

9. References

9.1. Normative References

- [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

9.2. Informative References

- [I-D.ietf-dmm-requirements]
Chan, A., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", draft-ietf-dmm-requirements-14 (work in progress), February 2014.
- [I-D.ietf-netext-logical-interface-support]
Melia, T. and S. Gundavelli, "Logical Interface Support for multi-mode IP Hosts", draft-ietf-netext-logical-interface-support-08 (work in progress), October 2013.
- [I-D.korhonen-dmm-prefix-properties]
Korhonen, J., Patil, B., Gundavelli, S., Seite, P., and D. Liu, "IPv6 Prefix Mobility Management Properties", draft-korhonen-dmm-prefix-properties-03 (work in progress), October 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.
- [NTMS2008]
Bertin, P., "A Distributed Dynamic Mobility Management Scheme designed for Flat IP Architectures.", NTMS'2008 , November 2008.

Authors' Addresses

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

Email: pierrick.seite@orange.com

Philippe Bertin
France Telecom - Orange
4, rue du Clos Courtel, BP 91226
Cesson-Sevigne 35512
France

Email: philippe.bertin@orange.com

Jong-Hyouk Lee
Telecom Bretagne
2, rue de la Chataigneraie
Cesson-Sevigne 35512
France

Email: jh.lee@telecom-bretagne.eu

DMM WG
Internet-Draft
Intended status: Informational
Expires: June 22, 2013

JC. Zuniga
InterDigital
CJ. Bernardos
UC3M
T. Melia
Alcatel-Lucent
C. Perkins
Futurewei
December 19, 2012

Mobility Practices and DMM Gap Analysis
draft-zuniga-dmm-gap-analysis-03

Abstract

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

The practices description and gap analysis are performed for IP-based mobility protocols, dividing them into three main families: IP client-based, IP network-based, and 3GPP mobility solutions.

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 22, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal

Provisions Relating to IETF Documents
 (<http://trustee.ietf.org/license-info>) in effect on the date of
 publication of this document. Please review these documents
 carefully, as they describe your rights and restrictions with respect
 to this document. Code Components extracted from this document must
 include Simplified BSD License text as described in Section 4.e of
 the Trust Legal Provisions and are provided without warranty as
 described in the Simplified BSD License.

Table of Contents

1. Introduction	4
2. Practices: deployment of existing solutions in a DMM fashion	4
2.1. Client-based IP mobility	4
2.1.1. Mobile IPv6 / NEMO	5
2.1.2. Mobile IPv6 Route Optimization	6
2.1.3. Hierarchical Mobile IPv6	7
2.1.4. Home Agent switch	8
2.1.5. IP Flow Mobility	8
2.1.6. Source Address Selection	8
2.2. Network-based IP mobility	9
2.2.1. Proxy Mobile IPv6	9
2.2.2. Local Routing	10
2.2.3. LMA runtime assignment	10
2.2.4. Source Address Selection	11
2.2.5. Multihoming in PMIPv6	11
2.3. 3GPP mobility	11
2.3.1. GPRS Tunnelling Protocol (GTP) and DSMIPv6	12
2.3.2. Local IP Access and Selected IP Traffic Offload (LIPA-SIPTO)	13
2.3.3. LIPA Mobility and SIPTO at the Local Network (LIMONET)	13
2.3.4. Data IDentification in ANDSF (DIDA) and Operator Policies for IP Interface Selection (OPIIS)	13
2.3.5. Multi-Access PDN Connectivity (MAPCON)	14
3. Gap Analysis: limitations in current practices	14
3.1. Client-based IP mobility	14
3.1.1. REQ1: Distributed deployment	14
3.1.2. REQ2: Transparency to Upper Layers when needed	15
3.1.3. REQ3: IPv6 deployment	16
3.1.4. REQ4: Existing mobility protocols	16
3.1.5. REQ5: Compatibility	17
3.1.6. REQ6: Security considerations	17
3.2. Network-based IP mobility	18
3.2.1. REQ1: Distributed deployment	18
3.2.2. REQ2: Transparency to Upper Layers when needed	19

3.2.3.	REQ3: IPv6 deployment	20
3.2.4.	REQ4: Existing mobility protocols	20
3.2.5.	REQ5: Compatibility	20
3.2.6.	REQ6: Security considerations	21
3.3.	3GPP mobility	21
3.3.1.	REQ1: Distributed deployment	21
3.3.2.	REQ2: Transparency to Upper Layers when needed	21
3.3.3.	REQ3: IPv6 deployment	21
3.3.4.	REQ4: Existing mobility protocols	21
3.3.5.	REQ5: Compatibility	22
3.3.6.	REQ6: Security considerations	22
4.	Conclusions	22
4.1.	Independent solution analysis	22
4.2.	Functional analysis	23
4.2.1.	Multiple anchoring	23
4.2.2.	Dynamic anchor assignment	24
4.2.3.	Multiple address management	25
4.3.	Combined solutions analysis	26
5.	IANA Considerations	27
6.	Security Considerations	27
7.	References	27
7.1.	Normative References	27
7.2.	Informative References	28
Appendix A.	Acknowledgments	30
Authors' Addresses	30

1. Introduction

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

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

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

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

This section documents practices for the deployment of existing mobility protocols in a distributed mobility management (DMM) fashion. The scope is limited to existing IPv6-based and 3GPP mobility protocols, such as Mobile IPv6 [RFC6275], NEMO Basic Support Protocol [RFC3963], Proxy Mobile IPv6 [RFC5213], 3GPP GPRS Tunneling Protocol, and protocol extensions, such as Hierarchical Mobile IPv6 [RFC5380], Mobile IPv6 Fast Handovers [RFC5568], Localized Routing for Proxy Mobile IPv6 [RFC6705], or 3GPP Selective IP Traffic Offload (SIPTO), among others [RFC6301].

The section is divided in three parts: IP client-based mobility, IP network-based mobility and 3GPP mobility solutions.

2.1. Client-based IP mobility

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

2.1.1.1. Mobile IPv6 / NEMO

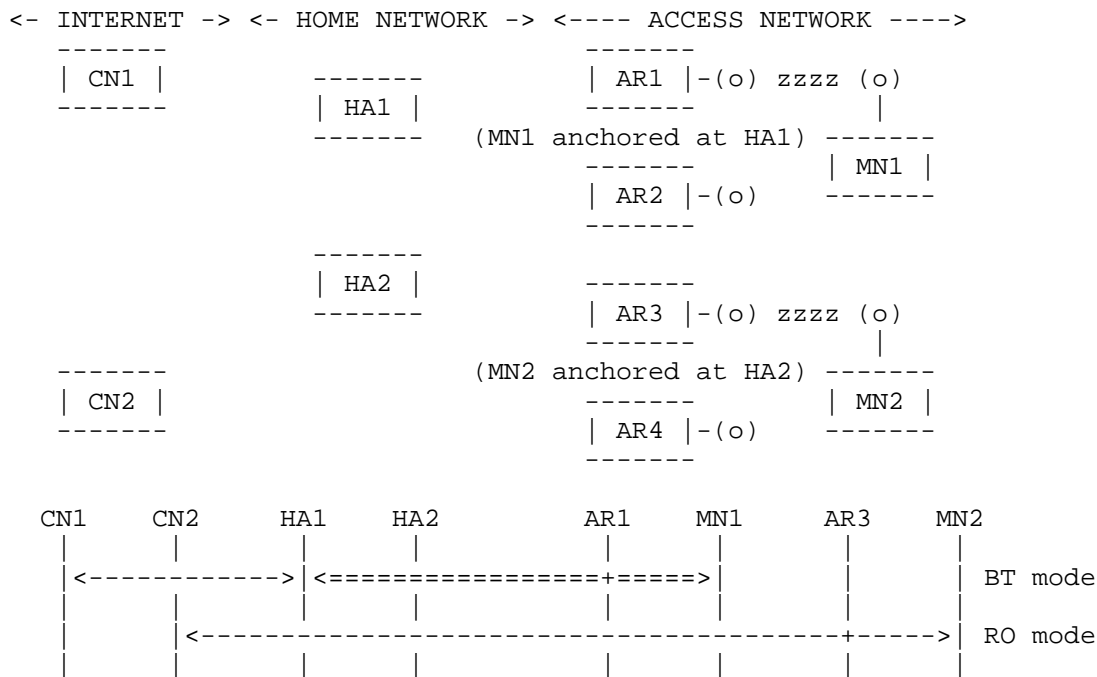


Figure 1: Distributed operation of Mobile IPv6 (BT and RO) / NEMO

Due to the heavy dependence on the home agent role, the base Mobile IPv6 and NEMO protocols (i.e., without additional extensions) cannot be easily deployed in a distributed fashion. One approach to distribute the anchors can be to deploy several HAs (as shown in Figure 1), and assign to each MN the one closest to its topological location [RFC4640], [RFC5026], [RFC6611]. In the example shown in Figure 1, MN1 is assigned HA1 (and a home address anchored by HA1), while MN2 is assigned HA2. Note that current Mobile IPv6 / NEMO specifications do not allow the simultaneous use of multiple home agents by a single mobile node instance, and therefore the benefits of this deployment model shown here are limited (unless multiple MIPv6 MN instances are run in parallel, each of them associated to a different HA). For example, if MN1 moves and attaches to AR3, the path followed by data packets would be suboptimal, as they have to traverse HA1, which is no longer close to the topological attachment point of MN1.

2.1.1.2. Mobile IPv6 Route Optimization

One of the main goals of DMM is to avoid the suboptimal routing caused by centralized anchoring. By default, Mobile IPv6 and NEMO 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. Mobile IPv6 also specifies the Route Optimization (RO) mode, which allows the MN to update its current location on the CNs, and then use the direct path between them. Using the example shown in Figure 1, MN1 is using BT mode with CN2 and MN2 is in RO mode with CN1. However, the RO mode has several drawbacks:

- o The RO mode is only supported by Mobile IPv6. There is no route optimization support standardized for the NEMO protocol, although many different solutions have been proposed.
- o The RO mode requires additional signaling, which adds some protocol overhead.
- o The signaling required to enable RO involves the home agent, and it is repeated periodically because of security reasons [RFC4225]. This basically means that the HA remains as single point of failure, because the Mobile IPv6 RO mode does not mean HA-less operation.
- o The RO mode requires additional support on the correspondent node (CN).

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 on the relevant correspondent nodes.

2.1.3. Hierarchical Mobile IPv6

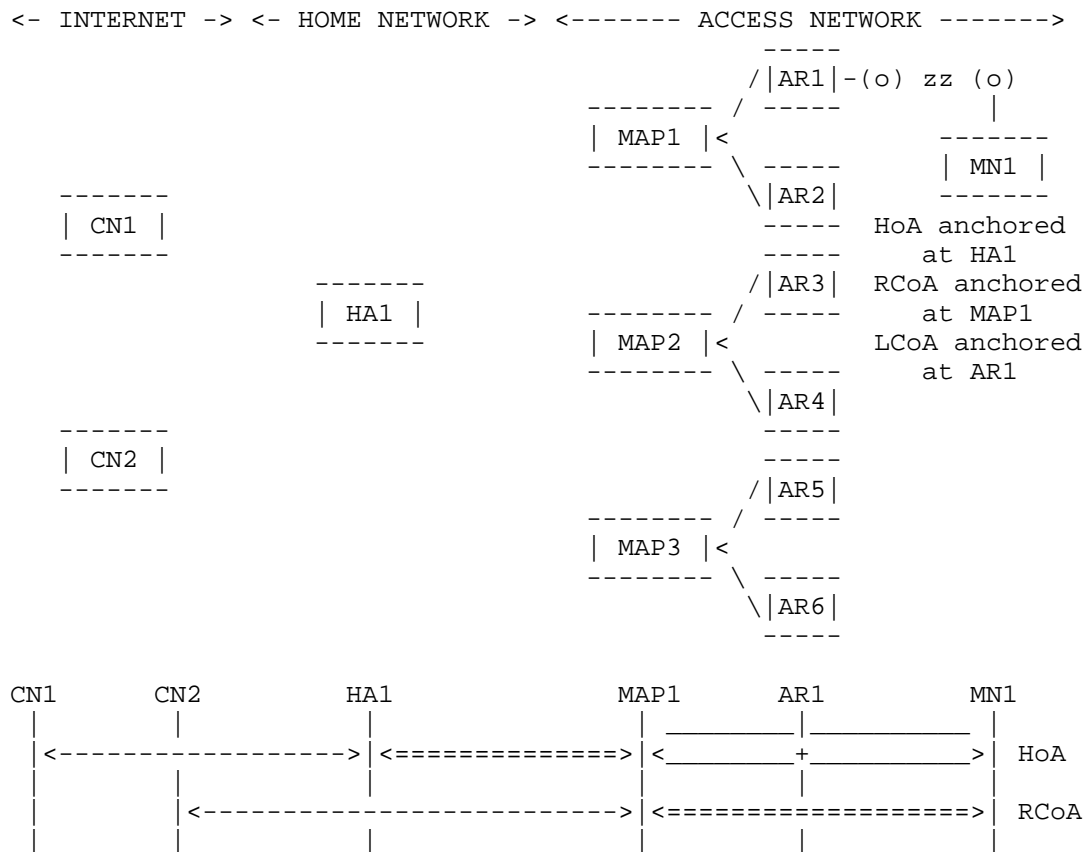


Figure 2: Hierarchical Mobile IPv6

Hierarchical Mobile IPv6 (HMIPv6) [RFC5380] allows reducing 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.

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

The use of HMIPv6 allows some route optimization, as a mobile node may decide to directly use the RCoA as source address for a communication with a given correspondent node, notably if the MN does not expect to move outside the local domain during the lifetime of the communication. This can be seen as a potential DMM mode of operation. In the example shown in Figure 2, MN1 is using its global HoA to communicate with CN1, while it is using its RCoA to communicate with CN2.

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

2.1.4. Home Agent switch

The Home Agent switch specification [RFC5142] defines a new mobility header for signaling a mobile node that it should acquire a new home agent. Although the purposes of this specification do not include the case of changing the mobile node's home address, as that might imply loss of connectivity for ongoing persistent connections, it 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.

2.1.5. IP Flow Mobility

There are different specifications meant to support IP Flow Mobility (IFOM) with Mobile IPv6, namely the multiple care-of address registration [RFC5648], the flow bindings in Mobile IPv6 and NEMO [RFC6089] and the traffic selectors for flow bindings [RFC6088]. The use of these extensions allows a mobile node to associate different flows with different care-of addresses that the mobile owns at a given time. This could also be used, combined with the route optimization support, to improve the paths followed by data packets, avoiding the traversal of the core network for selected flows.

2.1.6. Source Address Selection

The IPv6 socket API for source address selection [RFC5014], [RFC6724] can be used by an application running on a mobile node to express its preference of using a home address or a care-of address in a given connection. This allows, for example, an application which can survive an IP address change to always prefer the use of a care-of

address. Similarly, and as mentioned in [RFC6275], a mobile node can also prefer the use of a care-of address for sessions that are going to finish before the mobile node hands off to a different attachment point (e.g., short-lived connections like DNS dialogs). This could be based on user or operator policies, and it is typically performed by a connection manager (e.g., [I-D.seite-mif-cm]).

2.2. Network-based IP mobility

Proxy Mobile IPv6 (PMIPv6) [RFC5213] is the main network-based IP mobility protocol specified for IPv6. Architecturally, PMIPv6 is similar to MIPv6, as it relies on the function of the Local Mobility Anchor (LMA) to provide mobile nodes with mobility support, without requiring the involvement of the mobile nodes. The required functionality at the mobile node is provided in a proxy manner by the Mobile Access Gateway (MAG). We next describe how network-based mobility protocols and several additional extensions can be deployed to meet some of the DMM requirements [I-D.ietf-dmm-requirements].

2.2.1. Proxy Mobile IPv6

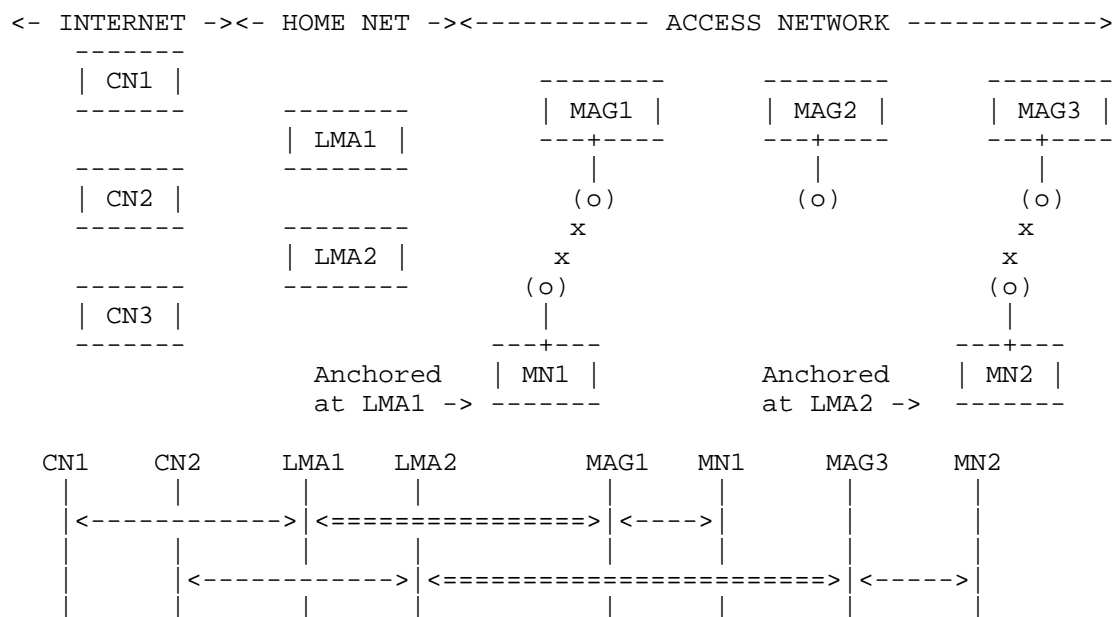


Figure 3: Distributed operation of Proxy Mobile IPv6

As with Mobile IPv6, plain Proxy Mobile IPv6 operation cannot be easily decentralized, as in this case there also exists a single network anchor point. One simple but still suboptimal approach,

would be to deploy several local mobility anchors and use a topological position-based assignment to attach mobile nodes (an example of this type of assignment is shown in Figure 3. This assignment can be static or dynamic (as described in Section 2.2.3). The main advantage of this simple approach is that the IP address anchor (i.e., the LMA) is placed close to the mobile node, and therefore resulting paths are close-to-optimal. On the other hand, as soon as the mobile node moves, the resulting path starts to deviate from the optimal one.

2.2.2. Local Routing

[RFC6705] enables 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.

In the context of 3GPP, the closest analogy is the use of the X2 interface between two eNBs to directly exchange data traffic during handover procedures. 3GPP does not foresee the use of local routing at any other point of the network given the structure of the EPS bearer model.

2.2.3. LMA runtime assignment

[RFC6463] specifies a runtime local mobility anchor assignment functionality and corresponding mobility options for Proxy Mobile IPv6. This runtime local mobility anchor assignment takes place during 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 case when the mobile node does not have any session active, or when running sessions can survive an IP address change.

2.2.4. Source Address Selection

Also in the context of network-based mobility, the use of a source address selection API can be considered as means to achieve better routing (by using different anchors). For instance, an MN connected to a PMIPv6 domain could attach two different wireless network interfaces to two different MAGs, hence configuring a different set of HNPs on both interfaces (potentially combining both IPv4 and IPv6). Based on application requirements or operator's policies the connection manager logic could instruct the IP stack on the MN to route selected traffic on a specific wireless interface [I-D.seite-mif-cm]. It should be noted that source address selection mostly provides for better routing but not session continuity.

2.2.5. Multihoming in PMIPv6

PMIPv6 provides some multihoming support. RFC 5213 specifies that the LMA can maintain one mobility session per attached interface and that upon handover the full set of HNPs can be moved to another interface in case of inter-technology handover (MAGs providing different wireless access technology) or maintained on the same interface in case of intra-technology handover (MAGs providing the same wireless access technology). An MN can also attach two different interfaces to the same PMIPv6 domain (as described in Section 2.2.4), hence resulting in a multihomed device being able to send/receive traffic sequentially or simultaneously from both network interfaces. [I-D.ietf-netext-pmipv6-flowmob] extends the base RFC5213 capabilities so that a mobility session can be shared across two different access networks. It derives that a selected flow could be routed through different paths, hence achieving some sort of better routing. Yet all the traffic is anchored at centralized anchor points.

2.3. 3GPP mobility

Architecturally, the 3GPP Evolved Packet Core (EPC) network is also similar to PMIPv6 and MIPv6, as it relies on the Packet Data Gateway (PGW) anchoring services to provide mobile nodes with mobility support (see Figure 4). There are client-based and network-based mobility solutions in 3GPP, which for simplicity we will analyze together. We next describe how 3GPP mobility protocols and several additional completed or on-going extensions can be deployed to meet some of the DMM requirements. [I-D.ietf-dmm-requirements].

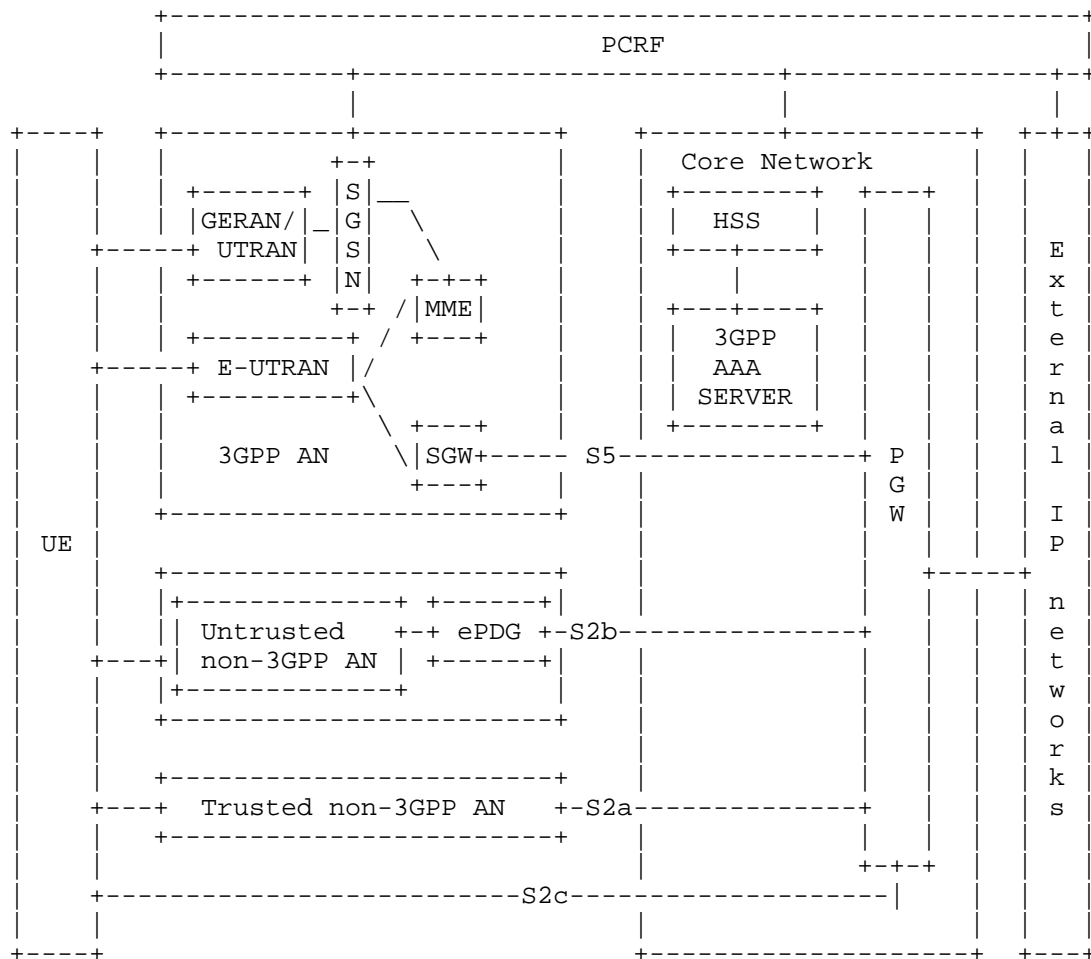


Figure 4: EPS (non-roaming) architecture overview

2.3.1. GPRS Tunnelling Protocol (GTP) and DSMIPv6

GPRS Tunnelling Protocol (GTP) [3GPP.29.060] is a network-based mobility protocol specified for 3GPP networks (S2a, S2b, S5 and S8 interfaces). Similar 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).

3GPP specifications also include client-based mobility support, based on adopting the use of Dual-Stack Mobile IPv6 (DSMIPv6) [RFC5555] for

the S2c interface. In this case, the UE implements the mobile node functionality, while the home agent role is played by the PGW.

2.3.2. Local IP Access and Selected IP Traffic Offload (LIPA-SIPTO)

A Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO) enabled network [3GPP.23.829] allows offloading some IP services at the local access network, above the Radio Access Network (RAN) or at the macro, without the need to traverse back to the PGW.

Similarly to the runtime local mobility anchor assignment described in Section 2.2.3, considerations have been discussed in 3GPP with respect to SIPTO. 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 is geographically/topologically close to the UE's point of attachment.

LIPA, on the other hand, enables an IP capable UE connected via a Home eNB (HeNB) to access other IP capable entities in the same residential/enterprise IP network without the user plane traversing the mobile operator's network core. In order to achieve this, a Local GW (L-GW) collocated with the HeNB is used. LIPA is established by the UE requesting a new 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.

2.3.3. LIPA Mobility and SIPTO at the Local Network (LIMONET)

Both SIPTO and LIPA have a very limited mobility support, specially in 3GPP specifications up to Rel-10. In Rel-11, there is currently a work item on LIPA Mobility and SIPTO at the Local Network (LIMONET) [3GPP.23.859] that is studying how to provide SIPTO and LIPA mechanisms with some additional, but still limited, mobility support. In a glimpse, LIPA mobility support is limited to handovers between HeNBs that are managed by the same L-GW (i.e., mobility within the local domain), while seamless SIPTO mobility is still limited to the case where the SGW/PGW is at or above Radio Access Network (RAN) level.

2.3.4. Data IDentification in ANDSF (DIDA) and Operator Policies for IP Interface Selection (OPIIS)

There are two ongoing work items in 3GPP that are currently addressing the issue of selecting a wireless interface or an IP address for a specific data application. The work item DIDA (Data IDentification in ANDSF) is addressing the need to map an application ID to a specific wireless interface, while the work item Operator

Policies for IP Interface Selection (OPIIS) is addressing the need of selecting the right APN for a given application.

Taking into account that there is a one to one link between APN and PDN connection (i.e., IP address) these work items clearly address from a 3GPP perspective the same problem space as [RFC6724], and the same considerations described in Section 2.2.4 apply here as well.

2.3.5. Multi-Access PDN Connectivity (MAPCON)

The Multi-Access PDN Connectivity (MAPCON) feature addresses the use of multiple PDN connections. Hence, this feature can make use of multiple wireless interfaces either sequentially or simultaneously.

3. Gap Analysis: limitations in current practices

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

The analysis is divided in three parts: IP client-based mobility, IP network-based mobility, and 3GPP mobility solutions. Each part analyzes how well the requirements listed in [I-D.ietf-dmm-requirements] are covered/met by the current practices, highlighting existing limitations and gaps.

3.1. Client-based IP mobility

3.1.1. REQ1: Distributed deployment

MIPv6 / NEMO A careful home agent deployment and policy configuration of the Mobile IPv6 / NEMO protocols can achieve some distribution. However, as soon as the mobile node moves and changes its initial attachment point, the anchors are no longer placed optimally, incurring in sub-optimal routes. This situation may be acceptable as long as the session is short-lived. If the mobile node is not expected to move within a limited area, this configuration might be considered sufficient. Otherwise, additional mechanisms to support dynamic anchoring would be needed. Note that a possible solution would be to run multiple instances of mobile IPv6 at the mobile node, each one managing a different HoA and bound to a different home agent. This would require, though, additional intelligence at the mobile node to be able to optimally select and manage source IP addresses for each session.

Mobile IPv6 RO The use of route optimization support enables a close-to anchor-less operation, which effectively can be considered as a fully distributed configuration. However, as explained before in this document, the home agent is still used for the signaling and therefore remains as a critical centralized component. Additionally, there is no standardized RO support for network mobility.

HMIPv6 The use of hierarchical mobile IPv6 can be seen as a step forward compared to a careful deployment of multiple home agents and its proper configuration, as it allows a mobile node to roam within a local domain, reducing the handover latency as well as the signaling overhead. If used together with mobile IPv6, traffic still has to traverse the centralized home agent, and therefore no distributed operation is achieved.

HA switch The home agent switch specification can be used to enable obtaining more benefits from a multiple-HA deployment, as the mobile node could be instructed to switch to a closer home agent. To avoid packet loss, this switch must be performed at periods of time in which the mobile node does not have any active connection running. Even if some packet loss were acceptable for active sessions, the change of home address would also require the mobile node to re-establish those sessions.

Flow mobility Considerations made for previous scenarios (e.g. for Route Optimization) could also apply here, extending those scenarios by the use of multiple attached interfaces.

SA selection API The use of proper source address selection decisions, enabled by smart connection managers [I-D.seite-mif-cm], or mobility aware applications using a selection API [RFC5014], [RFC6724], would allow the mobile node to realize substantial benefits from deployments providing multiple anchors.

3.1.2. REQ2: Transparency to Upper Layers when needed

MIPv6 / NEMO As a mobility protocol, the solution is transparent to the upper layers. However, as described before, this transparency comes with the cost of suboptimal routes if the MN moves away from its initial attachment point.

Mobile IPv6 RO The use of the route optimization support is transparent to the upper layers.

HMIPv6 The use of HMIPv6 is transparent to the upper layers.

HA switch The use of the home agent switch functionality is not transparent to the upper layers, as a change of home agent normally implies a change of home address. Therefore, the home agent can only be switched when there is no active session running on the mobile node. Since IP address continuity cannot be achieved at the relocated home agents, one gap that would need to be filled is the ability for the mobile node to convey HoA context from the previous home agent.

Flow mobility The use of flow mobility mechanisms is transparent to the upper layers.

SA selection API The use of an intelligent source address mechanisms is transparent to the upper layers if performed by the connection manager. However if the selection is performed by the applications themselves, via the use of the API, then applications have to be mobility-aware.

3.1.3. REQ3: IPv6 deployment

MIPv6 / NEMO Mobile IPv6 / NEMO protocols primarily support IPv6, although there are some extensions defined to also offer some IPv4 support [RFC5555].

Mobile IPv6 RO Route optimization only supports IPv6.

HMIPv6 HMIPv6 is only defined for IPv6.

HA switch The home agent switch specification supports only IPv6, although the use of the defined mechanisms to support dual stack IPv4/IPv6 mobile nodes would also enable some IPv4 support.

Flow mobility Flow mobility is only defined for IPv6.

SA selection API The use of source address selection mechanisms supports both IPv6 and IPv4.

3.1.4. REQ4: Existing mobility protocols

MIPv6 / NEMO These approaches are ones of the base IETF-standardized mobility protocols: [RFC6275] and [RFC3963].

Mobile IPv6 RO This approach is based on an existing protocol [RFC6275].

HMIPv6 This approach is based on an existing protocol [RFC5380].

HA switch This approach is based on an existing protocol [RFC5142].

Flow mobility This approach is based on existing protocols [RFC5648], [RFC6089] and [RFC6088].

SA selection API This approach is based on existing protocols [RFC6724] and [RFC5014].

3.1.5. REQ5: Compatibility

MIPv6 / NEMO This approach would be compatible with other protocols and work between trusted administrative domains, although as described before its operation would not provide the benefits of a fully distributed mechanism. The combination of different IP mobility protocols might have a performance/complexity cost associated, as described in [A. de la Oliva, et al.].

Mobile IPv6 RO This approach would be compatible with other protocols and work between trusted administrative domains, as long as mobile IPv6 is allowed. However, as highlighted before, mobile IPv6 route optimization requires specific support at the correspondent nodes.

HMIPv6 HMIPv6 is compatible with other protocols.

HA switch This approach would be compatible with other protocols and work between trusted administrative domains.

Flow mobility This approach would be compatible with other protocols and work between trusted administrative domains.

SA selection API This approach has no impact in terms of compatibility or use between trusted administrative domains.

3.1.6. REQ6: Security considerations

MIPv6 / NEMO This approach includes security considerations.

Mobile IPv6 RO This approach includes security considerations.

HMIPv6 This approach includes security considerations.

HA switch This approach includes security considerations.

Flow mobility This approach includes security considerations.

SA selection API This approach does not have security issues.

3.2. Network-based IP mobility

3.2.1. REQ1: Distributed deployment

PMIPv6 As for the case of MIPv6, a careful deployment of the local mobility anchors and policy configuration of the Proxy Mobile IPv6 protocol can achieve some distribution. However, as soon as the mobile node moves and changes its initial attachment point, the anchor is no longer placed optimally, incurring in sub-optimal routes, which might be quite noticeable in case of medium to large PMIPv6 domains. If the mobile node movement is restricted to a well known limited area and/or the PMIPv6 domain is not large, this configuration might be considered sufficient. Otherwise, additional mechanisms to support dynamic anchoring would be needed.

Local Routing As mentioned before, it enables optimal routing in three cases: the LMA manages the traffic of two mobile nodes connected to the same MAG, the LMA manages the traffic of two mobile nodes connected to different MAGs, the MAG manages the traffic of two mobile nodes connected to different LMAs. LR does not consider the case where the traffic should be optimized considering different MAGs and different LMAs. Inter LMA communication is not in scope. LR only enables better routing and does not consider the distribution of mobility anchors as such.

LMA Runtime Assignment The LMA runtime assignment is used to allocate an optimal LMA mostly for load balancing purposes, for instance in scenarios where LMAs run in a datacenter-like infrastructure. It can be used to allocate a different LMA based on other policies such as routing, although it is not clear how the technology can be used to achieve distributed mobility management, especially considering scalability issues. There are different gaps that would prevent using this mechanism as a way to meet all the DMM requirements: i) LMA runtime assignment can only be performed at the MN's attachment, so it would need to be extended to allow LMA re-location at any time; ii) LMA runtime assignment can only be initiated by current LMA; iii) it is not in the scope of the specification how the context is transferred between the involved LMAs.

Source Address Selection It can help in selecting a given IP source address although the current specifications have many limitations (for instance prefer IPv6 over IPv4, prefer HoA instead of CoA) and the socket extensions [RFC5014] require changes in the node. This solution alone is not sufficient to achieve anchors distribution in case of session continuity requirements, as some control logic (e.g., from a connection manager [I-D.seite-mif-cm]) is needed to intelligently perform source address selection.

Multihoming in PMIPv6 As summarized in the previous section a single mobility session belongs to a single LMA (at the most the same mobility session is shared across two access networks). As of today there is no possibility to distribute anchors and to move the session between different LMAs.

3.2.2. REQ2: Transparency to Upper Layers when needed

PMIPv6 As a mobility protocol, the solution provides transparent mobility support for a mobile node while roaming within the PMIPv6 domain (e.g., if a mobile node moves outside the domain, established sessions cannot be maintained, unless the MN implements Mobile IPv6). However, as for the MIPv6 case, this transparent mobility support comes with the cost of suboptimal routes if the MN moves away from its initial attachment point, especially in large PMIPv6 domains.

Local Routing During HO the standard mechanisms are used. In this sense if there is a MAG change while LR is enabled signaling is exchanged to inform the target MAG that upon handover LR should be re-established. The inter LMA case is not supported. For this solution the mobility context is always up, all the traffic receive seamless service.

LMA Runtime Assignment Seamless support is provided as per RFC 5213. Since the LMA cannot be changed at runtime, the solution provides transparency to the upper layers. However, if the solution were extended to allow dynamic LMA re-location, some extensions would be needed to provide IP address continuity.

Source Address Selection No seamless support is currently provided, since it requires solutions such as IP flow mobility for PMIPv6 [I-D.ietf-netext-pmipv6-flowmob].

Multihoming in PMIPv6 Seamless support falls back to standard PMIPv6 operations extended for IP flow mobility support. For this solution the mobility context is always up, all the traffic receive seamless service.

3.2.3. REQ3: IPv6 deployment

PMIPv6 Although Proxy Mobile IPv6 primarily support IPv6, there are also extensions defined to also offer some limited IPv4 support [RFC5844].

Local Routing It supports both IPv4 (limited to the support provided by [RFC5844]) and IPv6.

LMA Runtime Assignment It supports both IPv4 (limited to the support provided by [RFC5844]) and IPv6.

Source Address Selection It supports both IPv4 and IPv6.

Multihoming in PMIPv6 It supports both IPv4 (limited to the support provided by [RFC5844]) and IPv6.

3.2.4. REQ4: Existing mobility protocols

PMIPv6 This approach is one of the base IETF-standardized mobility protocols: [RFC5213].

Local Routing It reuses [RFC5213].

LMA Runtime Assignment It reuses [RFC5213].

Source Address Selection This approach is based on local support on the terminal only.

Multihoming in PMIPv6 It reuses [RFC5213].

3.2.5. REQ5: Compatibility

PMIPv6 This protocol is compatible with other protocols and can operate between trusted administrative domains, although there may be an associated penalty in terms of performance and/or complexity [A. de la Oliva, et al.].

Local Routing Since it extends [RFC5213], compatibility with existing network deployments and end hosts is provided.

LMA Runtime Assignment Since it extends [RFC5213], compatibility with existing network deployments and end hosts is provided.

Source Address Selection To enable the full set of use cases mentioned above extensions are required thus impacting the landscape of mobile devices. The extensions should not impact the network.

Multihoming in PMIPv6 Since it extends [RFC5213], compatibility is provided.

3.2.6. REQ6: Security considerations

PMIPv6 This approach includes security considerations.

Local Routing It reuses [RFC5213]. As such, the same security considerations apply.

LMA Runtime Assignment It reuses [RFC5213]. As such, the same security considerations apply.

Source Address Selection There is not signaling involved to perform this action.

Multihoming in PMIPv6 It reuses [RFC5213]. As such, the same security considerations apply.

3.3. 3GPP mobility

3.3.1. REQ1: Distributed deployment

SIPTO enables a certain degree of distribution, as SGW/PGW can be selected to be the closest geographically to the UE. This, together with the use of OPIIS (and MAPCON for the case the UE is using multiple interfaces), could be used to allow the use of different anchors as the UE moves. However, as described below, there is no support for dynamically changing the anchor while providing IP address continuity, which might be OK for short-lived sessions.

3.3.2. REQ2: Transparency to Upper Layers when needed

Seamless mobility at the local network is still not considered in SIPTO. Therefore, although SIPTO and LIPA allow offloading traffic from the network core similarly to the DMM approaches, even with LIMONET they just provide localized mobility support, requiring packet data network connections to be deactivated and re-activated when the UE is not moving locally.

3.3.3. REQ3: IPv6 deployment

3GPP specs support IPv6 as described in [RFC6459].

3.3.4. REQ4: Existing mobility protocols

Current 3GPP specifications make use of both IETF standardized mechanisms (e.g., PMIPv6, DSMIPv6), and custom made mechanisms, such

as GTP.

3.3.5. REQ5: Compatibility

All the 3GPP extensions listed in this document are compatible with 3GPP networks, at least for the same release these extensions are introduced or newer ones.

3.3.6. REQ6: Security considerations

3GPP extensions are assumed to be secure. TBD: refine (possibly extending) this section.

4. Conclusions

In this section we identify the gaps between existing mobility solutions and the DMM requirements and expected functionalities. We first summarize the identified IP-mobility protocols and provide a mapping (e.g., YES, NO, LIMITED) to the different DMM requirements listed in [I-D.ietf-dmm-requirements]. Following the independent analysis, a comparison between the solutions and the main DMM functionalities is provided. Finally, the possibility of using multiple solutions is addressed by combining different solutions according to the results found in the independent and functional analysis.

4.1. Independent solution analysis

	REQ1	REQ2	REQ3	REQ4	REQ5	REQ6
MIPv6/NEMO	NO	LIM	v6/v4	YES	LIM	YES
MIPv6 RO	NO	YES	v6	YES	LIM	YES
HMIPv6	NO	YES	v6	YES	LIM	YES
HA switch	NO	NO	v6	YES	YES	YES
FlowMob	NO	YES	v6/LIM v4	YES	YES	YES
SAS w/ CB	NO	YES	v6/v4	YES	YES	YES
PMIPv6	NO	LIM	v6/LIM v4	YES	LIM	YES
LR	NO	LIM	v6/LIM v4	YES	YES	YES
LMA RA	LIM	LIM	v6/LIM v4	YES	YES	YES
SAS w/ NB	NO	NO	v6/v4	YES	YES	YES
MuHo PMIPv6	NO	LIM	v6/LIM v4	YES	YES	YES

4.2. Functional analysis

The goal of this section is to identify and analyze the main functions that a DMM solution should provide in order to meet the DMM requirements [I-D.ietf-dmm-requirements]. This analysis is on purpose kept at high level, and will be used in the following section as main guideline for the final assessment of the gaps that cannot be covered with existing specified and deployed solutions (even if combined).

4.2.1. Multiple anchoring

Multiple (distributed) anchoring refers to the ability to anchor different sessions of a single mobile node at different anchors. In order to make this feature "DMM-friendly", some anchors should be placed closer to the mobile node. This implies the ability to deploy routers and assign locally anchored IP addresses at the edge of the network. This feature also requires potentially assigning multiple IP addresses to a single mobile node for its simultaneous use.

Figure 5 shows an example of the multiple anchoring function, in which a mobile network operator (MNO) has deployed multiple anchors, placed closer to or at the access network level. These (distributed) anchors provide attaching terminals with IP addresses that are locally anchored, allowing MNOs' traffic (Internet and operator services) to be locally offloaded (i.e., not traversing the MNO's core).

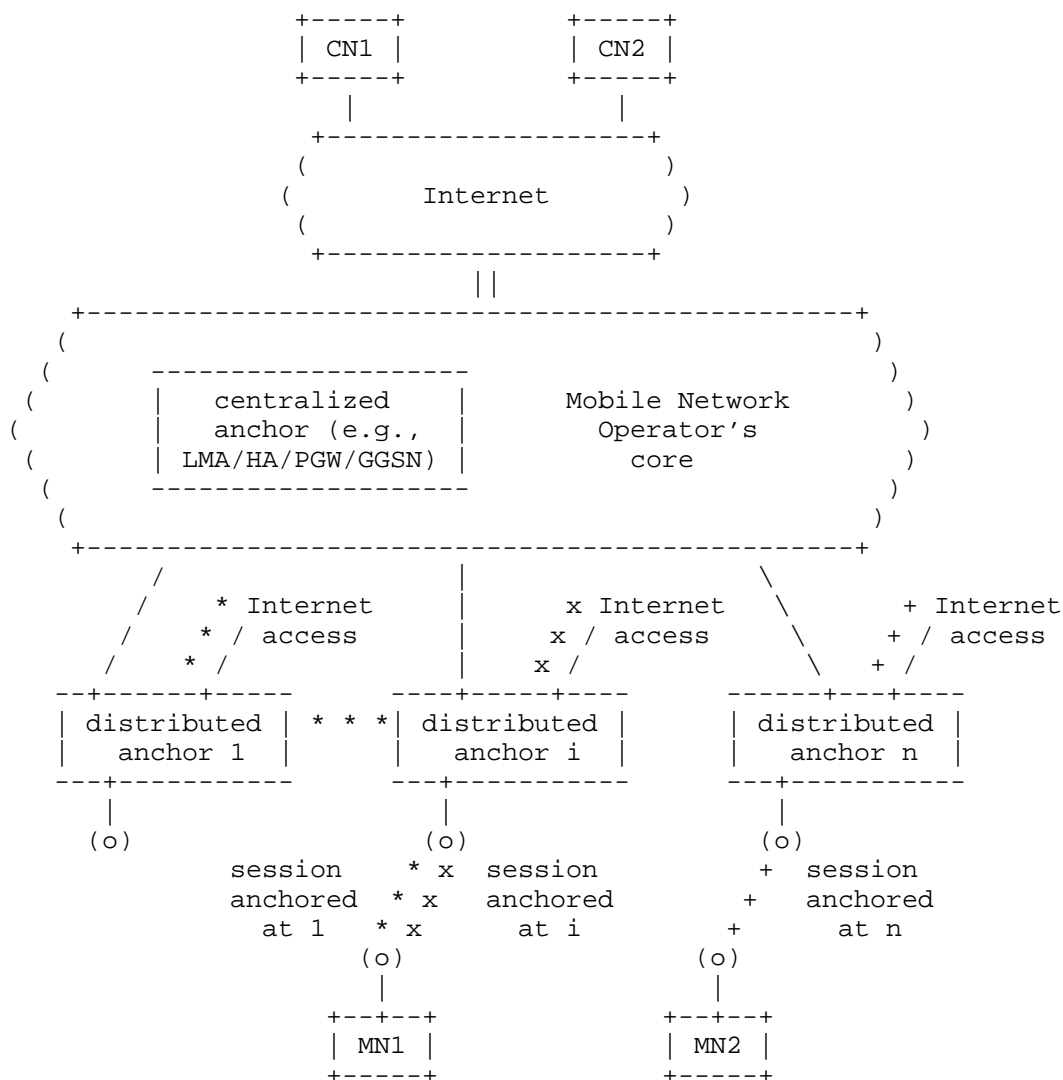


Figure 5: Multiple anchoring

4.2.2. Dynamic anchor assignment

Dynamic anchor re-location is the ability to i) optimally assign initial anchor, and ii) change the initially assigned anchor and/or assign a new one. This can be achieved either by changing anchor for all ongoing sessions (which might only be achievable with routing-based solutions), or by assigning new anchors for new sessions.

Figure 6 shows an example of what the dynamic anchor assignment function provides. A mobile node MN1, initially attached to the distributed anchor 1, establishes a session X (anchored at 1, i.e., optimal initial anchor assignment), which finishes before MN1 moves to the distributed anchor i. While connected to the distributed anchor i, a new session Y is established, which is anchored at i (i.e. assignment of a new anchor). Then MN1 moves and attaches to the distributed anchor n, while having session Y active, where MN1 is assigned n as its anchor for new sessions and (optionally) existing sessions are moved (i.e., change of assigned anchor).

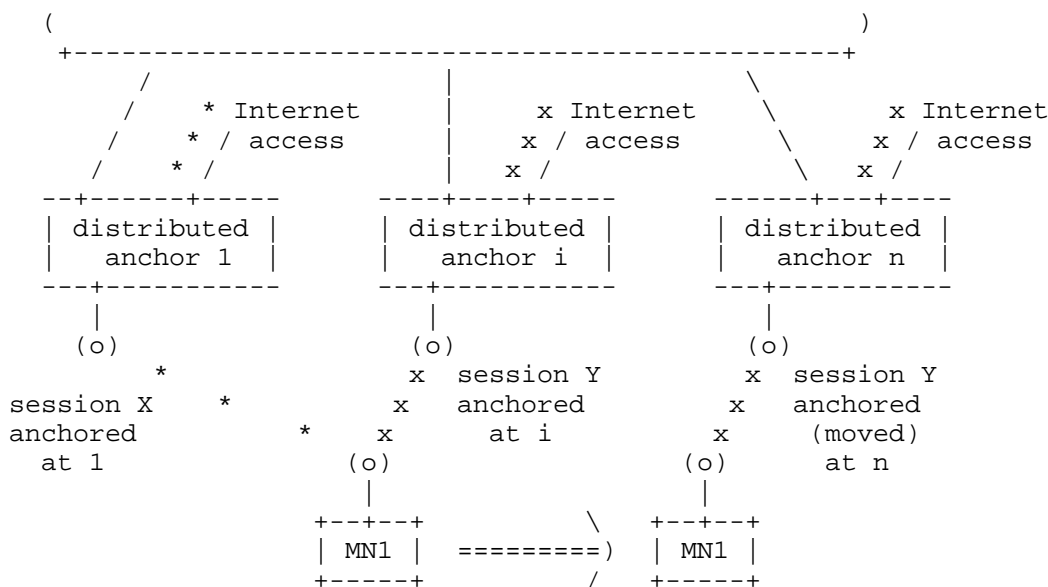


Figure 6: Dynamic anchor assignment

4.2.3. Multiple address management

Multiple IP address management refers to 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. Depending on the mobile node support, this functionality might require more or less support from the network side.

Figure 7 shows an example of multiple address management, in which MN1 initially obtained an IP address (IP a) when connected to the distributed anchor 1, which is then used for a session which remains active after MN1 moves and attaches to the distributed anchor i. MN1 also obtains a new IP address (IP b) to be used for sessions

initiated while attached to i . MN1 therefore needs to simultaneously manage and use multiple IP addresses, selecting the best one for each session. This selection might be performed by the mobile node solely or might be aided/performed with network support.

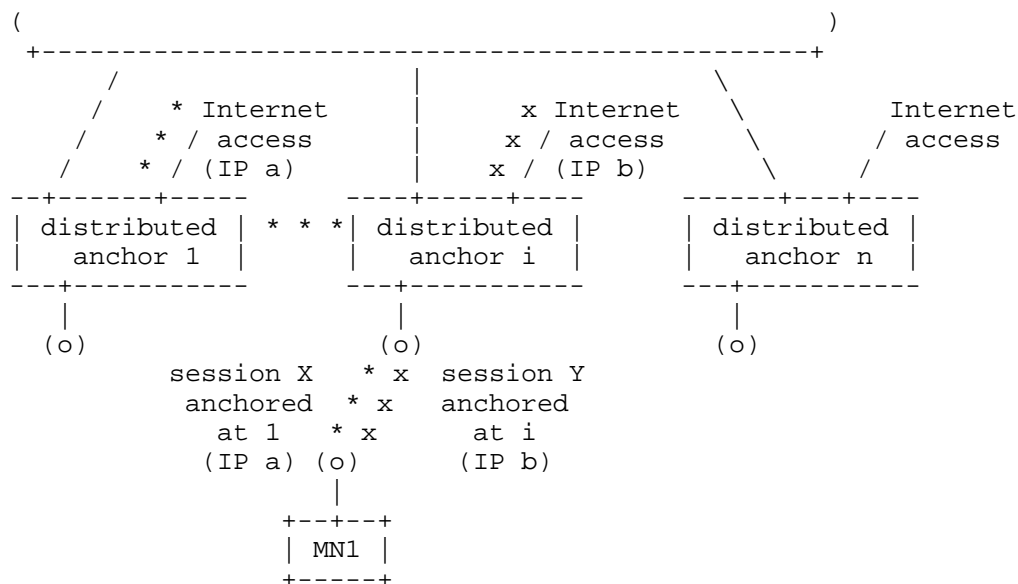


Figure 7: Multiple address management

4.3. Combined solutions analysis

The goal of this section is to evaluate how a solution based on combining the different standardized IP mobility solutions could meet the DMM requirements, making reference to the high-level functions identified above.

Both the main client- and network-based IP mobility protocols, namely (DS)MIPv6 and PMIPv6 allows to deploy multiple anchors (i.e., home agents and localized mobility anchors), therefore providing the functionality of multiple anchoring. However, existing solutions does 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 allow changing the anchor during an ongoing session.

Even if dynamic anchor change and new anchor assignment were supported, default address selection mechanisms would need to be improved, as mobile nodes would likely be assigned multiple IP addresses, anchored at different places. Therefore, smart address

selection, trying to always use the shortest path, would be required.

5. IANA Considerations

No IANA considerations.

6. Security Considerations

This is an informational document that analyzes practices for the deployment of existing mobility protocols in a distributed mobility management environment, and identifies the limitations in the current practices. One of the requirements that these practices has to meet is to take into account security aspects, including confidentiality and integrity. This is briefly analyzed for each of the considered practices, and will be extended in future versions of this document.

7. References

7.1. Normative References

- [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.
- [RFC5026] Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.
- [RFC5142] Haley, B., Devarapalli, V., Deng, H., and J. Kempf, "Mobility Header Home Agent Switch Message", RFC 5142, January 2008.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.
- [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.
- [RFC5648] Wakikawa, R., Devarapalli, V., Tsirtsis, G., Ernst, T.,

and K. Nagami, "Multiple Care-of Addresses Registration", RFC 5648, October 2009.

- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.
- [RFC6088] Tsirtsis, G., Giarreta, G., Soliman, H., and N. Montavont, "Traffic Selectors for Flow Bindings", RFC 6088, January 2011.
- [RFC6089] Tsirtsis, G., Soliman, H., Montavont, N., Giaretta, G., and K. Kuladinithi, "Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support", RFC 6089, January 2011.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
- [RFC6463] Korhonen, J., Gundavelli, S., Yokota, H., and X. Cui, "Runtime Local Mobility Anchor (LMA) Assignment Support for Proxy Mobile IPv6", RFC 6463, February 2012.
- [RFC6611] Chowdhury, K. and A. Yegin, "Mobile IPv6 (MIPv6) Bootstrapping for the Integrated Scenario", RFC 6611, May 2012.
- [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.

7.2. Informative References

- [3GPP.23.829]
3GPP, "Local IP Access and Selected IP Traffic Offload (LIPA-SIPTO)", 3GPP TR 23.829 10.0.1, October 2011.
- [3GPP.23.859]
3GPP, "LIPA Mobility and SIPTO at the Local Network", 3GPP TR 23.859 0.5.0, June 2012.
- [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.

- [A. de la Oliva, et al.]
de la Oliva, A., Soto, I., Calderon, M., Bernardos, C.,
and M. Sanchez, "The costs and benefits of combining
different IP mobility standards", Computer Standards &
Interfaces, accepted for publication, doi:10.1016/
j.csi.2012.08.003 , 2012.
- [I-D.ietf-dmm-requirements]
Chan, A., "Requirements for Distributed Mobility
Management", draft-ietf-dmm-requirements-02 (work in
progress), September 2012.
- [I-D.ietf-netext-pmipv6-flowmob]
Bernardos, C., "Proxy Mobile IPv6 Extensions to Support
Flow Mobility", draft-ietf-netext-pmipv6-flowmob-05 (work
in progress), October 2012.
- [I-D.patil-dmm-issues-and-approaches2dmm]
Patil, B., Williams, C., and J. Korhonen, "Approaches to
Distributed mobility management using Mobile IPv6 and its
extensions", draft-patil-dmm-issues-and-approaches2dmm-00
(work in progress), March 2012.
- [I-D.perkins-dmm-matrix]
Perkins, C., Liu, D., and W. Luo, "DMM Comparison Matrix",
draft-perkins-dmm-matrix-04 (work in progress), July 2012.
- [I-D.seite-mif-cm]
Seite, P. and J. Zuniga, "MIF API Conn Mngr
Considerations", draft-seite-mif-cm-00 (work in progress),
September 2012.
- [RFC4225] Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E.
Nordmark, "Mobile IP Version 6 Route Optimization Security
Design Background", RFC 4225, December 2005.
- [RFC4640] Patel, A. and G. Giarretta, "Problem Statement for
bootstrapping Mobile IPv6 (MIPv6)", RFC 4640,
September 2006.
- [RFC5014] Nordmark, E., Chakrabarti, S., and J. Laganier, "IPv6
Socket API for Source Address Selection", RFC 5014,
September 2007.
- [RFC6301] Zhu, Z., Wakikawa, R., and L. Zhang, "A Survey of Mobility
Support in the Internet", RFC 6301, July 2011.
- [RFC6459] Korhonen, J., Soininen, J., Patil, B., Savolainen, T.,

Bajko, G., and K. Iisakkila, "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)", RFC 6459, January 2012.

Appendix A. Acknowledgments

The work of Carlos J. Bernardos and Telemaco Melia has been partially supported by the European Community's Seventh Framework Programme (FP7-ICT-2009-5) under grant agreement n. 258053 (MEDIEVAL project). The work of Carlos J. Bernardos has also been partially supported by the Ministry of Science and Innovation of Spain under the QUARTET project (TIN2009-13992-C02-01). The authors would like to thank Konstantinos Pentikousis, Georgios Karagiannis, Jouni Korhonen, Jong-Hyouk Lee, Marco Liebsch, Elena Demaria, Peter McCann, Luo Wen and Julien Laganier for their valuable comments.

Authors' Addresses

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

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

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

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

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

Email: telemaco.melia@alcatel-lucent.com

Charles E. Perkins
Futurewei
USA

Email: charliep@computer.org

