

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.

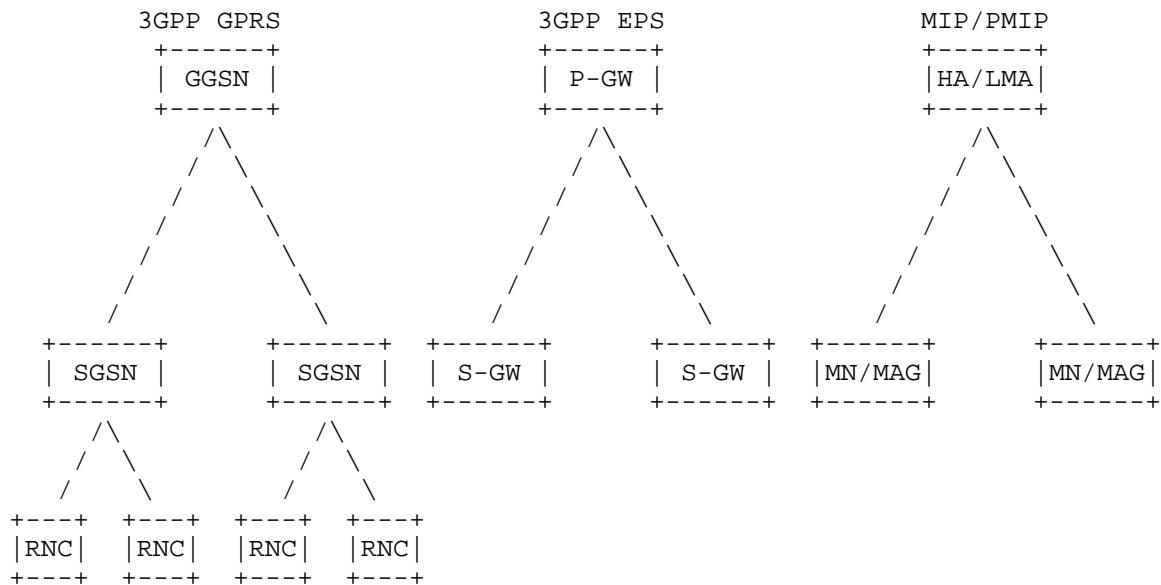


Figure 1. Centralized mobility management.

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.

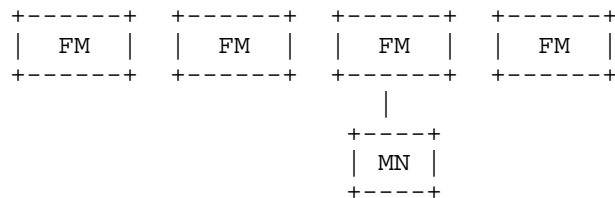


Figure 2. Distributed mobility management.

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., Waehlis, 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

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

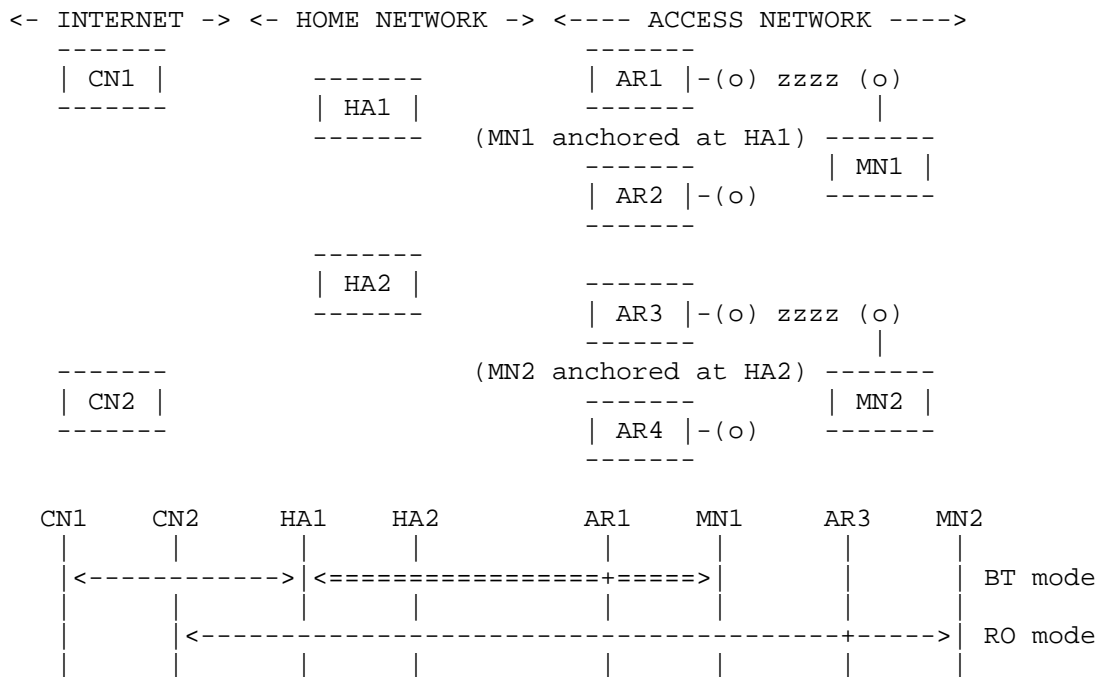


Figure 1: Distributed operation of Mobile IPv6 (BT and RO) / NEMO

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.

2.1.1.3. Hierarchical Mobile IPv6

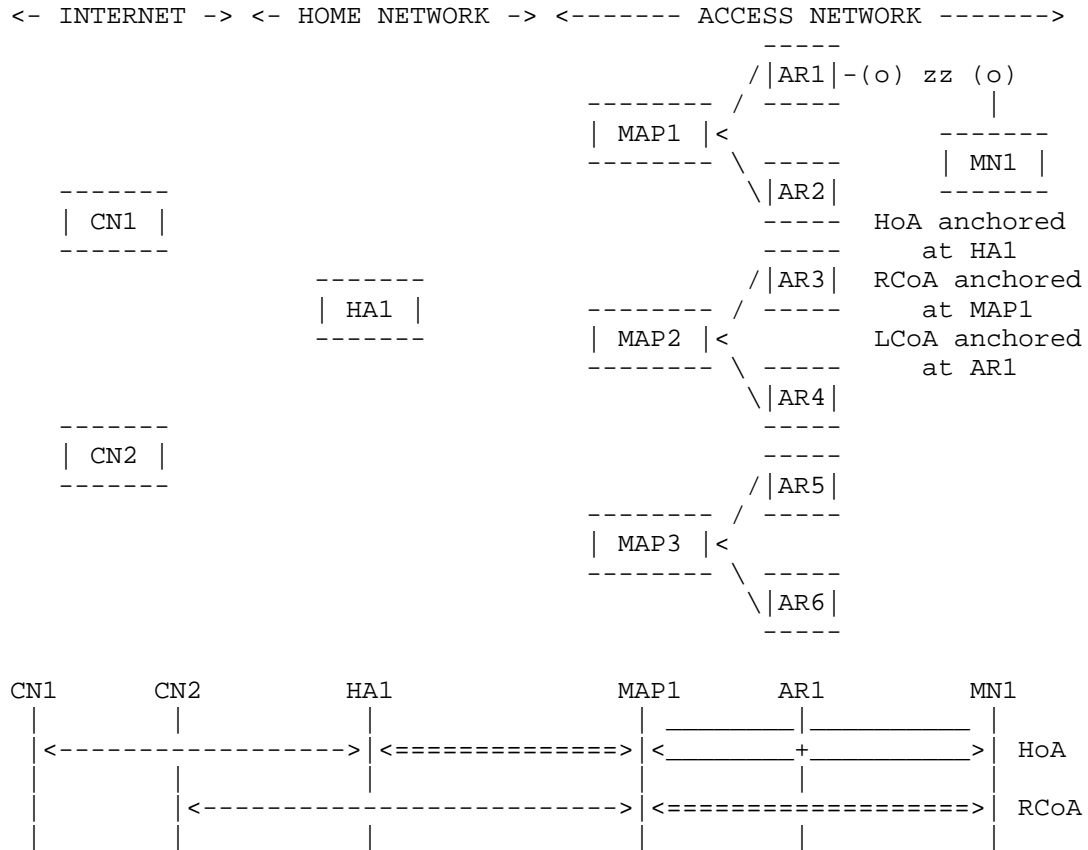


Figure 2: Hierarchical Mobile IPv6

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

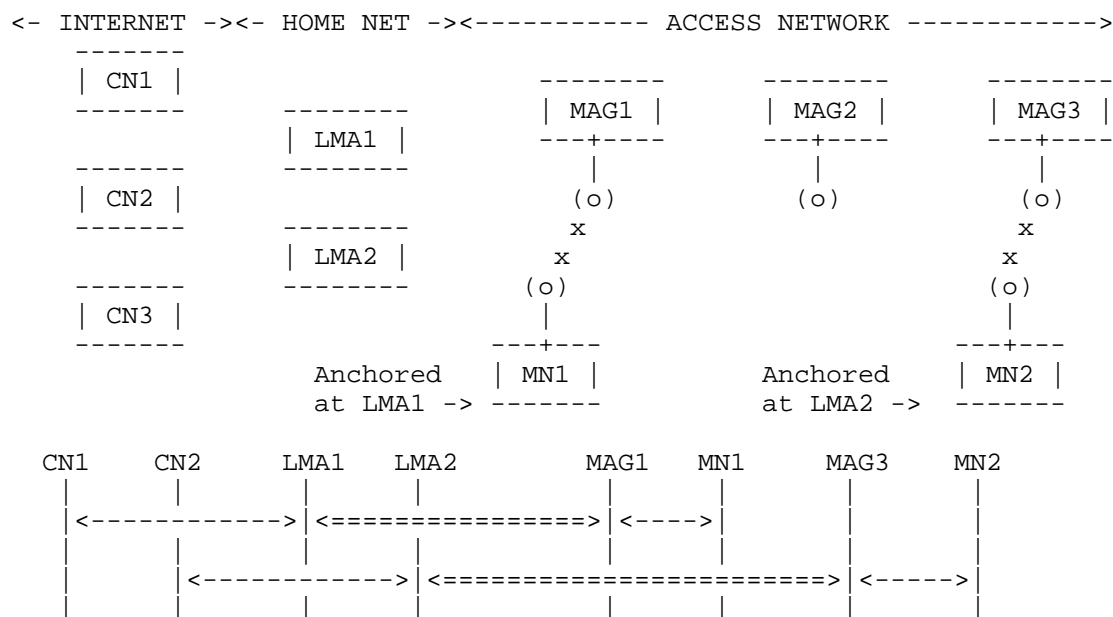


Figure 3: Distributed operation of Proxy Mobile IPv6

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].

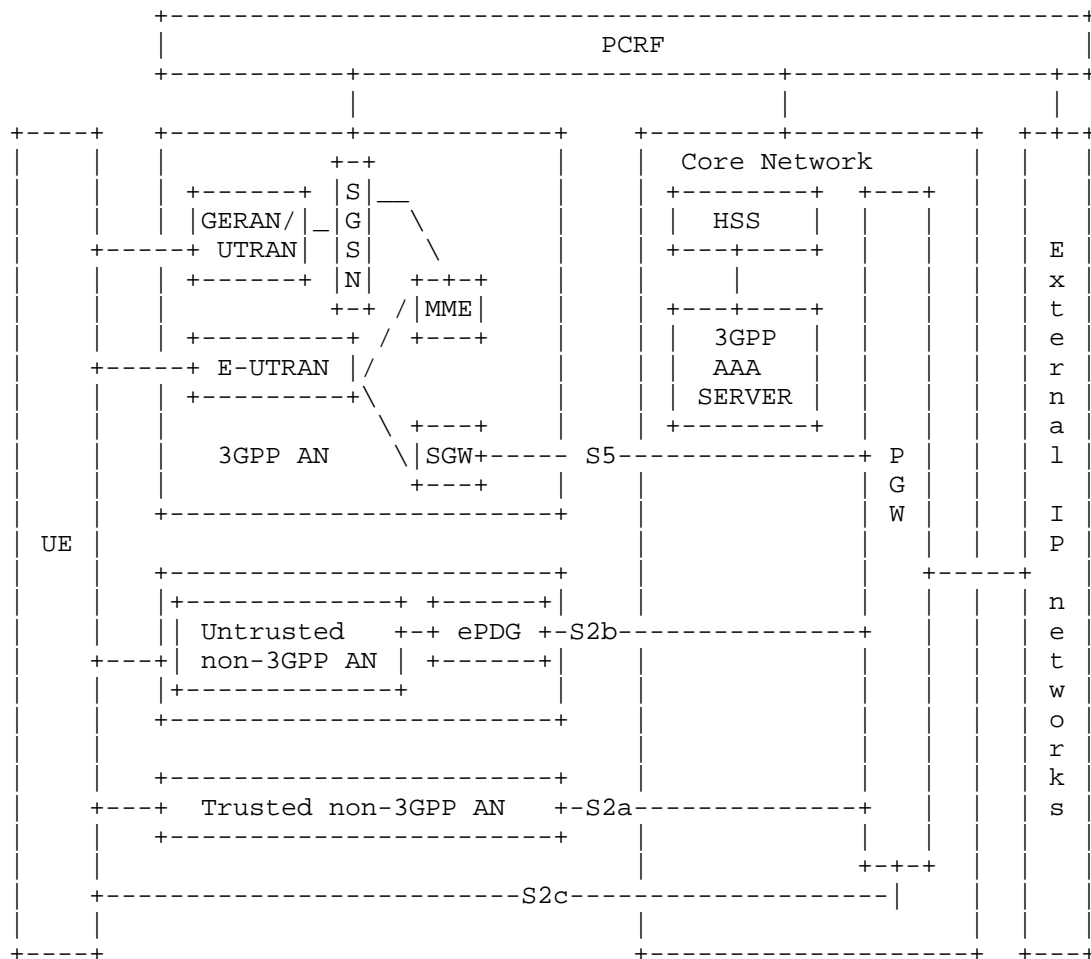


Figure 4: EPS (non-roaming) architecture overview

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).

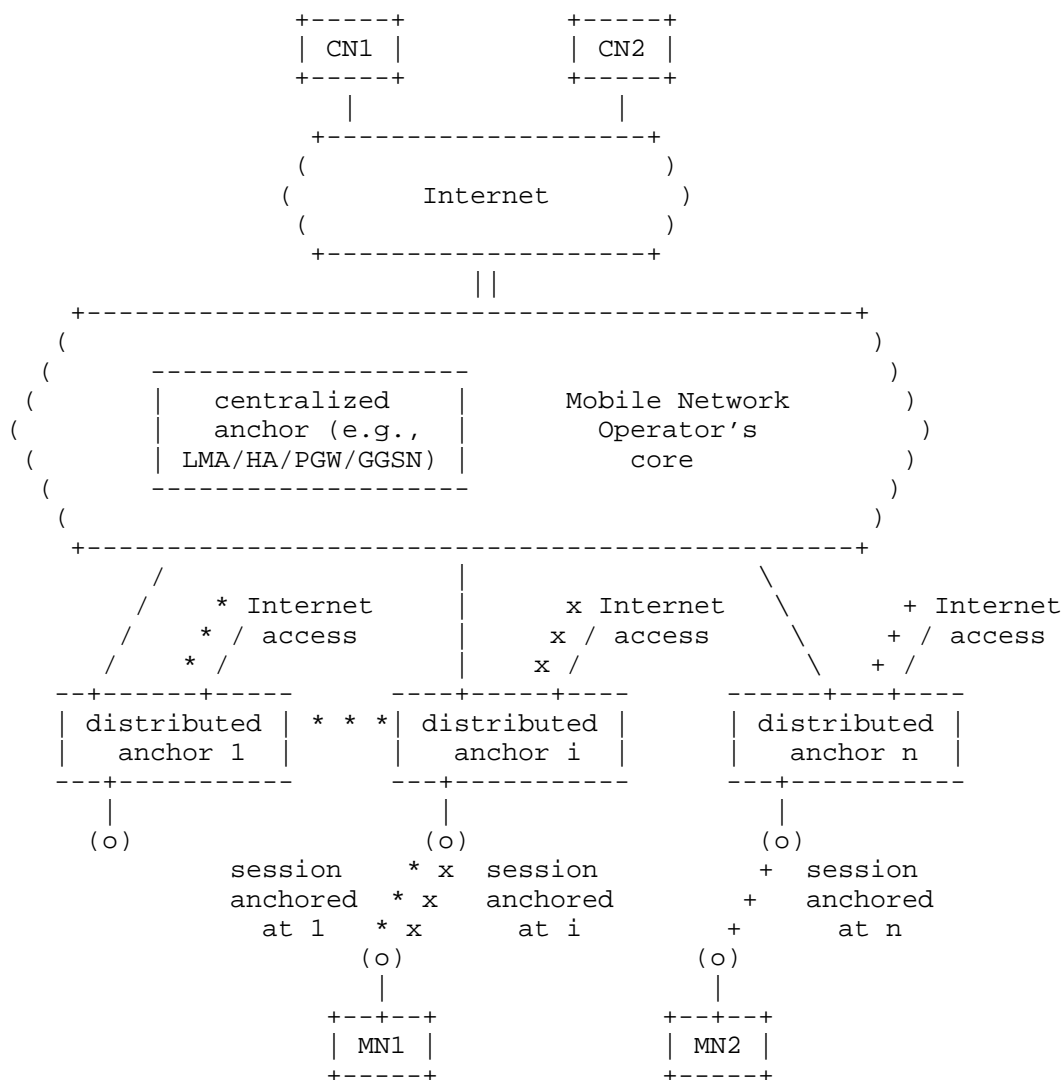


Figure 5: Multiple anchoring

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).

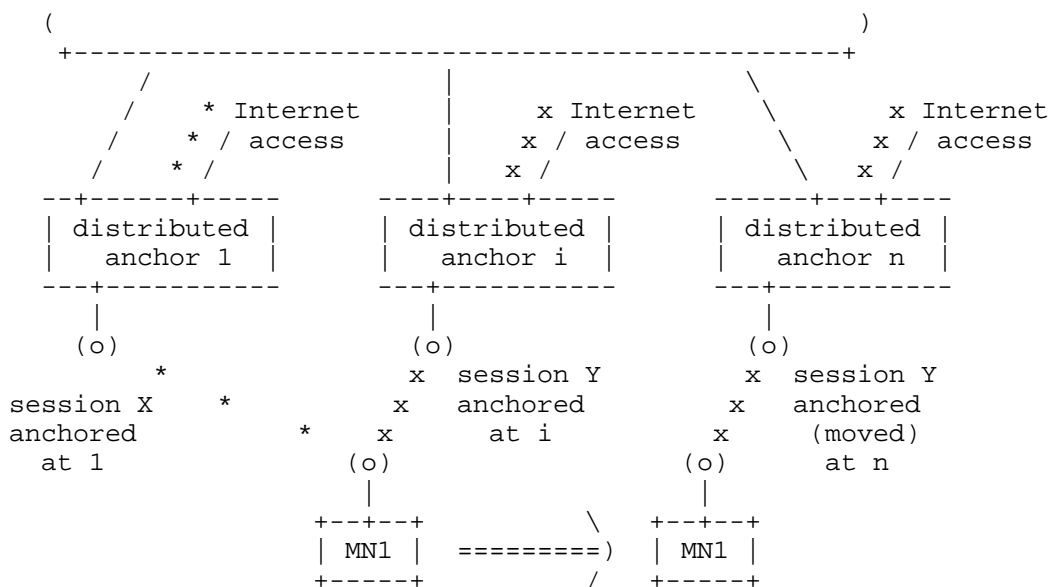


Figure 6: Dynamic anchor assignment

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.

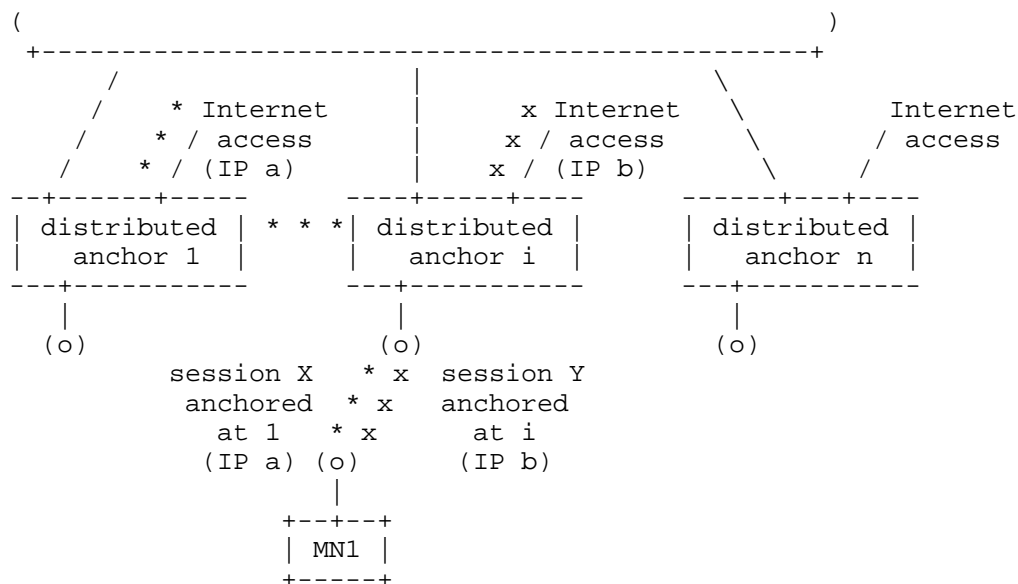


Figure 7: Multiple address management

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

