

DMM
Internet-Draft
Intended status: Informational
Expires: August 29, 2013

H. Chan
Huawei Technologies
P. Seite
France Telecom - Orange
K. Pentikousis
Huawei Technologies
February 25, 2013

Distributed Mobility Management Framework
draft-chan-dmm-framework-01

Abstract

This document introduces a framework for mobility management protocols in terms of their key, abstract logical functions. We explain how the framework is capable of presenting a unified view, reducing the clutter that prevents a casual reader from understanding the commonalities between different approaches in mobility management. A first order application of this framework is to enable 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.

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 29, 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	3
2. Conventions and Terminology	4
3. Mobility Management Logical Functions	4
4. Mobility Protocol Functional Decomposition	5
4.1. Decomposing Mobile IPv6	6
4.2. From MIPv6 to PMIPv6	6
4.3. Hierarchical Mobile IPv6	8
4.4. Distributing Mobility Anchors	9
4.5. Migrating Home Agents	10
5. DMM Functional Decomposition Scenarios	11
5.1. Flat Network Scenario	11
5.1.1. Network-based Mobility Management	12
5.1.2. Client-based Mobility Management	13
5.2. DMM with Control and Data Plane Separation	14
6. Security Considerations	16
7. IANA Considerations	16
8. References	16
8.1. Normative References	16
8.2. Informative References	16
Authors' Addresses	18

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 DMM architecture can be designed using primarily existing mobility management protocols with some extensions. This is reflected in the requirement included in [I-D.ietf-dmm-requirements]: distributed mobility management is to first use existing protocols and their extensions before considering new protocol designs. Although this a key requirement as we move forward, it does not point to which extensions are needed let alone how to devise them.

Mobile IPv6 [RFC6275], for instance, which is a logically centralized mobility management approach addressing primarily hierarchical mobile networks, has numerous variants and extensions including, PMIPv6 [RFC5213], Hierarchical MIPv6 (HMIPv6) [RFC5380], Fast MIPv6 (FMIPv6) [RFC5568] [RFC4988], Proxy-based FMIPv6 (PFMIPv6) [RFC5949], just to name a few. 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 MIP specification came into life. This document argues that we can gain much more insight into the design space of DMM protocols by abstracting the functionality 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. What is more, this document shows how to reconfigure these logical functions towards various distributed mobility management designs.

The rest of this document is organized as follows. After setting the stage with conventions and terminology in the following section, Section 3 introduces the framework abstractions, based on common functionality we observe in the current crop of mobility management protocols. This includes three logical functions, namely, home address allocation, mobility routing and location management. Such functional decomposition will enable us to clearly separate data and 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. Next, Section 4 shows that these logical functions can indeed perform the same functions as 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. Finally, Section 5 presents scenarios where the functional aspects of the framework are illustrated.

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].

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]. This includes terms such as mobile node (MN), correspondent node (CN), home agent (HA), home address (HoA), care-of-address (CoA), local mobility anchor (LMA), and mobile access gateway (MAG).

In addition, this document uses the following term:

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

3. Mobility Management Logical Functions

Functional entity (FE) decomposition is an often-used engineering approach that enables us to look at the similarities and differences of complex systems while keeping track of their important operational aspects. Earlier work, for instance, in the European research project Ambient Networks investigated how to create an advanced and forward-looking architecture aiming primarily for mobile and wireless networks [Book-AN]. A key goal was to design mechanisms that can be deployed in a variety of settings (ad-hoc or operator-controlled) and scale from small home networks with little human supervision to sensor networks deployed over large geographical areas with limited resources, to large professionally-managed infrastructure networks. The project put forward the concept of the Ambient Control Space (ACS) which relies on only three interfaces; interested readers can find more details in [Book-AN].

Within the ACS, novel mobility management mechanisms were developed based on the concept of self-containing Functional Entities (FEs) which featured well-defined interfaces and interactions with each other. This systematic decomposition enabled the development of several mobility management mechanisms which put emphasis on different aspects. Examples of these approaches include the Generic Link Layer [Paper-GLL], Multi-radio Resource Management [Paper-MRRM], and [Paper-NODEID], which has some similarities with HIP. Later work in this area capitalized on the established FEs within the ACS to

define new mechanisms, that were not originally envisioned, such as [Paper-ANHASA].

Following this tradition, this document applies a similar approach to logically decomposing mobility management functions. This way we can establish a common framework that will enable us to reason about DMM functionality with well-defined and well-understood FEs or logical functions. As a first step, the DMM Framework presented in this document demonstrates that the existing mobility management functions of MIPv6, PMIPv6, and HMIPv6 can be abstracted into the following logical functions:

1. Anchoring function: allocation of home network prefix or HoA to an MN that registers with the network;
2. Mobility Router (MR) function: packets interception and forwarding to/from the MN HoA 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 MN internetwork location, which includes a mapping of the HoA to the mobility anchoring point that the MN is anchored to;
4. Location Update (LU) function: provisioning of MN location information to the LM function;
5. Routing Control (RC) function: MR function forwarding state configuration.

In addition, the Access Router (AR) logical function provides first-hop network access and includes functionality below the network layer, e.g. radio communication facilities. An AR may provide home address allocation as well as act as MR.

4. Mobility Protocol Functional Decomposition

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. Decomposing Mobile IPv6

Fig. 1 illustrates the Mobile IPv6 [RFC6275] functional decomposition using the logical functions introduced in Section 3. The combination of the MR, LM and HoA allocation logical functions in Network1 effectively defines the home agent or the mobility anchor. In the depicted network scenario, the mobile node designated as MN11 was originally attached to Network1 and was allocated an IP prefix for its home address (HoA11). At a later stage, MN11 moves to Network3, where it is allocated a new prefix to configure the IP address IP32. LM1 maintains the binding HoA11:IP32 so that packets from its correspondent node CN21 in Network2 destined to HoA11 can be intercepted by MR1, which will then tunnel them to IP32. MN11 must perform mobility signaling using the LU function.

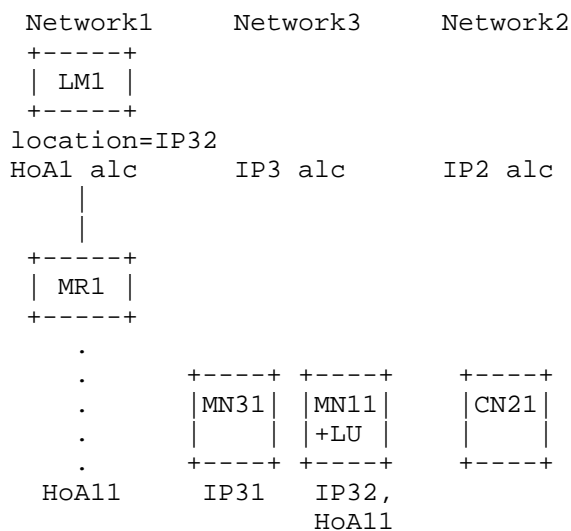


Figure 1. Functional decomposition of Mobile IPv6

4.2. From MIPv6 to PMIPv6

The functional decomposition of Proxy Mobile IPv6 [RFC5213] according to the proposed framework is shown in Fig. 2. In PMIPv6, the combination of LM, MR, and HoA allocation effectively defines the Local Mobility Anchor (LMA). The combination of AR and LU together with additional signaling with MN comprises the Mobile Access Gateway (MAG). In the figure, MN11 is attached to the access router AR31 which has the IP address IP31 in Network3. LM1 maintains the binding HoA11:IP31. The access router AR31 also behaves like a home link to MN11 so that MN11 can use its original IP address HoA11.

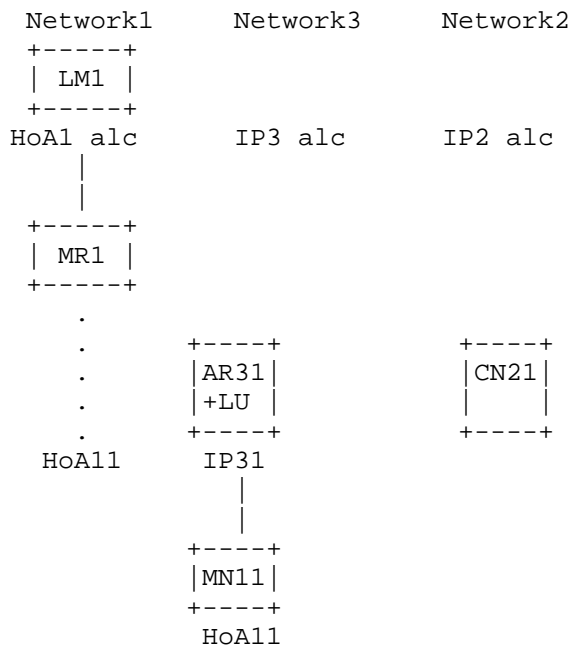
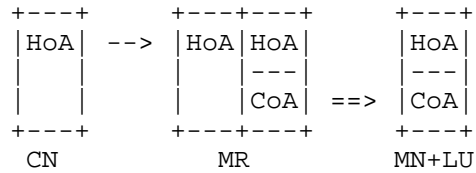


Figure 2. Functional decomposition of PMIPv6

MIPv6 and PMIPv6 both employ the same concept of separating the session identifier (HoA) from the routing address (CoA). Fig. 3 contrasts (a) MIPv6 with (b) PMIPv6 by illustrating the destination IP address in the network-layer header as a packet traverses the network from the CN to the MN. Note that MIPv6 and PMIPv6 bundle three mobility management logical functions, namely, LM1, IP1 prefix allocation and MR1 into the home agent (HA) and Local Mobility Anchor (LMA), respectively.

Fig. 3 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 in the former case, 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 in MIPv6, such signaling can be confined between the AR+LU and the 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.

(a) MIPv6:



(b) PMIPv6:

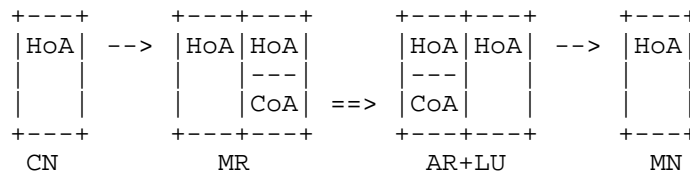


Figure 3. Network layer in the protocol stack of packets sent from the CN and tunneled (a) to the MN+LU in MIPv6; and (b) to the AR+LU in PMIPv6 showing the destination IP address as the packet traverses from the CN to the MN.

4.3. Hierarchical Mobile IPv6

The functional decomposition of Hierarchical Mobile IPv6 [RFC5380] is shown in Fig. 4. Besides the logical functions LM1, MR1, and HoA1 prefix allocation in Network1, as we have seen above for MIPv6 and PMIPv6, there is an MR function (MR3) in the visited network (Network3). MR3 acts also as 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 tracks the LM binding HoA11:IP32. The combined function of MR and the LM proxy function is the Mobility Anchor Point (MAP).

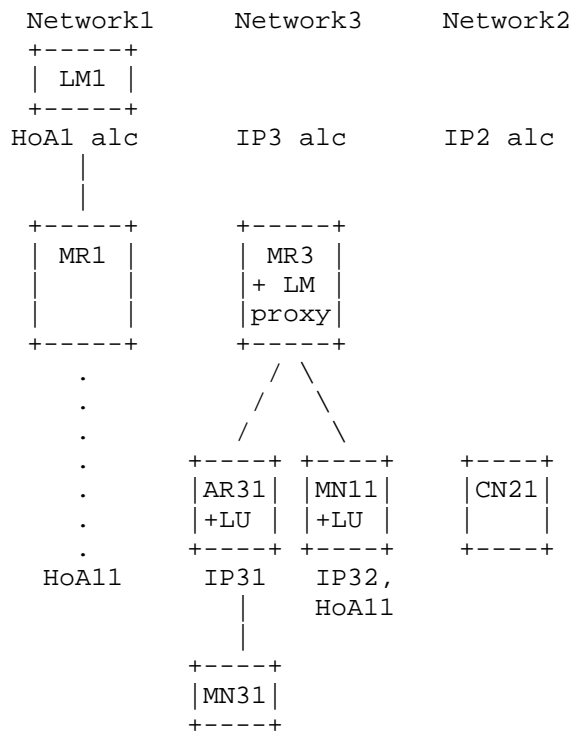


Figure 4. Functional decomposition of Hierarchical Mobile IPv6

Note that as depicted in Fig. 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

As we have seen so far, the framework is sufficiently expressive to enable us to decompose the major MIPv6 variants. It is possible to replicate the mobility anchoring function for any of MIPv6, PMIPv6, or HMIPv6, in multiple networks as shown in Fig. 5 which illustrates such an example with three networks.

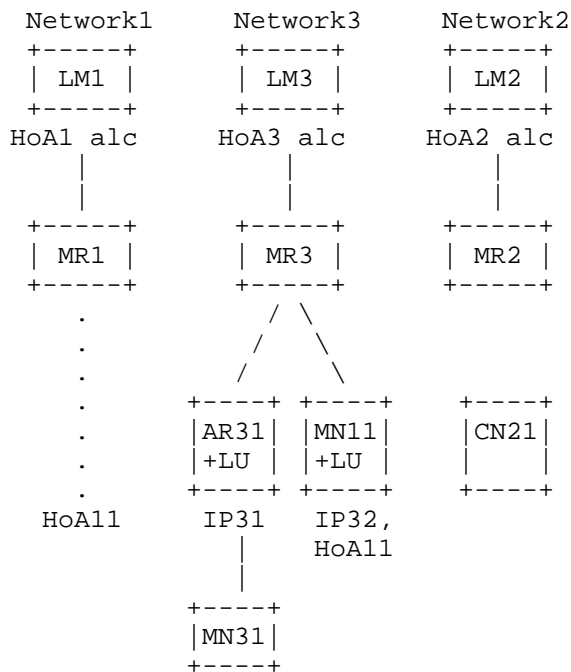


Figure 5. Distributing mobility anchors using the DMM Framework logical functions

4.5. Migrating Home Agents

When all logical functions of the Framework are bundled into a 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 advocated in [Paper-Migrating.Home.Agents]. A functional decomposition of Migrating Home Agents is shown in Fig. 6: 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 three 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 the CN, i.e. MR2 in the example of Fig. 6. Using the LM information in LM0, MR2 will use the binding HoA11:IP32 to tunnel the packets to MN11.

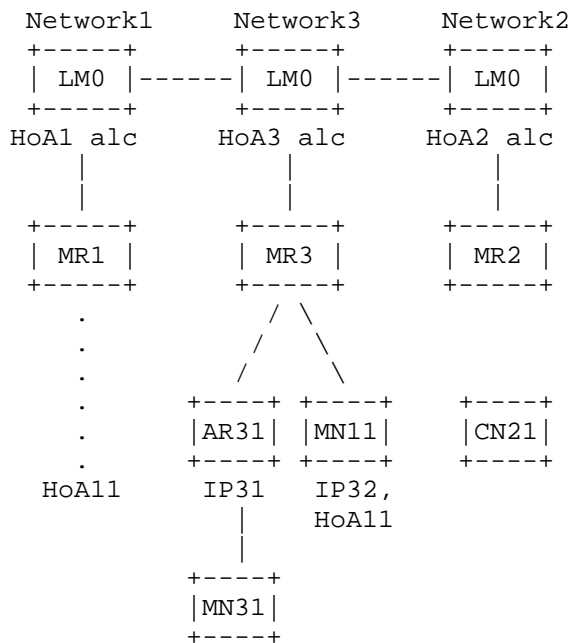


Figure 6. Functional decomposition of Migrating Home Agents

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 necessary for 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 Fig. 6 takes the place of MN31 which is attached to AR31, the resulting mobility management becomes network-based.

5. DMM Functional Decomposition Scenarios

This section covers the functional description of DMM. Basically, the scenarios present a way to distribute the logical mobility functions.

5.1. Flat Network Scenario

In a flat network, the logical functions may all be located at the AR as shown in Figs. 7 and 8, respectively. For example,

[I-D.seite-dmm-dma] and [I-D.bernardos-dmm-distributed-anchoring] are PMIPv6-based implementations of this scenario. These two figures depict the network- and client-based distributed mobility management scenarios, respectively. 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. AR can act as a standard IP router;
2. AR can provide the MR function (i.e. act as mobility anchor);
3. AR can provide the LU function;
4. AR can provide both MR and LU functions.

5.1.1.1. Network-based Mobility Management

The functional decomposition of network-based mobility management is depicted in Fig. 7. In case (1), MN1 attaches to AR1. AR advertises the 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 on behalf of 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. That is, HoA3 is used for all new IP communications, 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.

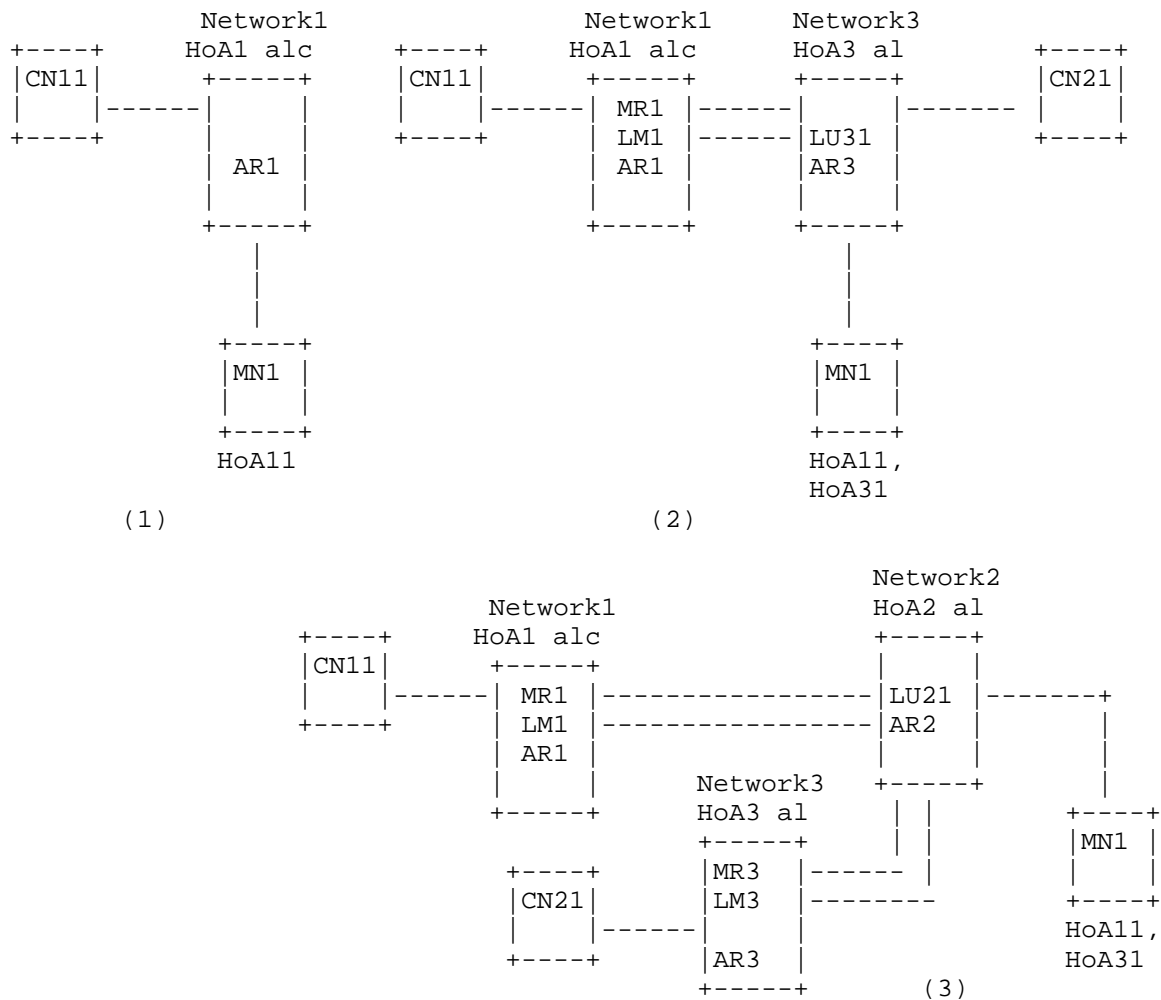


Figure 7. Network-based DMM architecture for a flat network

5.1.2. Client-based Mobility Management

The functional decomposition of client-based mobility management is depicted in Fig. 8. In case (1), MN1 attaches to AR1. AR advertises the 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. 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.

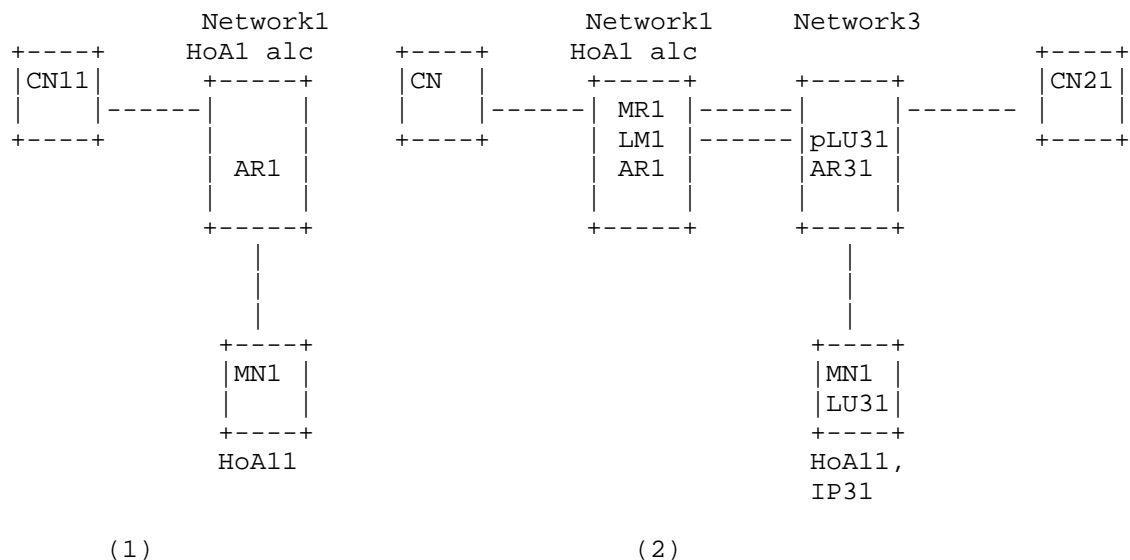


Figure 8. Client-based DMM architecture for a flat network

5.2. DMM with Control and Data Plane Separation

This section considers a scenario which involves 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 functional decomposition described in this document can be used to understand better the data and control plane separation.

Fig. 9 shows an example DMM topology with the same three networks we have been using in Fig. 5. As in Fig. 5, each network in Fig. 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 information with each other.

In addition to these features, the LM function in Fig. 9 is a distributed database, possibly implemented with multiple virtual or physical servers, handling the mapping of HoA to CoA. To perform

mobility routing, the MRs need the location information which is maintained at LM1, LM2, and LM3. 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.

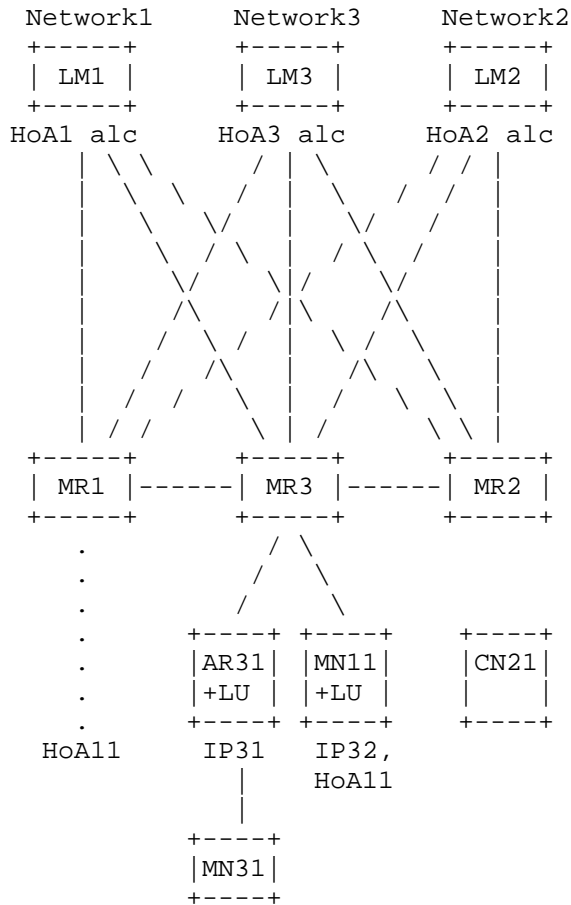


Figure 9. DMM with Control and Data Plane Separation

Fig. 9 illustrates three MRs (MR1, MR2, and MR3) in three networks. In this scenario we take that MN11 has moved from Network1 supported by MR1 and LM1 to Network3 supported by MR3 and LM3. MN11 may use the home address (HoA11) allocated to it when it was directly connected to the former network for those application sessions that

were started when the mobile node was attached there and do require session continuity after the handover to the latter network. When MN11 is connected to Network1, no location management is needed; LM1 will not keep an entry for HoA11. After MN11 handovers to Network3, the LM1 server maintains a mapping of HoA11 to MR3. That is, LM1 points to Network3 and it is this network that will keep track of how to reach MN11. Such a hierarchical mapping can prevent frequent signaling updates to LM1, as MN11 performs intra-network handover(s) within the Network3 domain. In other words, the concept of hierarchical mobile IP [RFC5380] is applied here for location management only but not for data plane routing.

6. Security Considerations

TBD

7. IANA Considerations

This document presents no IANA considerations.

8. References

8.1. Normative References

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

8.2. Informative References

[Book-AN] Niebert, N., Schieder, A., Zander, J., and R. Hancock (Eds.), "Ambient networks: co-operative mobile networking for the wireless world.", Wiley, 2007.

[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.ietf-dmm-requirements]
Chan (Ed.) et al., H., "Requirements for Distributed Mobility Management", draft-ietf-dmm-requirements-03 (work in progress), December 2012.

[I-D.seite-dmm-dma]
Seite, P., Bertin, P., and JH. Lee, "Distributed Mobility

Anchoring", draft-seite-dmm-dma-06 (work in progress), January 2013.

[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-ANHASA]

Pentikousis, K., Agüero, R., Gebert, J., Galache, J., Blume, O., and P. Paakkonen, "The Ambient Networks heterogeneous access selection architecture", Mobility, Multiaccess, and Network Management (M2NM) 2007. First Ambient Networks Workshop on. Sydney, Australia, October 2007, pp. 49-54, October 2007.

[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-GLL]

Koudouridis, G., Agüero, R., Alexandri, E., Choque, J., Dimou, K., Karimi, H., Lederer, H., Sachs, J., and R. Sigle, "Generic link layer functionality for multi-radio access networks", Proc. IST Mobile and Wireless Communication Summit 2005., 2005.

[Paper-MRRM]

Berggren, F., Bria, A., Badia, L., Karla, I., Litjens, R., Magnusson, P., Meago, F., Tang, H., and R. Veronesi, "Multi-radio resource management for ambient networks", Personal, Indoor and Mobile Radio Communications (PIMRC) 2005. IEEE 16th International Symposium on. Vol. 2, pp. 942-946, 2005.

[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-NODEID]

Ahlgren, B., Eggert, L., Ohlman, B., and A. Schieder, "Ambient networks: Bridging heterogeneous network domains", Personal, Indoor and Mobile Radio Communications (PIMRC) 2005. IEEE 16th International Symposium on. Vol. 2, pp. 937-941, 2005.

[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.

[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.

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

[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
Carnotstrasse 4
10587 Berlin
Germany

Email: k.pentikousis@huawei.com

DMM
Internet-Draft
Intended status: Informational
Expires: May 8, 2015

D. Liu, Ed.
China Mobile
JC. Zuniga, Ed.
InterDigital
P. Seite
Orange
H. Chan
Huawei Technologies
CJ. Bernardos
UC3M
November 4, 2014

Distributed Mobility Management: Current practices and gap analysis
draft-ietf-dmm-best-practices-gap-analysis-09

Abstract

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

Status of This Memo

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

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

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

This Internet-Draft will expire on May 8, 2015.

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	2
2. Terminology	3
3. Functions of existing mobility protocols	3
4. DMM practices	5
4.1. Assumptions	5
4.2. IP flat wireless network	6
4.2.1. Host-based IP DMM practices	7
4.2.2. Network-based IP DMM practices	11
4.3. Flattening 3GPP mobile network approaches	13
5. Gap analysis	16
5.1. Distributed mobility management - REQ1	16
5.2. Bypassable network-layer mobility support for each application session - REQ2	19
5.3. IPv6 deployment - REQ3	20
5.4. Considering existing mobility protocols - REQ4	20
5.5. Coexistence with deployed networks/hosts and operability across different networks - REQ5	21
5.6. Operation and management considerations - REQ6	21
5.7. Security considerations - REQ7	22
5.8. Multicast - REQ8	22
5.9. Summary	23
6. Security Considerations	25
7. Contributors	25
8. References	26
8.1. Normative References	26
8.2. Informative References	26
Authors' Addresses	30

1. Introduction

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

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

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

2. Terminology

All general mobility-related terms and their acronyms used in this document are to be interpreted as defined in the Mobile IPv6 base specification [RFC6275], in the Proxy Mobile IPv6 specification [RFC5213], and in the Distributed Mobility Management Requirements [RFC7333]. These terms include mobile node (MN), correspondent node (CN), home agent (HA), Local Mobility Anchor (LMA), Mobile Access Gateway (MAG), centrally deployed mobility anchors, distributed mobility management, hierarchical mobile network, flatter mobile network, and flattening mobile network.

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

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

3. Functions of existing mobility protocols

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

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

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

1. Anchoring Function (AF): allocation to a mobile node of an IP address, i.e., Home Address (HoA), or prefix, i.e., Home Network Prefix (HNP) topologically anchored by the advertising node. That is, the anchor node is able to advertise a connected route into the routing infrastructure for the allocated IP prefixes. This function is a control plane function.
2. Internetwork Location Information (LI) function: managing and keeping track of the internetwork location of an MN. The location information may be a binding of the IP advertised address/prefix, e.g., HoA or HNP, to the IP routing address of the MN or of a node that can forward packets destined to the MN. It is a control plane function.

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

3. Forwarding Management (FM) function: packet interception and forwarding to/from the IP address/prefix assigned to the MN, based on the internetwork location information, either to the destination or to some other network element that knows how to forward the packets to their destination.

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

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

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

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

4. DMM practices

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

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

4.1. Assumptions

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

1. Both host- and network-based solutions are considered.
2. Solutions should allow selecting and using the most appropriate IP anchor among a set of available candidates.
3. Mobility management should be realized by the preservation of the IP address across the different points of attachment (i.e., provision of IP address continuity). This is in contrast to certain transport-layer based approaches such as Stream Control Transmission Protocol (SCTP) [RFC4960] or application-layer mobility.

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

4.2. IP flat wireless network

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

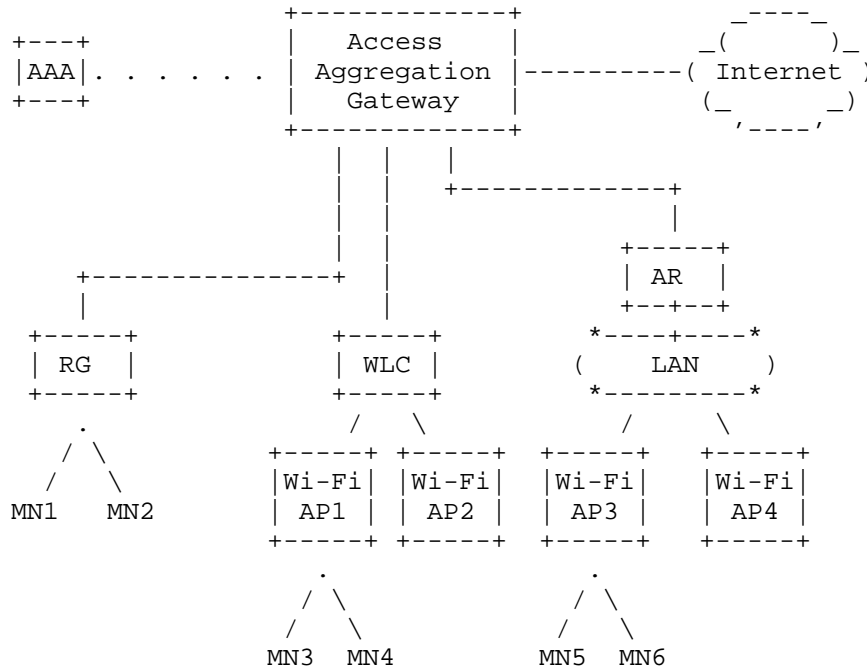


Figure 1: IP Wi-Fi network architectures

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

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

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

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

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

4.2.1. Host-based IP DMM practices

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

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

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

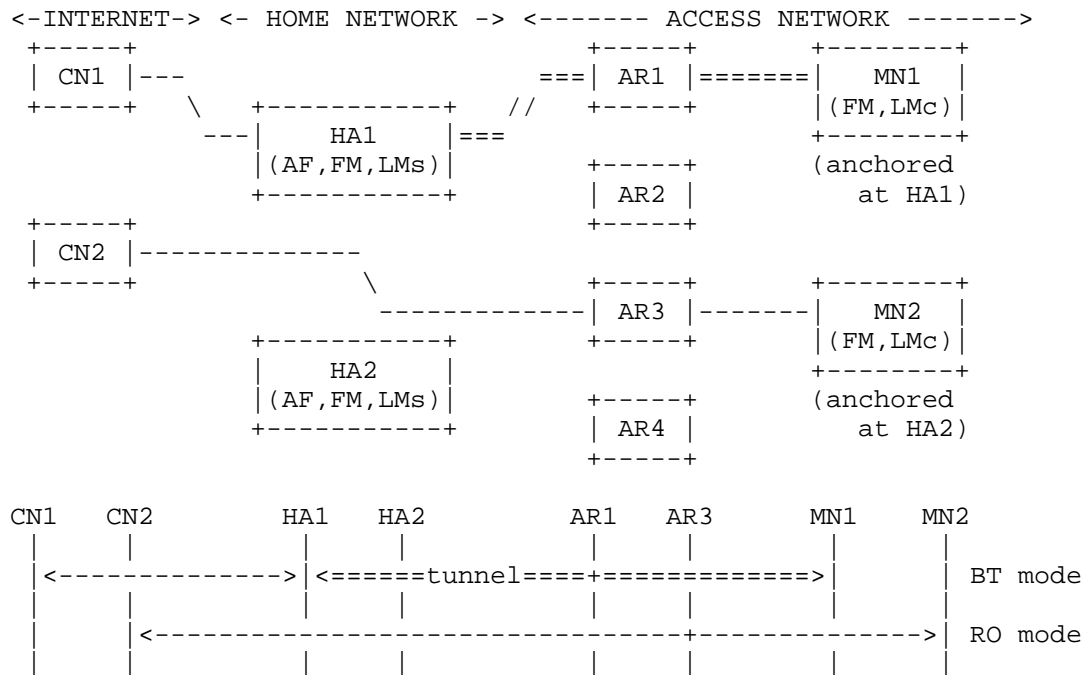


Figure 2: Distributed operation of Mobile IPv6 (BT and RO) / NEMO

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

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

- o The RO mode is only supported by Mobile IPv6. There is no route optimization support standardized for the NEMO protocol because of the security problems posed by extending return routability tests for prefixes, although many different solutions have been proposed [RFC4889].
- o The RO mode requires signaling that adds some protocol overhead.
- o The signaling required to enable RO involves the home agent and is repeated periodically for security reasons [RFC4225]. Therefore the HA remains a single point of failure.
- o The RO mode requires support from the CN.

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

Hierarchical Mobile IPv6 (HMIPv6) [RFC5380] (as shown in Figure 3), is another host-based IP mobility extension which can be considered as a complement to provide a less centralized mobility deployment. It allows the reduction of the amount of mobility signaling as well as improving the overall handover performance of Mobile IPv6 by introducing a new hierarchy level to handle local mobility. The Mobility Anchor Point (MAP) entity is introduced as a local mobility handling node deployed closer to the mobile node. It provides LI intermediary function between the LI server (LIs) at the HA and the LI client (LIc) at the MN. It also performs the FM function to tunnel with the HA and also with the MN.

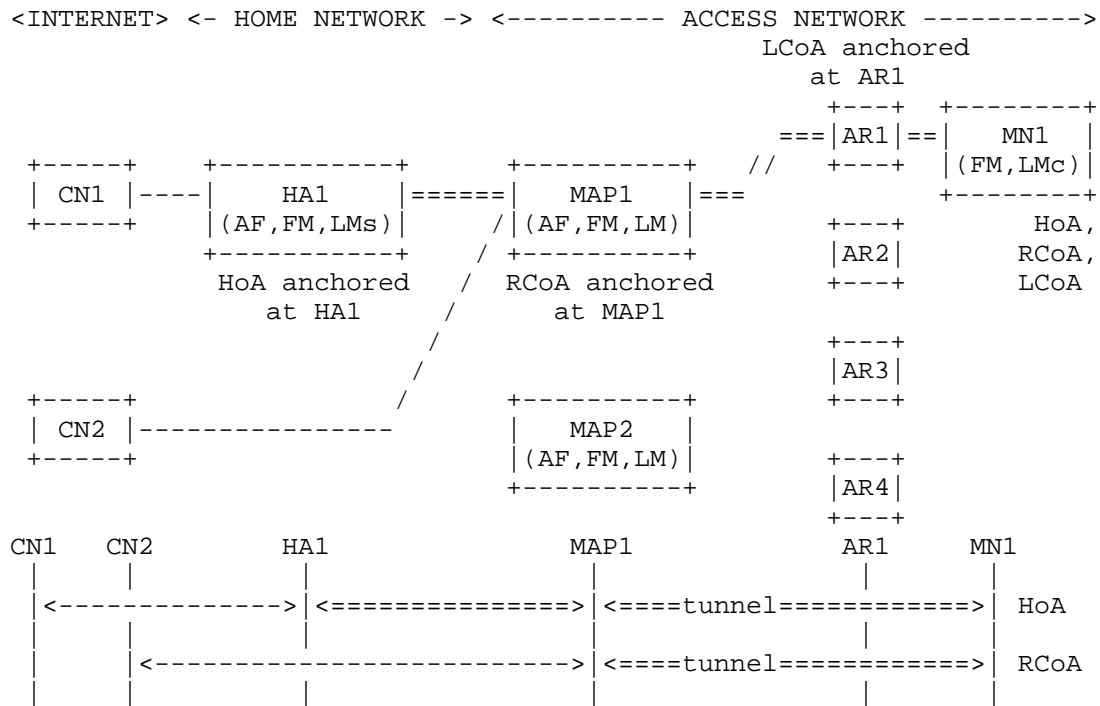


Figure 3: Hierarchical Mobile IPv6

When HMIPv6 is used, the MN has two different temporary addresses: the Regional Care-of Address (RCoA) and the Local Care-of Address (LCoA). The RCoA is anchored at one MAP, which plays the role of local home agent, while the LCoA is anchored at the access router level. The mobile node uses the RCoA as the CoA signaled to its home agent. Therefore, while roaming within a local domain handled by the same MAP, the mobile node does not need to update its home agent, i.e., the mobile node does not change its RCoA.

The use of HMIPv6 enables a form of route optimization, since a mobile node may decide to directly use the RCoA as source address for a communication with a given correspondent node, particularly if the MN does not expect to move outside the local domain during the lifetime of the communication. This can be seen as a potential DMM mode of operation, though it fails to provide session continuity if and when the MN moves outside the local domain. In the example shown in Figure 3, MN1 is using its global HoA to communicate with CN1, while it is using its RCoA to communicate with CN2.

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

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

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

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

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

4.2.2. Network-based IP DMM practices

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

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

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

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

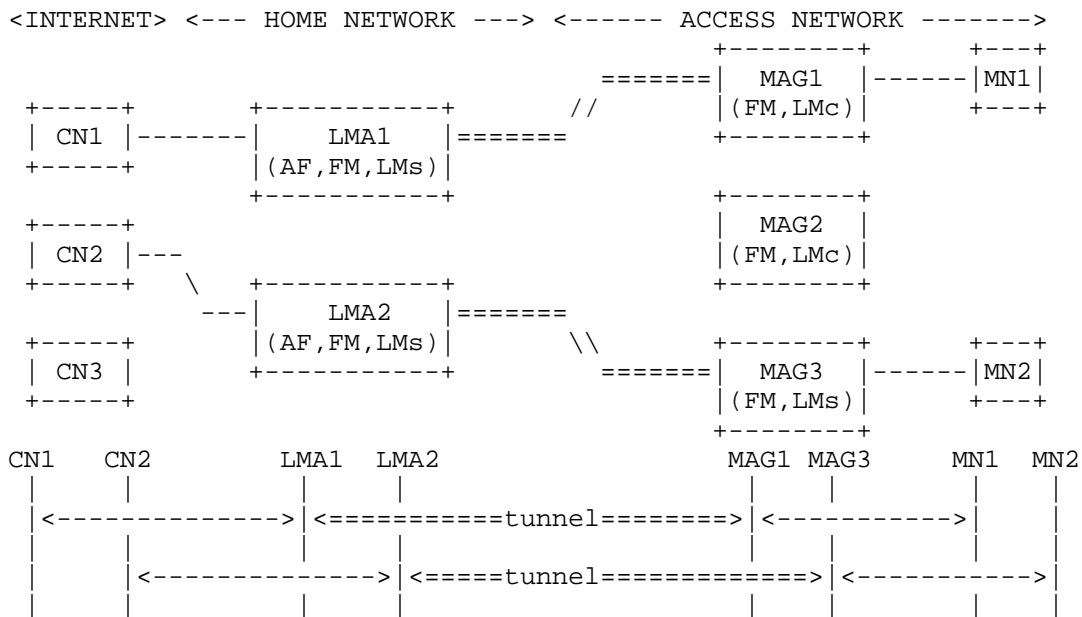


Figure 4: Distributed operation of Proxy Mobile IPv6

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

An interesting extension that can also be used to facilitate the deployment of network-based mobility protocols in a distributed mobility management environment is the support of LMA runtime assignment described in [RFC6463]. This extension specifies a runtime Local Mobility Anchor assignment functionality and corresponding mobility options for Proxy Mobile IPv6. This runtime Local Mobility Anchor assignment takes place during the Proxy Binding Update / Proxy Binding Acknowledgment message exchange between a mobile access gateway and a local mobility anchor. While this mechanism is mainly aimed for load-balancing purposes, it can also be used to select an optimal LMA from the routing point of view. A runtime LMA assignment can be used to change the assigned LMA of an MN, for example, in cases when the mobile node does not have any active session, or when the running sessions can survive an IP address change. Note that several possible dynamic Local Mobility Anchor discovery solutions can be used, as described in [RFC6097].

4.3. Flattening 3GPP mobile network approaches

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

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

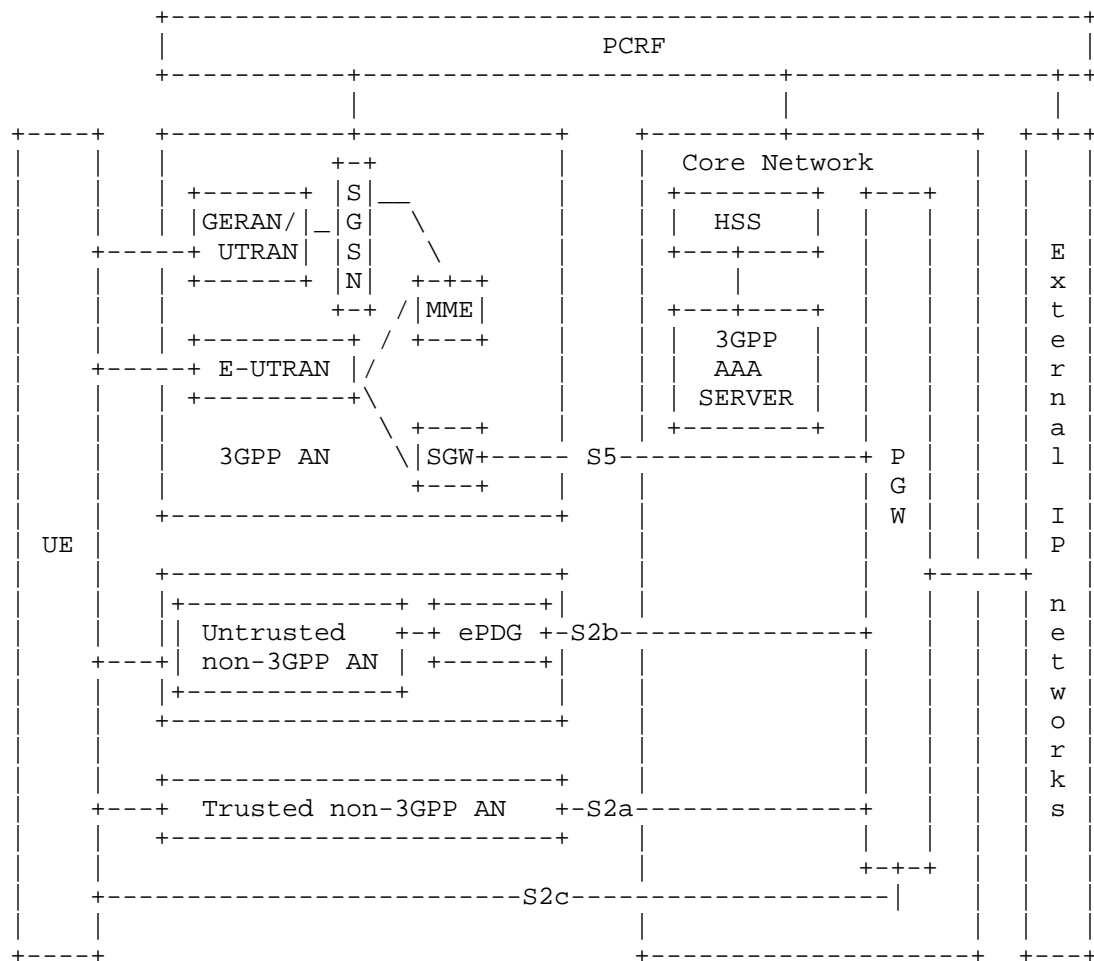


Figure 5: EPS (non-roaming) architecture overview

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

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

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

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

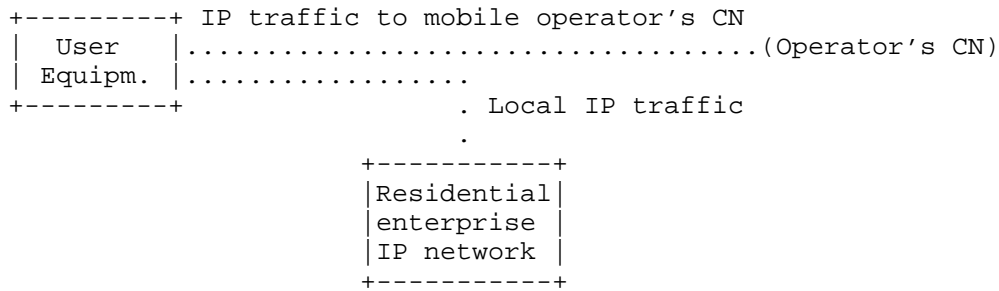


Figure 6: LIPA scenario

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

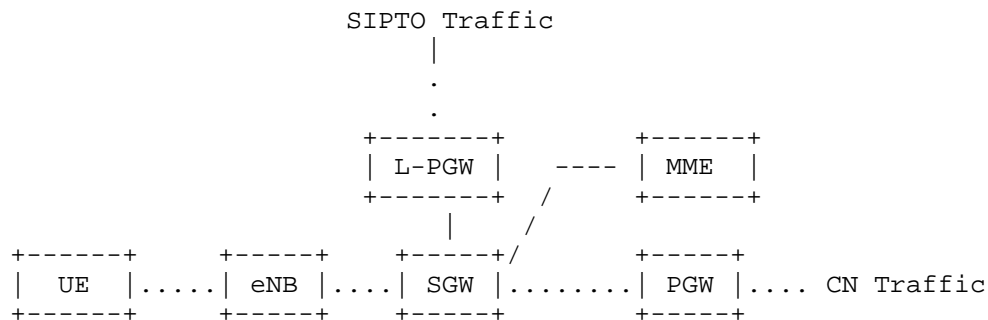


Figure 7: SIPTO architecture

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

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

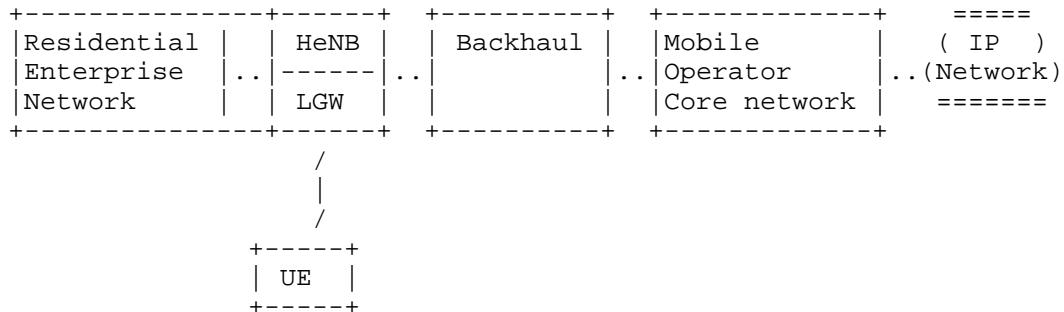


Figure 8: LIPA architecture

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

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

5. Gap analysis

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

5.1. Distributed mobility management - REQ1

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

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

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

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

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

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

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

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

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

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

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

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

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

- o Dynamically assign/relocate anchor: a mobility anchor is assigned only to sessions which use the network-layer mobility support. The MN may thus manage more than one session; some of them may be associated with anchored IP address(es), while the others may be associated with local IP address(es).
- o Multiple IP address management: this function is related to the preceding and is about the ability of the mobile node to simultaneously use multiple IP addresses and select the best one (from an anchoring point of view) to use on a per-session/application/service basis. This requires MN to acquire information regarding the properties of the available IP addresses.

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

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

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

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

5.3. IPv6 deployment - REQ3

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

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

5.4. Considering existing mobility protocols - REQ4

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

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

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

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

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

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

5.6. Operation and management considerations - REQ6

This requirement actually comprises several aspects, as summarized below.

- o 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.
- o A DMM solution has to describe in what environment and how it can be scalably deployed and managed.
- o A DMM solution has to support mechanisms to test if the DMM solution is working properly.
- o A DMM solution is expected to expose the operational state of DMM to the administrators of the DMM entities.
- o A DMM solution, which supports flow mobility, is also expected to support means to correlate the flow routing policies and the observed forwarding actions.
- o A DMM solution is expected to support mechanisms to check the liveness of the forwarding path.
- o A DMM solution has to provide fault management and monitoring mechanisms to manage situations where update of the mobility session or the data path fails.

- o A DMM solution is expected to be able to monitor the usage of the DMM protocol.
- o DMM solutions have to support standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules, which are expected to be created for DMM when needed for such configuration.

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

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

5.7. Security considerations - REQ7

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

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

5.8. Multicast - REQ8

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

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

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

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

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

5.9. Summary

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

- GAP1-1: Existing solutions only provide an optimal initial anchor assignment, a gap being the lack of dynamic anchor change/new anchor assignment. Neither the HA switch nor the LMA runtime assignment allows changing the anchor during an ongoing session. MOBIKE allows change of GW but its applicability has been scoped to a very narrow use case.
- GAP1-2: The MN needs to be able to perform source address selection. Proper mechanism to inform the MN is lacking to provide the basis for the proper selection.
- GAP1-3: Currently, there is no efficient mechanism specified by the IETF that allows the dynamic discovery of the presence of nodes that can play the role of anchor, discover their capabilities and allow the selection of the most suitable one. However, the following mechanisms could help discovering anchors:
- Dynamic Home Agent Address Discovery (DHAAD): the use of the home agent (H) flag in Router Advertisements (which indicates that the router sending the Router Advertisement is also functioning as a Mobile IPv6 home agent on the link) and the MAP option in Router Advertisements defined by HMIPv6.
- GAP1-4: While existing network-based DMM practices may allow the deployment of multiple LMAs and dynamically select the best

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

- GAP2-1: The information of which sessions at the mobile node are active and are using the mobility support need to be transferred to or shared with the network. Such mechanism has not been defined.
- GAP2-2: The mobile node needs to simultaneously use multiple IP addresses with different properties. There is a lack of mechanism to expose this information to the mobile node which can then update accordingly its source address selection mechanism.
- GAP2-3: The handling of mobility management has not been to the granularity of an individual session of a user/device before. The combination of session identification and user/device identification may be lacking.
- GAP6-1: Mobility management protocols have not thoroughly documented how, or whether, they support the following list of operation and management considerations:
- * A DMM solution needs to consider configuring a device, monitoring the current operational state of a device, responding to events that impact the device, possibly by modifying the configuration and storing the data in a format that can be analyzed later.
 - * A DMM solution has to describe in what environment and how it can be scalably deployed and managed.
 - * A DMM solution has to support mechanisms to test if the DMM solution is working properly.
 - * A DMM solution is expected to expose the operational state of DMM to the administrators of the DMM entities.
 - * A DMM solution, which supports flow mobility, is also expected to support means to correlate the flow routing policies and the observed forwarding actions.

- * A DMM solution is expected to support mechanisms to check the liveness of the forwarding path.
- * A DMM solution has to provide fault management and monitoring mechanisms to manage situations where update of the mobility session or the data path fails.
- * A DMM solution is expected to be able to monitor the usage of the DMM protocol.
- * DMM solutions have to support standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules, which are expected to be created for DMM when needed for such configuration.

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

6. Security Considerations

The deployment of DMM using existing IP mobility protocols raises similar security threats as those encountered in centralized mobility management systems. Without authentication, a malicious node could forge signaling messages and redirect traffic from its legitimate path. This would amount to a denial of service attack against the specific node or nodes for which the traffic is intended. Distributed mobility anchoring, while keeping current security mechanisms, might require more security associations to be managed by the mobility management entities, potentially leading to scalability and performance issues. Moreover, distributed mobility anchoring makes mobility security problems more complex, since traffic redirection requests might come from previously unconsidered origins, thus leading to distributed points of attack. Consequently, the DMM security design needs to account for the distribution of security associations between additional mobility entities and fulfill the security requirement of [RFC7333].

7. Contributors

This document has benefited to valuable contributions from

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

who had produced a matrix to compare the different mobility protocols and extensions against a list of desired DMM properties. They were useful inputs in the early work of gap analysis. He had continued to give suggestions as well as extensive review comments to this documents.

8. References

8.1. Normative References

- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
- [RFC7333] Chan, H., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", RFC 7333, August 2014.

8.2. Informative References

- [I-D.anipko-mif-mpvd-arch]
Anipko, D., "Multiple Provisioning Domain Architecture", draft-anipko-mif-mpvd-arch-05 (work in progress), November 2013.
- [I-D.bhandari-dhc-class-based-prefix]
Systems, C., Halwasia, G., Gundavelli, S., Deng, H., Thiebaut, L., Korhonen, J., and I. Farrer, "DHCPv6 class based prefix", draft-bhandari-dhc-class-based-prefix-05 (work in progress), July 2013.
- [I-D.gundavelli-v6ops-community-wifi-svcs]
Gundavelli, S., Grayson, M., Seite, P., and Y. Lee, "Service Provider Wi-Fi Services Over Residential Architectures", draft-gundavelli-v6ops-community-wifi-svcs-06 (work in progress), April 2013.
- [I-D.ietf-netext-pmip-cp-up-separation]
Wakikawa, R., Pazhyannur, R., Gundavelli, S., and C. Perkins, "Separation of Control and User Plane for Proxy Mobile IPv6", draft-ietf-netext-pmip-cp-up-separation-07 (work in progress), August 2014.
- [I-D.korhonen-6man-prefix-properties]
Korhonen, J., Patil, B., Gundavelli, S., Seite, P., and D. Liu, "IPv6 Prefix Properties", draft-korhonen-6man-prefix-properties-02 (work in progress), July 2013.

- [IEEE.802-16.2009]
"IEEE Standard for Local and metropolitan area networks
Part 16: Air Interface for Broadband Wireless Access
Systems", IEEE Standard 802.16, 2009,
<[http://standards.ieee.org/getieee802/
download/802.16-2009.pdf](http://standards.ieee.org/getieee802/download/802.16-2009.pdf)>.
- [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P.
Thubert, "Network Mobility (NEMO) Basic Support Protocol",
RFC 3963, January 2005.
- [RFC4066] Liebsch, M., Singh, A., Chaskar, H., Funato, D., and E.
Shim, "Candidate Access Router Discovery (CARD)", RFC
4066, July 2005.
- [RFC4067] Loughney, J., Nakhjiri, M., Perkins, C., and R. Koodli,
"Context Transfer Protocol (CXTF)", RFC 4067, July 2005.
- [RFC4225] Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E.
Nordmark, "Mobile IP Version 6 Route Optimization Security
Design Background", RFC 4225, December 2005.
- [RFC4295] Keeni, G., Koide, K., Nagami, K., and S. Gundavelli,
"Mobile IPv6 Management Information Base", RFC 4295, April
2006.
- [RFC4555] Eronen, P., "IKEv2 Mobility and Multihoming Protocol
(MOBIKE)", RFC 4555, June 2006.
- [RFC4640] Patel, A. and G. Giarretta, "Problem Statement for
bootstrapping Mobile IPv6 (MIPv6)", RFC 4640, September
2006.
- [RFC4889] Ng, C., Zhao, F., Watari, M., and P. Thubert, "Network
Mobility Route Optimization Solution Space Analysis", RFC
4889, July 2007.
- [RFC4960] Stewart, R., "Stream Control Transmission Protocol", RFC
4960, September 2007.
- [RFC5014] Nordmark, E., Chakrabarti, S., and J. Laganier, "IPv6
Socket API for Source Address Selection", RFC 5014,
September 2007.
- [RFC5026] Giarretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6
Bootstrapping in Split Scenario", RFC 5026, October 2007.

- [RFC5142] Haley, B., Devarapalli, V., Deng, H., and J. Kempf, "Mobility Header Home Agent Switch Message", RFC 5142, January 2008.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.
- [RFC5555] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.
- [RFC5568] Koodli, R., "Mobile IPv6 Fast Handovers", RFC 5568, July 2009.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.
- [RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.
- [RFC6020] Bjorklund, M., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, October 2010.
- [RFC6097] Korhonen, J. and V. Devarapalli, "Local Mobility Anchor (LMA) Discovery for Proxy Mobile IPv6", RFC 6097, February 2011.
- [RFC6224] Schmidt, T., Waehlich, M., and S. Krishnan, "Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains", RFC 6224, April 2011.
- [RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.
- [RFC6463] Korhonen, J., Gundavelli, S., Yokota, H., and X. Cui, "Runtime Local Mobility Anchor (LMA) Assignment Support for Proxy Mobile IPv6", RFC 6463, February 2012.
- [RFC6475] Keeni, G., Koide, K., Gundavelli, S., and R. Wakikawa, "Proxy Mobile IPv6 Management Information Base", RFC 6475, May 2012.

- [RFC6611] Chowdhury, K. and A. Yegin, "Mobile IPv6 (MIPv6) Bootstrapping for the Integrated Scenario", RFC 6611, May 2012.
- [RFC6697] Zorn, G., Wu, Q., Taylor, T., Nir, Y., Hoeper, K., and S. Decugis, "Handover Keying (HOKEY) Architecture Design", RFC 6697, July 2012.
- [RFC6705] Krishnan, S., Koodli, R., Loureiro, P., Wu, Q., and A. Dutta, "Localized Routing for Proxy Mobile IPv6", RFC 6705, September 2012.
- [RFC6724] Thaler, D., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, September 2012.
- [RFC7028] Zuniga, JC., Contreras, LM., Bernardos, CJ., Jeon, S., and Y. Kim, "Multicast Mobility Routing Optimizations for Proxy Mobile IPv6", RFC 7028, September 2013.
- [SDO-3GPP.23.401]
3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", 3GPP TS 23.401 10.10.0, March 2013.
- [SDO-3GPP.23.402]
3GPP, "Architecture enhancements for non-3GPP accesses", 3GPP TS 23.402 10.8.0, September 2012.
- [SDO-3GPP.24.303]
3GPP, "Mobility management based on Dual-Stack Mobile IPv6; Stage 3", 3GPP TS 24.303 10.0.0, June 2013.
- [SDO-3GPP.29.060]
3GPP, "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface", 3GPP TS 29.060 3.19.0, March 2004.
- [SDO-3GPP.29.274]
3GPP, "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3", 3GPP TS 29.274 10.11.0, June 2013.
- [SDO-3GPP.29.281]
3GPP, "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)", 3GPP TS 29.281 10.3.0, September 2011.

[SDO-3GPP.29.303]

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

Authors' Addresses

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

Email: liudapeng@chinamobile.com

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

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

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

Email: pierrick.seite@orange.com

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

Email: h.a.chan@ieee.org

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: <http://www.it.uc3m.es/cjbc/>

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.

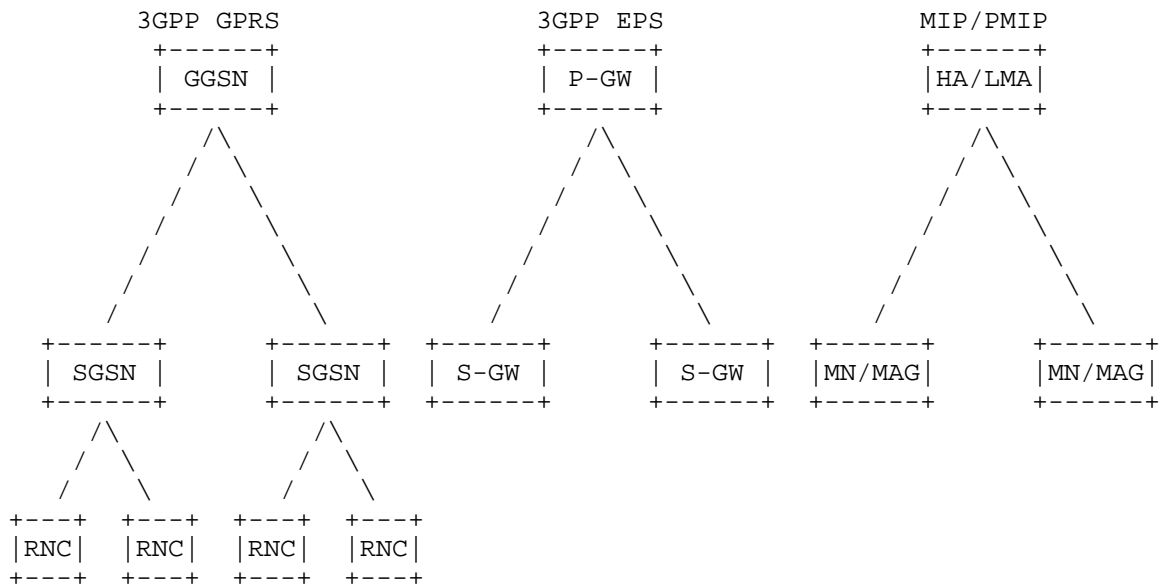


Figure 1. Centralized mobility management.

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.

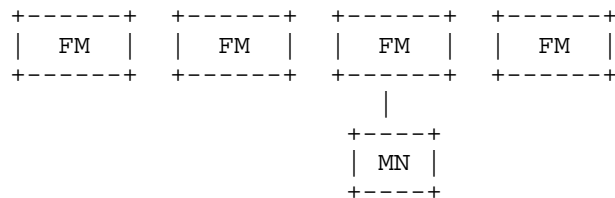


Figure 2. Distributed mobility management.

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 Working Group
Internet-Draft
Updates: 5014 (if approved)
Intended status: Standards Track
Expires: May 10, 2014

D. Liu
H. Deng
China Mobile
C. Perkins
Futurewei
November 06, 2013

Mobility API Extension for Distributed Mobility Management
draft-liu-dmm-mobility-api-02

Abstract

In order to provide an appropriate level of mobility support that a mobile node may require for proper performance of various applications, it is important to enable applications to select addresses that will be managed properly by the mobility management infrastructure. Previous documents have enabled address selection on the basis of certain characteristics such as randomness, temporary usage, scope of validity, and so on. This document proposes new classes of addresses in addition to those already available, to enable an application to receive certain kinds of mobility support.

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 10, 2014.

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	2
2. Terminology	2
3. Proposed Extension of RFC 5014	2
4. Usage Example	3
5. IANA Considerations	4
6. Security Considerations	4
7. Acknowledgements	4
8. References	4
8.1. Normative References	4
8.2. Informative References	4
Authors' Addresses	5

1. Introduction

An extension to the socket API (see [RFC5014]) has been specified to allow an application to identify its preference among multiple source addresses. Furthermore, there are proposals ([I-D.draft-korhonen-6man-prfix-properties] and [I-D.draft-bhandari-dhc-class-based-prefix-04]) to extend router advertisement to carry property and class information for the advertised prefixes. Those proposals enable a mobile node to learn the property and class information for the prefix from the router advertisement message. This document proposes an extension to [RFC5014] which would add more prefix classes so that an application could select prefixes with properties that are important for distributed mobility management.

2. 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 RFC 2119 [RFC2119].

3. Proposed Extension of RFC 5014

A socket API extension defined in [RFC5014] is used for IPv6 source address selection. An application can use this API to override the default source address selection mechanism for IPv6. Currently, the following types of source address selection preference are defined in [RFC5014]:

IPV6_PREFER_SRC_HOME /* Prefer Home address as source */

IPV6_PREFER_SRC_COA /* Prefer Care-of address as source */

IPV6_PREFER_SRC_TMP /* Prefer Temporary address as source */

IPV6_PREFER_SRC_PUBLIC /* Prefer Public address as source */

IPV6_PREFER_SRC_CGA /* Prefer CGA address as source */

IPV6_PREFER_SRC_NONCGA /* Prefer a non-CGA address as source */

This document proposes the addition of two new flags:

IPV6_PREFER_SRC_LOCAL_HNP /* Prefer a local home prefix */

IPV6_PREFER_SRC_REMOTE_HNP /* Prefer a remote home prefix */

The local home prefix may be preferred by applications which are likely to discontinue operations before the device travels to distant networks. On the other hand, a remote home prefix may be more suitable for continued operation over wide areas, but at potentially increased cost for mobility management.

4. Usage Example

This section gives usage examples for the new flags API extension.

Relevant distributed mobility management practices are discussed in [I-D.draft-ietf-dmm-best-practices-gap-analysis-01] and [I-D.draft-seite-dmm-dma-06]. The concept of dynamic anchoring concept is introduced, which means that the mobile node can have multiple mobility anchor points. Then, the mobile node can select a locally allocated IP address for newly launched applications for optimized routing. When the application continues communications while the mobile node moves to a new point of attachment, the mobile node can nevertheless still use the IP address allocated by previous anchor point for the on going communications. When the application terminates, the mobile node will release the IP address allocated by the previous anchor point.

In the dynamic anchoring scenario, the newly started application should use an IP address allocated by the local mobility anchor. The application can use IPV6_PREFER_SRC_LOCAL_HNP flag to select the local allocated IP address. For more long-lived communications, the application can use IPV6_PREFER_SRC_REMOTE_HNP flag to select the home address allocated by the previous mobility anchor to enable session continuity.

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. Acknowledgements

TBD

8. References

8.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC5014] Nordmark, E., Chakrabarti, S., and J. Laganier, "IPv6 Socket API for Source Address Selection", RFC 5014, September 2007.

8.2. Informative References

- [I-D.draft-bhandari-dhc-class-based-prefix-04]
 , "DHCPv6 class based prefix ", draft-bhandari-dhc-class-based-prefix-04 (work in progress), February 2013.
- [I-D.draft-ietf-dmm-best-practices-gap-analysis-01]
 , "Distributed Mobility Management: Current practices and gap analysis ", draft-ietf-dmm-best-practices-gap-analysis-01 (work in progress), June 2013.
- [I-D.draft-korhonen-6man-prfix-properties]
 , "IPv6 Prefix Properties", draft-korhonen-6man-prfix-properties (work in progress), February 2013.

[I-D.draft-seite-dmm-dma-06]
 , "Distributed Mobility Anchoring", draft-seite-dmm-dma-06
 (work in progress), Nov 2013.

Authors' Addresses

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

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

Hui Deng
China Mobile
32 Xuanwumen West Street
Beijing, Xicheng District 100053
China

Email: denghui@chinamobile.com

Charles E. Perkins
Futurewei Inc.
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1-408-330-5305
Email: charliep@computer.org

Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 09, 2014

D. Liu
H. Deng
China Mobile
July 08, 2013

Mobility Support in Software Defined Networking
draft-liu-sdn-mobility-00

Abstract

This document discusses the SDN mobility problem and potential 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 January 09, 2014.

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	2
2. Conventions and Terminologies	2
2.1. Conventions used in this document	2
2.2. Terminology	2
3. Motivation of SDN mobility	2
4. SDN mobility problem analysis and potential solutions	3
4.1. Enhance SDN to support mobility tunnel handling.	3
4.2. Routing based SDN mobility support	4
5. Security Considerations	5
6. IANA Considerations	5
7. References	5
7.1. Normative References	5
7.2. Informative References	5
Authors' Addresses	6

1. Introduction

Software defined networking provides a very flexible way to process IP packets and flows. It decouples the control and forwarding function of traditional IP appliance. IP mobility support has been specified by IETF. There is currently not much discussion regarding the mobility support in SDN network. This document discusses the motivation, problem and potential solution of the mobility support in SDN network.

2. Conventions and Terminologies

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

SDN: Software Defined Networking

3. Motivation of SDN mobility

IP mobility support has been specified in IETF for years. Both [RFC2002], [RFC3775], [RFC5555],[RFC5213] share the similar idea that it introduce an anchoring point to maintain the mapping of the home address and routing address of the mobile node. It uses tunnel to encapsulate the user traffic so that the application layer is not aware of the mobility event.

IP protocol has been used intensively in current cellular network architecture. For example, in LTE network architecture, IP support is enabled in the data plane. Also In the control plane and mobility support, IP mobility protocol is used. Both S2a/S2b/S2c interface is specified that can based on IP mobility protocol.

There is ongoing research work and discussions of using SDN in cellular network. SDN can provide the IP packets processing ability for the cellular core network. Mobility support is critical for the cellular core network. If mobility can be supported by SDN, the cellular core network can be significantly simplified. The data plane traffic routing can also be optimized. The following figure shows an architecture of the cellular core network that build upon SDN concept.

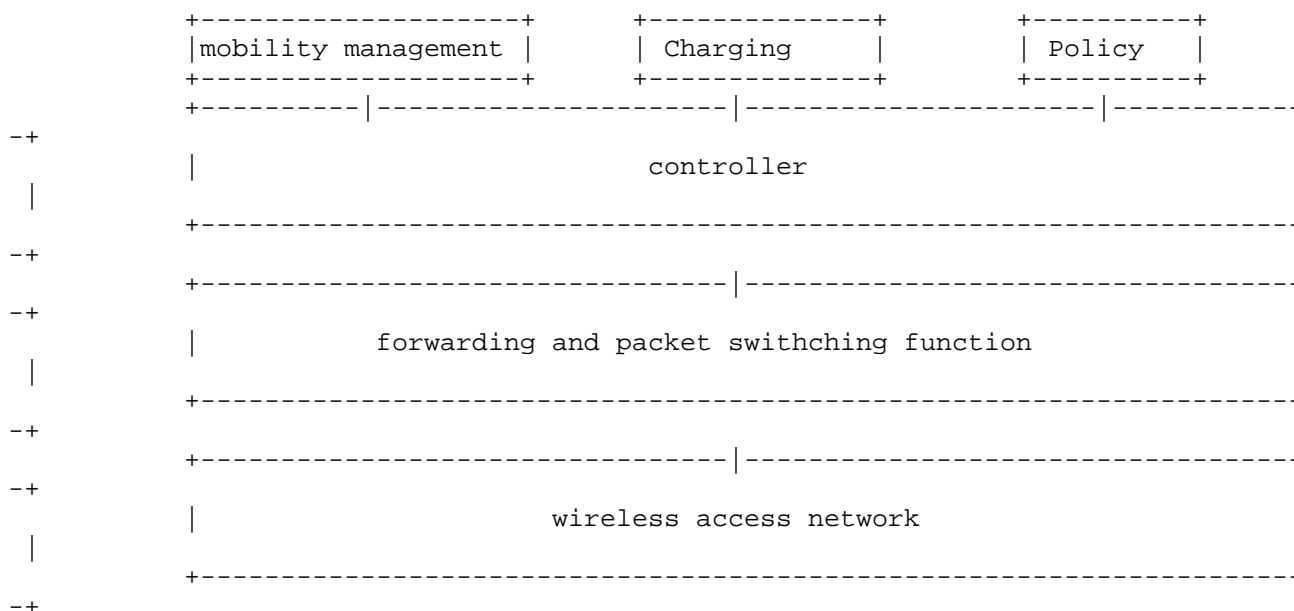


Figure 1. SDN based Mobile core network

4. SDN mobility problem analysis and potential solutions

The purpose of mobility management is to maintain the session continuity from the application's perspective. Normally, when a mobile node change its attachment point, its IP address will be changed accordingly. If there is no mobility support, the application layer session will be broken. For example, TCP session can not survive when the source IP address changes.

There are several potential ways for SDN network to support mobility. The following sections will discuss the potential solution in detail.

4.1. Enhance SDN to support mobility tunnel handling.

Current mobility protocol mainly follows the concept of mobility anchor. Mobility anchor point maintain the mapping of home address

and routing address. For example, in Mobile IP, the home agent maintain the mapping of home address and care of address. When the care of address changes due to mobile node's movement, the foreign agent or the mobile node will send binding update request to the home agent to update the binding cache entry. The foreign agent or the mobile node will set up bi-directional tunnel towards the home agent. All the user traffic will be encapsulated in the bi-directional tunnel.

To enable SDN to support mobility, one potential solution is to enable the SDN controller and SDN forwarding function to support IP mobility protocol related tunnelling processing.

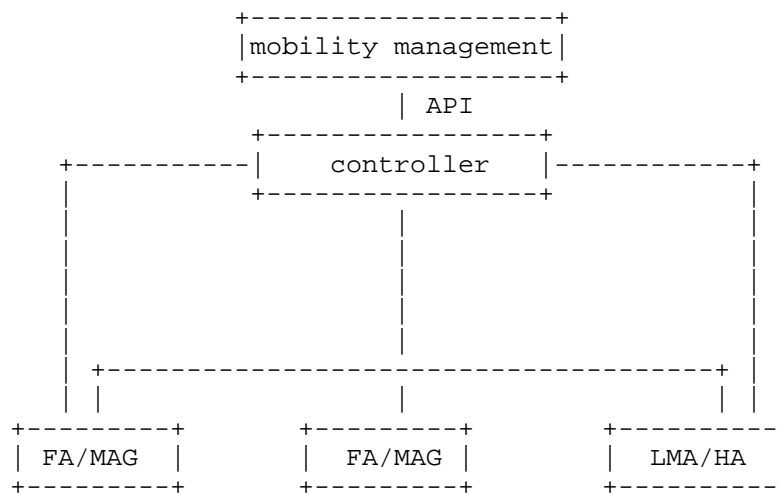


Figure 2. Enhance SDN to support mobility tunnel processing

The mobility management function could run on top of the controller. The controller controls the forwarding function. To support mobility, the mobility management function monitors the mobile node's movement event. When the FA/MAG detects the mobile node's movement, it needs to update the binding cache entry that maybe maintained in the mobility management function. The mobility management function then control the forwarding function(FA/MAG) to do the mobility tunnel processing. When the packets arrives at the LMA/HA, the mobility management function will controll the forwarding function to decapsulate the packets and forward the packets to the Internet.

4.2. Routing based SDN mobility support

SDN provides a very flexible way of packet and flow processing. It is in nature can react quickly on the routing changes of the network. When the mobile node changes its point of attachment, the forwarding function will notify the mobility management function running on top of the controller, the controller then calculate the forwarding rules based on the destination IP address of the IP packet. The controller then push the forwarding rules to the forwarding function and the IP packet will be forwarded accordingly. When the user session terminated, the mobility management function will delete the forwarding rules. In this manner, the application layer session continuity will be guaranteed since the mobile node's IP address is not changed during the movement.

There are lots of interesting problems need to be solved to make SDN support mobility. For example, the forwarding function needs to detect the movement event of the mobile node and notify the controller and mobility management function in a timely manner. A routing path needs to be set up from the MAG/FA to the Internet access point in a timely manner. To achieve this, new protocol and mechanism may need to be defined in IETF.

5. Security Considerations

TBD

6. IANA Considerations

None

7. References

7.1. Normative References

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

7.2. Informative References

[RFC2002] Perkins, C., "IP Mobility Support", RFC 2002, October 1996.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

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

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

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

Authors' Addresses

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

Hui Deng
China Mobile
32 Xuanwumen West Street
Beijing, Xicheng District 100053
China

Email: denghui@chinamobile.com

INT Area
Internet-Draft
Intended status: Informational
Expires: May 11, 2014

R. Wakikawa
Softbank Mobile
S. Matsushima
Softbank Telecom
B. Patil
Individual
B. Chen
Sprint
D. Joachimpillai(DJ)
Verizon Labs
H. Deng
China Mobile
November 07, 2013

Requirements and use cases for separating control and user planes in
mobile network architectures
draft-wakikawa-req-mobile-cp-separation-00

Abstract

Virtualization and cloud services have evolved significantly in the last few years. Additionally trends in virtualization like Network Function Virtualization and Software Defined Networking are bound to have implications to mobile network architectures of cellular systems (3G/4G), WiFi and others. IETF has developed a number of mobility protocols that are used in the industry today. Mobility network architectures continue to evolve and it is likely that they will embrace virtualization and cloud services trends as well. The IETF can play a role in defining the mobility protocols that support architectures which leverage virtualization and cloud technologies. This document captures several use cases and requirements for a virtualized mobile network architecture.

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, 2014.

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	2
2. Motivation: Virtualization	3
3. Requirements	4
4. Use Cases	6
5. Potential of New Mobile Architecture	6
6. IANA Considerations	8
7. Security Considerations	8
8. References	9
8.1. Normative References	9
8.2. Informative References	9
Authors' Addresses	10

1. Introduction

The concept of User- and control- plane are well-known in networking. Especially, the 3rd Generation Partnership Project (3GPP) employs this concept in their mobile network architecture. These two planes are conceptually decoupled in the 3GPP architecture.

In the past, IETF has developed tunnel based mechanisms for mobile nodes such as Mobile IPv6 [RFC6275][RFC5555], Proxy Mobile IPv6 [RFC5213][RFC5844] and NEMO [RFC3963]. All the mobility protocols discussed in the past are summarized in [RFC6301]. Similarly, 3GPP has developed another tunnel protocol called GPRS Tunneling Protocol (GTP). These tunnel- based protocol creates a data path for a mobile node between the mobile node and an anchor point (s). There is a case where an access router terminates a tunnel instead of a mobile node (ex. Proxy Mobile IP). In the 3GPP architecture, a tunnel is established between Serving Gateway and PDN Gateway per a mobile node

by either Proxy Mobile IPv6 or GTP (at s5 interface). The signaling like Binding Update and user's packets are routed along a same path in Evolved Packet Core (EPC). Therefore, the control and the user planes of these mobility protocols are tightly related and cannot be clearly decoupled, although there are several implementation efforts.

2. Motivation: Virtualization

The recent innovations and trends of Software Defined Networking (SDN) and NFV (Network Function Virtualization) promotes to decouple User and Control planes. SDN consists of two entities named a controller and a vSwitch. The controller is responsible for signaling exchange and the vSwitches handles data forwarding based on the states fed by the controller. There are various controller that user can program vSwitch dynamically to adjust and optimize networks on the fly. Controller are often implemented with Virtualization technology and run as a software on hypervisors. On the other hand, NFV is discussed at the ETSI NFV ISG and is introduced in [NFV-WHITEPAPER]. Operators build its network with variety of proprietary hardware appliances today. If they can get rid of these physical appliances and could shift to a cloud-based service, they will have a lot of benefits, specially CAPEX and OPEX reduction. This document assumes that SDN and NFV will impact our daily network operations and managements. Expected network functions are Mobility Management Entity (MME), Serving Gateway (SGW) PDN Gateway(PGW), etc. With NFV, EPC can be operated onto servers/hyper-visors. We name it virtualized-EPC (vEPC) in this document. NFV will bring networking functions currently run on dedicated hardware onto a cloud network.

It is good timing to re-visit the basic architecture of mobility system. Although the tunneling-based protocols are sustaining mobile traffic, SDN and NFV can introduce a new architecture that truly decoupled user- and control planes. This document summarizes requirements of the new architecture and its potential use cases.

Benefits of NFV are summarized below. Detailed explanation can be found in [NFV-WHITEPAPER]). As a potential drawback, today's eco-system of mobile appliances might be affected. However, we believe there are various approaches to enhance current eco-system and migrate to new mobility approach.

- o [Flexible Network Operations]: The control functions are no longer in appliances deployed widely in operator's network and can be run at hypervisor (cloud). It is easier to add and/ or delete functions from the services, because no physical construction is needed. Network operations will be much simpler and easier because complications of today's network are pushed to NFV (i.e. hypervisor).

- o [Flexible Resource Managements]: The network functions can be run on hypervisor and are now less dependent on proprietary hardware. Adding additional resources is easier in hypervisor, while adding or replacing physical appliances require installation, construction, configuration, and even migration plan without service cutoff. NFV also brings multi-tenancy and allows a single platform for different services and users. The operator can optimize resources and costs to share a NFV platform for multiple customers (ex. MVNO customers) and services (ex. multiple APNs).
- o [Faster Speed of Time to Market]: When an operator wants a new function to its network and services, the operator needs to negotiate appliance vendors to implement the new functions or to find alternative equipment supporting the new function. It takes a longer time to convince the vendors, or to replace existing hardware. However, if functions can be implemented as a software, it is much faster to implement the functions on NFV. Even the operator may implement them and try the new functions by themselves. Field trial is also getting easier because of no physical installation or replacement. You may turn on a new function in NFV and observe how the new function behaves in your network. NFV can save preparation time and tuning time of the new function.
- o [Cost Optimization]: Last but not least, Cost is the most important motivation for operators to realize NFV. Operators can remove many of proprietary appliances from its network and replace them with industry standard servers, switches and routers. In addition, it is easy to scale up and down operator's services so that resources can be always tuned to the size of services. In addition, operational costs led by any physical hardware such as power supply, maintenance, installation, construction and replacement can be minimized or even removed. The network design can be simpler, because complicated functions could be handled by NFV. That simple operation may enable automatic configurations and prevent unnecessary trouble-shooting. As a result, CAPEX and OPEX can be always optimized and lowered.

3. Requirements

What is a role of IETF to discuss mobility architecture? IETF is not the right place to discuss, for instance, how to achieve virtualization or NFV. An important IETF activity must be to decouple the control- and user- planes of mobility protocols. IETF also should design and standardize protocols as building block of the new mobility architecture. In doing so, the new mobility solutions can be easily designed and implemented with interoperability across multiple vendors and platforms. Otherwise, NFV solutions can be

easily fragmented due to many proprietary solutions for the protocol separations. As stated in [NFV-WHITEPAPER], interoperability is highly important.

This section lists up requirements of the new mobility architecture.

Separation of Control- and User- Planes

Due to tight relationship of the control- and user- planes in today's mobile architecture, resource increase is always provisioned to both planes at once. It prevents flexible resource arrangement and introduces high capital investment and over-provisioned resources to one of planes. If NFV is deployed, it is expected that computing resources can be independently allocated to the control planes in a flexible manner.

Flat Design for Distributed Operation

Today's 3GPP architecture introduces PDN gateway (PGW) as a gateway to external networks like the Internet. PGW manages all traffic from and to UEs and could be a bottleneck and single point of failure of network connectivity. In addition, due to recent rapid traffic increase, it is important to perform traffic engineering and to offload traffic to multiple locations (ex. SGW, PGW, eNodeB). For enhancements of traffic engineering capability, more flat design with multiple gateways is expected so that traffic can be distributed to all these gateways. There were proposals how to enable flat design to (Proxy) Mobile IP such as [I-D.wakikawa-mext-haha-interop2008] in IETF. Distributed Mobility Management (DMM) Working Group has also discussed how to extend Mobile IP-based solutions to support traffic distribution in an optimal way by removing centrally deployed anchors that is like a Home Agent.

Stateless in User Plane

Ultimate goal of vEPC is to remove all mobility specific states from the forwarding nodes in the user-plane of vEPC. If we succeed in this, industry standard routers and switches can be used to forward mobile nodes traffic in the user plane of vEPC. A mobile node's specific states are kept in both an IP header of the mobile node's packets and a routing entry of the mobile node.

Shared backbone for fixed and mobile convergence

If User plane focus only on packet forwarding, the user plane can be shared for both fixed and mobile services. Most of mobile operators have wired services and could share the backbone. With recent state-of-arts of routing technology,

it is reasonable to assume that routing system can dynamically propagate networking state information available on Control plane. Thus, both mobile and fixed packets are routed only on the user plane. No special treatment is needed for packets of mobile nodes and vice versa.

Packet Processing Support: DPI, Accounting, Firewall
In the today's mobile system like EPC-based cellular system, mobile packets are inspected and examined for various services and accounting such as DPI, FireWall, NAT, AAA, and so on. This is one of the reason that all packets are processed in the control plane. However, these L4-L7 services are also expected to be virtualized along with NFV and SDN trends. In IETF, there is an effort of SFC (Service Function Chaining) to discuss this topics. A new mechanism or trigger to provide these network services to mobile packets are needed on the user plane.

4. Use Cases

Use cases of the new mobility architecture are networks with local mobility support. Global mobility is not target of our activity. Global and local mobility are defined in [RFC3753]. Typical examples of local mobility network are cellular network (EPC: Evolved Packet Core), WiMAX, service provider WiFi and so on. Our use cases should meet the following characteristics.

- o A same provider conceptually provide access network (i.e. user plane) and mobility support (i.e. control plane).
- o A provider should be able to setup a route for the mobile node dynamically on the user plane according to the status on control plane.

Network access and mobility management are conceptually provided by a same provider. That is to say that a mobile ndoe only moves in the provider's network, i.e. local mobility.

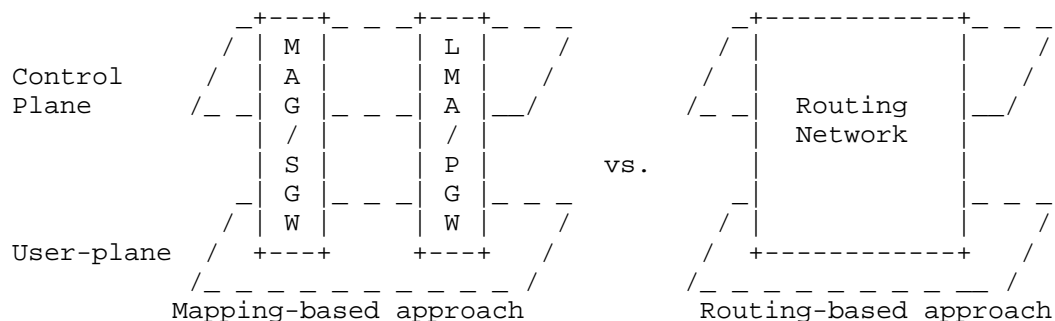
5. Potential of New Mobile Architecture

[RFC6301] investigates the mobile architecture and classifies into 2 approaches such as Routing-Based and Mapping-Based Approaches, described in Figure 1. Both approaches do not take account of control and user planes separation.

- o Routing-based approach: Mobility is provided by dynamic routing. A mobile node keeps its IP address regardless of its point of attachments. Dynamic routing mechanism keeps track of a mobile

node's movements and updates routing tables so as to support continuous reachability.

- o Mapping-based approach: Mobility is achieved by a mapping between mobile node's identifier and dynamically assigned IP address at an attachment point. This mapping is managed in networks and updated every time a mobile node moves. Packets are first routed to the node managing the mapping and redirected to a mobile node according to the mapping. This redirection is often implemented by a tunneling mechanism. Mobile IP is the most famous protocol of this approach.



2 approaches of Mobile Architecture

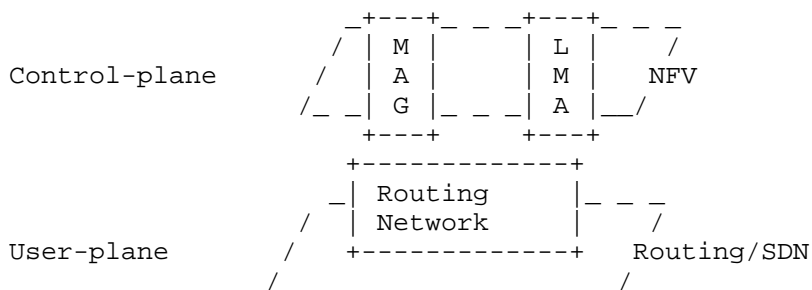
Figure 1

As we mentioned earlier, the most of mobility protocols deployed today uses the mapping-based approach. There is a good reason of adapting mapping and tunneling in mobility protocols, that is global mobility and signaling. A mobile node should be able to move anywhere on the Internet and be reachable from anyone on the Internet. There were routing based global mobility solutions like Boeing global mobility [Boeing-BGP] and WINMO [RFC6301]. In these proposals, BGP was used to propagate forwarding information of mobile nodes to the Internet. Whenever a mobile node changes its point of attachment, the route must be updated. Due to scalability and stability issues of the Internet, this solution was not recommended by IETF [Boeing-BGP]. However, as Boeing showed, it is doable to support global mobility by using BGP routing update. If scalability is not your concern, a routing based approach becomes a candidate of the mobility solution.

While global mobility is important, today's "reality" is that your cell phones (i.e. UE or mobile node) are moving just within an

operator's network and fully controlled in your local managed domain (ex. EPC). If mobility support can be limited within an operator, we believe a routing based approach is feasible and practical for today's mobile system.

If the concept of NFV and SDN were realized and deployed, we could have strong tools to split control and user planes. Figure 2 shows a possibility that nodes on the Control plane are virtualized in generic cloud environment, however user packets won't go through those virtualized nodes. Instead of dedicated proprietary equipment like MAG and LMA to process signaling of mobility support, virtualized software running on hypervisor will take care of signaling on the control plane. After signaling completion, the status is reflected as forwarding information to switches and routes in the user plane. The reflection can be implemented by routing or SDN solutions. As a result, packets to and from mobile nodes are no longer tunneled between MAG and LMA but they are directly routed on the user plane. Figure 2 could relax hyper-visor and data-path capacity requirements. The user plane will be agnostic from sessions and bearers states, of which are generated and maintained in the Control-plane. It forwards the packets based on a destination address of packets and routing entries injected by the control plane.



New Mobility architecture

Figure 2

6. IANA Considerations

This memo includes no request to IANA.

7. Security Considerations

There are no security considerations specific to this document at this moment.

8. References

8.1. Normative References

- [I-D.vandeveldde-idr-remote-next-hop]
Velde, G., Patel, K., Rao, D., Raszuk, R., and R. Bush,
"BGP Remote-Next-Hop", draft-vandeveldde-idr-remote-next-hop-03 (work in progress), October 2012.
- [RFC5512] Mohapatra, P. and E. Rosen, "The BGP Encapsulation Subsequent Address Family Identifier (SAFI) and the BGP Tunnel Encapsulation Attribute", RFC 5512, April 2009.

8.2. Informative References

- [Boeing-BGP]
Andrew, ., "Global IP Network Mobility using Border Gateway Protocol (BGP)", IAB Plenary IAB Plenary of IETF 62nd, March 2005.
- [I-D.ietf-softwire-map]
Troan, O., Dec, W., Li, X., Bao, C., Matsushima, S., Murakami, T., and T. Taylor, "Mapping of Address and Port with Encapsulation (MAP)", draft-ietf-softwire-map-07 (work in progress), May 2013.
- [I-D.savolainen-stateless-pd]
Savolainen, T. and J. Korhonen, "Stateless IPv6 Prefix Delegation for IPv6 enabled networks", draft-savolainen-stateless-pd-01 (work in progress), February 2010.
- [I-D.wakikawa-mext-haha-interop2008]
Wakikawa, R., Shima, K., and N. Shigechika, "The Global HAHA Operation at the Interop Tokyo 2008", draft-wakikawa-mext-haha-interop2008-00 (work in progress), July 2008.
- [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.
- [NFV-WHITEPAPER]
Network Operators, ., "Network Functions Virtualization, An Introduction, Benefits, Enablers, Challenges and Call for Action", SDN and OpenFlow SDN and OpenFlow World Congress, October 2012.

- [RFC3753] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.
- [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5555] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
- [RFC6301] Zhu, Z., Wakikawa, R., and L. Zhang, "A Survey of Mobility Support in the Internet", RFC 6301, July 2011.
- [RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, August 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.
- [RFC6877] Mawatari, M., Kawashima, M., and C. Byrne, "464XLAT: Combination of Stateful and Stateless Translation", RFC 6877, April 2013.

Authors' Addresses

Ryuji Wakikawa
Softbank Mobile
1-9-1, Higashi-Shimbashi, Minato-Ku
Tokyo 105-7322
Japan

Email: ryuji.wakikawa@gmail.com

Satoru Matsushima
Softbank Telecom
1-9-1, Higashi-Shimbashi, Minato-Ku
Tokyo 105-7322
Japan

Email: satoru.matsushima@g.softbank.co.jp

Basavaraj Patil
Individual

Email: bpatill@gmail.com

Bonnie Chen
Sprint
6220 Sprint Parkway
Overland Park, KS 66251
USA

Email: Bonnie.Chen@Sprint.com

Damascene Joachimpillai (DJ)
Verizon Labs

Email: damascene.joachimpillai@verizon.com

Hui Deng
China Mobile
53A, Xibianmennei Ave., Xuanwu District
Beijing 100053
China

Email: denghui02@gmail.com

dmm
Internet-Draft
Intended status: Informational
Expires: March 31, 2014

C. Xiong
J. Liu
Huawei Technologies
September 27, 2013

MN IP reachablility for the DMM
draft-xiong-dmm-ip-reachability-00

Abstract

In distributed mobility management (DMM) environment, the mobile node (MN) has more than one IP addresses and can use different IP address to communicate with different hosts.

When a new correspondent node (CN) initials an IP session with MN, the CN needs to find and select one of the MN's IP addresses to best (e.g. with low delay) for the IP session..

This draft provides two solutions to find and select of MN's IP addresses, one is DDNS[rfc 2136]-based solution, the other is Server Register-based solution.

Status of This Memo

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

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

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

This Internet-Draft will expire on March 31, 2014.

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	2
2. Terminology and Abbreviation	3
2.1. Conventions Used in This Document	3
2.2. Terminology	3
3. Problem Statement	3
4. Solutions	4
4.1. Solution1: DDNS server	4
4.2. Solution2: Server Registration	5
4.2.1. P2P mode	5
4.2.2. Server Central mode	6
4.2.3. Combined mode	7
5. Security Considerations	8
6. IANA Considerations	8
7. Acknowledgments	8
8. Normative Reference	8
Authors' Addresses	9

1. Introduction

In distributed mobility management (DMM) environment, the mobile node (MN) has more than one IP addresses and can use different IP address to communicate with different hosts.

When a new correspondent node (CN) initials an IP session with MN, the CN needs to find and select one of the MN's IP addresses to best (e.g. with low delay) for the IP session..

This draft provides two solutions to find and select of MN's IP addresses, one is DDNS[rfc 2136]-based solution that MN registers its new IP address to DDNS server, and CN obtains the MN's new IP address info from DDNS server, then initials an IP session to the MN. The other is Server Register-based solution that MN and CN both register their new IP addresses and ports info to the same server for a given service, e.g., MSN messenger and there are three methods for CN to obtain the MN's IP address info and initial an IP session to the MN, which are P2P mode, server central mode, and combined mode.

P2P mode: CN directly initials a new IP session to MN with the help of retrieved info from server.

Server central mode: CN initials a new IP session to MN, which has to pass through the server.

Combined mode: for control plane, CN initials the connection to MN by Server central mode. For user plane, CN initials the IP session to MN by P2P mode.

2. Terminology and Abbreviation

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

MR: Mobile Router

CN: Correspondent Node

DDNS: Distributed DNS

GUID: Global Unique ID

P2P: Peer To Peer

3. Problem Statement

In distributed mobility management (DMM) environment, mobile node(MN) always has more than one IP addresses to communicate with other ends. There is no problem for MN to initial a new IP session with any other CN by using MN's latest IP address, so we provide solutions below based on requirement initialed by CN. However, when a new correspondent node(CN) initials an IP session with MN, CN doesn't know how to choose MN's IP address and which one to choose.

MN attached to MR1, and MN initials the IP1 session with CN1 through MR1 using IP1 allocated by MR1. When MN moves, and attaches to MR2, MN1 initials the IP2 session with CN2 using IP2 allocated by MR2, IP1 session continuity is still kept .

Then, a new CN3 initials a new IP session with MN1, there are some problems to be solved.

1) How CN3 to get MN1's IP address?

2) Which IP address for CN3 to choose? Why?

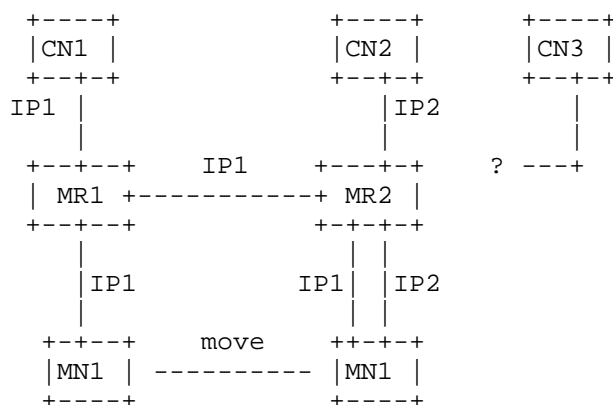


Figure 1: MN routing with multiple IP addresses

4. Solutions

4.1. Solution1: DDNS server

In this solution, each MN has a global unique ID (GUID), e.g. FQDN [RFC4703] , and DDNS server are needed to store MN's latest IP address and port info. When MN1 attached to MR1, MN1 registers its new IP1 address, port info and MN1 ID to DDNS server, and MN1 initials the IP1 session with CN1, as described in Fig2. When MN1 moves and attaches to MR2, MN1 registers its new IP2 address, port info and MN1 ID to DDNS server, and MN1 initials the IP2 session with CN2; IP1 session continuity is kept.

At the moment, CN3 initials a new IP session with MN1, firstly CN3 has to requests MN1's latest IP address and port info from DDNS server, and DDNS Server responses with MN1's latest IP address and port info, then CN3 directly initials to setup the IPx session between CN3 with returning info above. If CN3 cached MN1 IP address, CN3 initials to setup IP session with MN1 using the cached IP address.

However, There still needs some additional functions or mechnism to support for this solution:

- 1) There needs a mechnism to allocate a permanent GUID for MN, because currently, not each GUID is allocated for a MN permanently.

2) There still needs a way (out scope of this draft) for CN3 to acquire MN ID and DDNS server address.

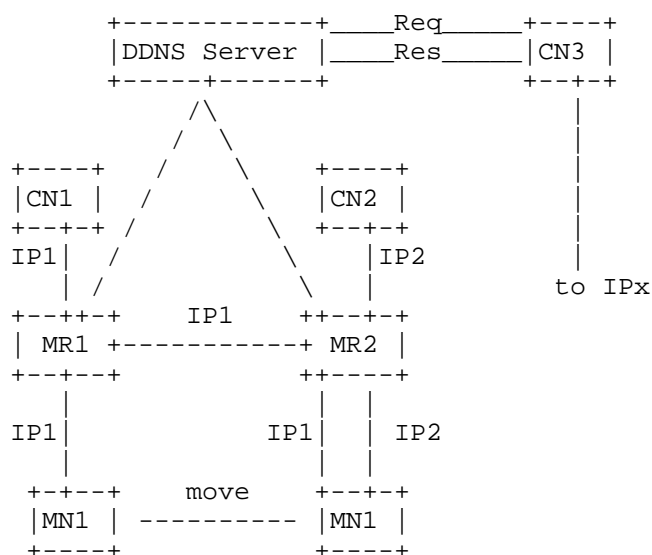


Figure 2: MN's IP reachability with DDNS server

4.2. Solution2: Server Registration

In this solution, for some special service, e.g., MSN Messenger, MN1 and CN3 both register their IP addresses and posts info to the same server, after attaching to new MR, they register their new IP addresses and ports info to server again. There are three mode for CN to initial a new IP session with MN, which is including P2P mode[RFC5694], Server central mode and Combined mode.

4.2.1. P2P mode

At the beginning, CN3 registered its new IP address to Server. When CN3 initials a new IP session with MN1, firstly, CN3 sends "service request to MN1" message to server, and server retures MN1's latest IP address and port info to CN3, CN3 directly initials to setup the new IP session with MN1 using the returing info above, as described in Fig3.

When MN1 attaches to a new MR, and updates the server with a new IP address, the established IP session between MN1 and CN3 is unaffected and IP session continuity is kept. The CN3 does not need to cache MN1 IP address, since if CN3 initials a new IP session with MN1 again, the server will provide MN1's latest IP address and port info to CN3 by sending the "Service Request to MN1" message to server.

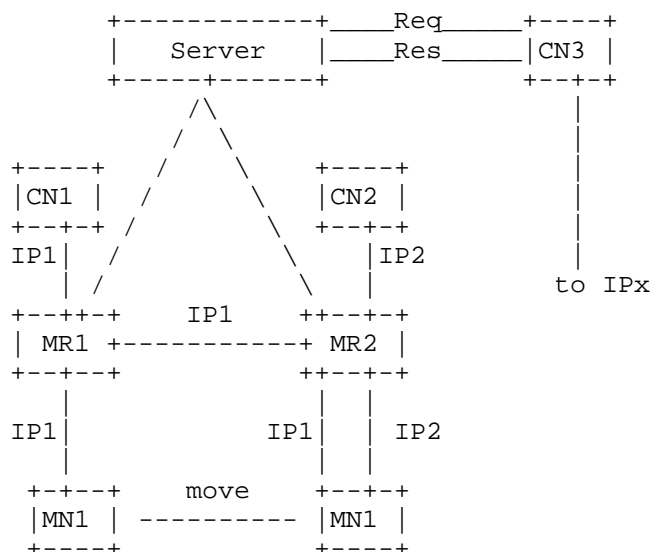


Figure 3: MN's reachability with Server Registration by P2P mode

4.2.2. Server Central mode

At the beginning, CN3 registered its new IP address and port info to Server. When CN3 initials a new IP session with MN1, as described in Fig4, firstly, CN3 sends "service request to MN1" message to server, and then, server sends "service request from CN3" message to MN1. After that CN3 initial to setup the path "CN3 --- Server --- MN1" for user and control plane.

In this mode, MN1 can use another IP address to setup the user plane, in this case the MN1 does not need to immediately update the server with new IP address. In this way, the session continuity is kept but the servicer (e.g. IMS) must supports two user plane.

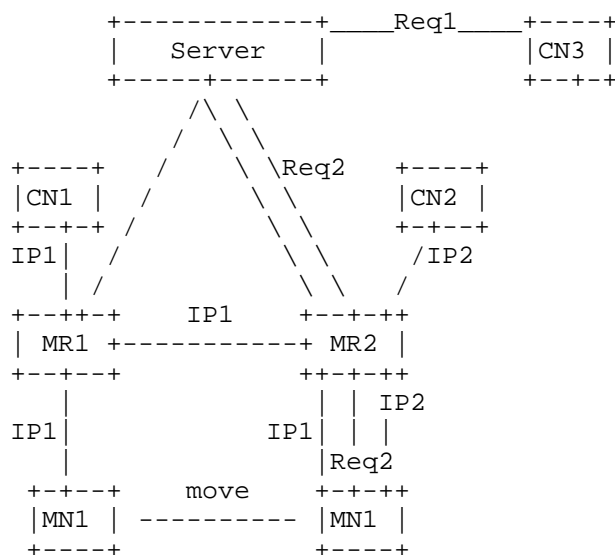
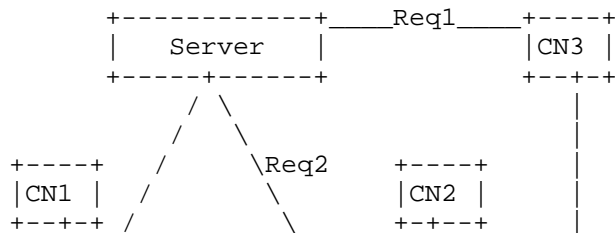


Figure 4: MN's reachability with Server Registration by Server central mode

4.2.3. Combined mode

Combined mode: combining P2P mode and Server Central mode.

In this mode, for control plane, CN3 sends "service request to MN1" message to server, and server sends "service request from MN1" message to MN1, the server is in the path of the signaling path between the CN3 and MN1, as described in Fig5. For data plane, MN1 responses the request from server with MN1's latest IP address and port info, and the server returns the info to CN3, and CN3 directly initial to setup new IP session between CN3 and MN1 with the returning info above.



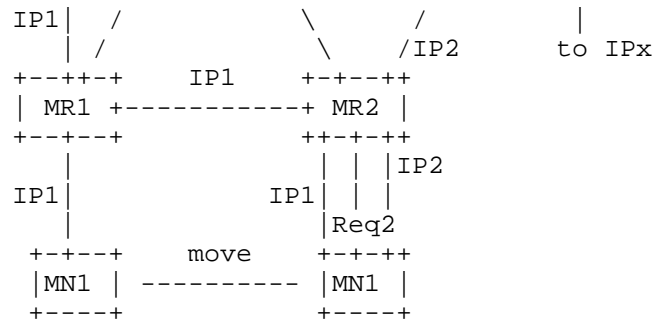


Figure 5: MN's reachability with Server Registration by Combined mode

5. Security Considerations

TBD.

6. IANA Considerations

This document needs a mechanism to allocate permanent GUID for a MN described in Section 4.1, which is to be made through IANA Expert Review.

7. Acknowledgments

Thanks to my colleagues for their sincerely help and comments when drafting this document.

8. Normative Reference

- [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.
- [RFC4703] Stapp, M. and B. Volz, "Resolution of Fully Qualified Domain Name (FQDN) Conflicts among Dynamic Host Configuration Protocol (DHCP) Clients", RFC 4703, October 2006.

[RFC5694] Camarillo, G. IAB, "Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability", RFC 5694, November 2009.

Authors' Addresses

Chunshan Xiong
Huawei Technologies
BeiQing Road No.156
HaiDian District , Beijing 100095
China

Email: sam.xiongchunshan@huawei.com

Jianning Liu
Huawei Technologies
BeiQing Road No.156
HaiDian District , Beijing 100095
China

Email: liujianning.liu@huawei.com

DMM Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 04, 2014

A. Yegin
K. Kweon
J. Lee
J. Park
Samsung
July 03, 2013

On Demand Mobility Management
draft-yegin-dmm-ondemand-mobility-00

Abstract

Applications differ with respect to whether they need IP session continuity and/or IP address reachability. The network providing the same type of service to any mobile host and any application running on the host yields inefficiencies. This document describes a solution for taking the application needs into account in selectively providing IP session continuity and IP address reachability on a per-socket basis.

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 January 04, 2014.

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	2
2. Notational Conventions	3
3. Solution	4
3.1. Types of IP Addresses	4
3.2. Granularity of Selection	5
3.3. On Demand Nature	5
3.4. Conveying the Selection	6
4. Security Considerations	7
5. IANA Considerations	8
6. References	8
6.1. Normative References	8
6.2. Informative References	8
Authors' Addresses	9

1. Introduction

In the context of Mobile IP [RFC5563][RFC6275][RFC5213][RFC5944], following two attributes are defined for the IP service provided to the mobile hosts:

IP session continuity: The ability to maintain an ongoing IP session by keeping the same local end-point IP address throughout the session despite moving among different IP networks. The IP address of the host may change between two independent IP sessions, but that does not jeopardize the IP session continuity. IP session continuity is essential for mobile hosts to maintain ongoing IP sessions without any interruption.

IP address reachability: The ability to maintain the same IP address for an extended period of time. The IP address shall stay the same across independent IP sessions, and even in the absence of any IP session. The IP address may be published in a long-term registry (e.g., DNS), and it shall be available for serving incoming (e.g., TCP) connections. IP address reachability is essential for mobile hosts to use specific/published IP addresses.

Mobile IP is designed to provide both IP session continuity and IP address reachability to mobile hosts. Architectures utilizing these protocols (e.g., 3GPP, 3GPP2, WIMAX) ensure that every one of the mobile hosts attached to the compliant networks enjoy these benefits. Every application running on each one of those mobile hosts is

subjected to the same treatment with respect to the IP session continuity and IP address reachability.

It should be noted that in reality not every application may need those benefits. IP address reachability is required for applications running as servers (e.g., a camera mounted on a bus). But, a typical client application (e.g., web browser) does not necessarily require IP address reachability. Similarly, IP session continuity is not required for all types of applications either. Applications performing brief communication (e.g., DNS client) can survive without having IP session continuity support.

Achieving IP session continuity and IP address reachability by using Mobile IP incur some cost. This solution forces the mobile host's IP traffic to traverse a centrally-located router (Home Agent, HA), which incurs additional transmission latency and use of additional network resources, adds to the network CAPEX and OPEX, and decreases the reliability of the network with the introduction of a single point of failure [I-D.ietf-dmm-requirements]. Therefore, IP session continuity and IP address reachability should be used selectively.

Furthermore, even when an application needs IP session continuity, it may be able to satisfy that need by using a solution above the IP layer, such as MPTCP [RFC6824], SIP mobility [RFC3261], or an application-layer mobility solution. Those higher-layer solutions are not subject to the same issues that arise with the use of Mobile IP since they can utilize the most direct data path between the end-points. But, if Mobile IP is being applied to the mobile host, those higher-layer protocols are rendered useless because their operation is inhibited by the Mobile IP. Since Mobile IP ensures the IP address of the mobile host remains fixed (despite the location and movement of the mobile host), the higher-layer protocols never detect the IP-layer movement and never engage in mobility management.

This document proposes a solution where the applications running on the mobile host can indicate whether they need IP session continuity or IP address reachability. The IP stack on the mobile host, in conjunction with the network, would provide the required type of IP service. It is for the benefit of both the users and the network operators not to engage an extra level of service unless it is absolutely necessary. So it is expected that applications and networks compliant with this specification would utilize this solution to use network resources more efficiently.

2. Notational 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 [RFC2119].

3. Solution

3.1. Types of IP Addresses

Three types of IP addresses are defined with respect to the mobility management.

- Home Network Anchored Address

This is what standard Mobile IP provides with a Home Address (HoA). The mobile host is configured a HoA from a centrally-located Home Network. Both IP session continuity and IP address reachability are provided to the mobile host with the help of a router in the Home Network (Home Agent, HA). This router acts as an anchor for the IP address of the mobile host.

- Access Network Anchored Address

This type of IP address provides IP session continuity but not IP address reachability. It is achieved by ensuring that the IP address used at the beginning of the session remains usable despite the movement of the mobile host. But the IP address may change after the end of ongoing IP sessions, therefore it does not exhibit persistence.

The IP address is allocated by a serving IP gateway. When the mobile host moves to another network, the previously serving gateway becomes an anchor gateway and starts treating the IP address as a Home Address with the help of the received binding updates. A tunnel is established between the anchor gateway and the current care-of address of the mobile host (whether configured on the host itself [RFC5944][RFC6275], or on the serving gateway [RFC5213][RFC5563]) for ensuring the session continuity using the same IP address.

- Unanchored Address

This type of IP address provides neither IP session continuity nor IP address reachability. The IP address is obtained from the serving IP gateway and it is not maintained across gateway changes. In other words, the IP address may be released and replaced by a new IP address when the IP gateway changes due to the mobile host's mobility.

Applications running as servers at a published IP address require Home Network Anchored Address. Long-standing applications (e.g., an SSH session) may also require this type of address. They could use Access Network Anchored Address, but that can produce sub-optimal results if the mobile host ends up far from the anchor gateway. Enterprise applications that connect to an enterprise network via virtual LAN require Home Network Anchored Address.

Applications with short-lived transient IP sessions can use Access Network Anchored Address. For example: Email client, web browser, calendar, app store client, etc.

Applications with very short IP sessions, such as DNS client and instant messengers, can utilize Unanchored Address. Even though they could very well use Home or Access Network Anchored Addresses, the transmission latency would be the minimum when an Unanchored Address is used.

3.2. Granularity of Selection

The IP address type selection is made at per-socket granularity. Different parts of the same application may have different needs. For example, control part of the application may require Home Network Anchored Address in order to stay reachable, whereas data part of the application may be satisfied with Access Network Anchored Address.

3.3. On Demand Nature

At any point in time, a mobile host may have any mixture of IP addresses configured. Zero or more Unanchored, zero or more Access Network Anchored, and zero or more Home Network Anchored IP addresses may be available on the IP stack of the host. The mixture may be as a result of the host policy, or as a result of the application demand.

If an IP address of the requested type is not available, then the IP stack shall attempt to configure one. For example, a host may not always have a Home Network Anchored IP address available as this is rarely used. In case an application requests one, then the IP stack shall make an attempt to configure one using Mobile IP. If Mobile IP is not available to the host, or if its operation fails, then the IP stack shall fail the associated socket request. In case of successful Mobile IP operation, a Home Network Anchored IP Address gets configured on the mobile host. If another socket requests a Home Network Anchored IP address at a later time, then the same IP address may be served to that socket as well. When the last socket using the requested IP address is closed, the IP address may be released.

The following are matters of policy, which may be dictated by the host itself, the network operator, or the compliant network architecture:

- The initial set of IP addresses configured on the host at the boot time.
- Permission to grant various types of IP addresses to a requesting application.
- Determination of a default address type when an application does not make any explicit indication, whether it already supports the required API or it is a legacy application.

3.4. Conveying the Selection

The selection of the address type is conveyed from the applications to the IP stack in a way to influence the source address selection algorithm [RFC6724].

The current source address selection algorithm operates on the available set of IP addresses when selecting an address. According to the proposed solution, if the requested type IP address is not available at the time of the request, then the IP stack shall make an attempt to configure one such IP address. The selected IP address shall be compliant with the requested IP address type, whether it is selected among available addresses or dynamically configured. In the absence of a matching type (because it is not available and not configurable on demand), the source address selection algorithm shall return an empty set.

A Socket API-based interface for enabling applications to influence the source address selection algorithm is described in [RFC5014]. That specification defines IPV6_ADDR_PREFERENCES option at the IPPROTO_IPV6 level. That option can be used with setsockopt() and getsockopt() calls to set and get address selection preferences.

Furthermore, that RFC also specifies two flags that relate to IP mobility management: IPV6_PREFER_SRC_HOME and IPV6_PREFER_SRC_COA. These flags are used for influencing the source address selection to prefer either a Home Address or a Care-of Address.

Unfortunately, these flags do not satisfy the aforementioned needs due to the following reasons, therefore new flags are proposed in this document:

- Current flags indicate a "preference" whereas there is a need for indicating "requirement". Source address selection algorithm does

not have to produce an IP address compliant with the "preference" , but it has to produce an IP address compliant with the "requirement".

- Current flags influence the selection made among available IP addresses. The new flags force the IP stack to configure a compliant IP address if none is available at the time of the request.

- The Home vs. Care-of Address distinction is not sufficient to capture the three different types of IP addresses described in Section 2.1.

The following new flags are defined in this document and they shall be used with Socket API in compliance with the [RFC5014]:

```
IPV6_REQUIRE_HOME_ANCHORED /* Require Home Anchored address as source */
```

```
IPV6_REQUIRE_ACCESS_ANCHORED /* Require Access Anchored address as source */
```

```
IPV6_REQUIRE_UNANCHORED /* Require Unanchored address as source */
```

More than one of these flags may be set on the same socket. In that case, an IP address compliant with any one of them shall be selected.

When any of these new flags is used, then the IPV6_PREFER_SRC_HOME and IPV6_PREFER_SRC_COA flags, if used, shall be ignored.

These new flags are used with `setsockopt()/getsockopt()`, `getaddrinfo()`, and `inet6_is_srcaddr()` functions [RFC5014]. Similar with the `setsockopt()/getsockopt()` calls, `getaddrinfo()` call shall also trigger configuration of the required type IP address, if one is not already available. When the new flags are used with `getaddrinfo()` and the triggered configuration fails, the `getaddrinfo()` call shall ignore that failure (i.e., not return an error code to indicate that failure). Only the `setsockopt()` shall return an error when configuration of the requested type IP address fails.

Application of this solution to IPv4 is TBD.

4. Security Considerations

The setting of certain IP address type on a given socket may be restricted to privileged applications. For example, a Home Anchored IP Address may be provided as a premium service and only certain applications may be allowed to use them. Setting and enforcement of such privileges are outside the scope of this document.

5. IANA Considerations

TBD

6. References

6.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC5014] Nordmark, E., Chakrabarti, S., and J. Laganier, "IPv6 Socket API for Source Address Selection", RFC 5014, September 2007.
- [RFC6724] Thaler, D., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, September 2012.

6.2. 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-05 (work in progress), June 2013.
- [RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5563] Leung, K., Dommety, G., Yegani, P., and K. Chowdhury, "WiMAX Forum / 3GPP2 Proxy Mobile IPv4", RFC 5563, February 2010.
- [RFC5944] Perkins, C., "IP Mobility Support for IPv4, Revised", RFC 5944, November 2010.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
- [RFC6824] Ford, A., Raiciu, C., Handley, M., and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses", RFC 6824, January 2013.

Authors' Addresses

Alper Yegin
Samsung
Istanbul
Turkey

Email: alper.yegin@partner.samsung.com

Kisuk Kweon
Samsung
Suwon
South Korea

Email: kisuk.kweon@samsung.com

Jinsung Lee
Samsung
Suwon
South Korea

Email: js81.lee@samsung.com

Jungshin Park
Samsung
Suwon
South Korea

Email: shin02.park@samsung.com