Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 13, 2013

H. Chan (Ed.)
Huawei Technologies

July 12, 2012

Requirements of distributed mobility management
draft-ietf-dmm-requirements-01

Abstract

The traditional hierarchical structure of cellular networks has led to deployment models which are heavily centralized. Mobility management with centralized mobility anchoring in existing hierarchical mobile networks is quite prone to suboptimal routing and issues related to scalability. Centralized functions present a single point of failure, and inevitably introduce longer delays and higher signaling loads for network operations related to mobility management. This document defines the requirements for distributed mobility management for IPv6 deployment. The objectives are to match the mobility deployment with the current trend in network evolution, to improve scalability, to avoid single point of failure, to enable transparency to upper layers only when needed, etc. The distributed mobility management also needs to be compatible with existing network deployments and end hosts, and be secured.

Status of this Memo

This Internet-Draft will expire on January 13, 2013.

Copyright Notice

Table of Contents

1. Introduction

In the past decade a fair number of mobility protocols have been standardized. Although the protocols differ in terms of functions and associated message format, we can identify a few key common features:

> presence of a centralized mobility anchor providing global reachability and an always-on experience;
>
> extensions to optimize handover performance while users roam across wireless cells;
>
> extensions to enable the use of heterogeneous wireless interfaces for multi-mode terminals (e.g. cellular phones).

The presence of the centralized mobility anchor allows a mobile device to be reachable when it is not connected to its home domain. The anchor point, among other tasks, ensures reachability of forwarding of packets destined to or sent from the mobile device. Most of the deployed architectures today have a small number of centralized anchors managing the traffic of millions of mobile subscribers. Compared with a distributed approach, a centralized approach is likely to have several issues or limitations affecting performance and scalability, which require costly network dimensioning and engineering to resolve.

To optimize handovers from the perspective of mobile nodes, the base protocols have been extended to efficiently handle packet forwarding between the previous and new points of attachment. These extensions are necessary when applications impose stringent requirements in terms of delay. Notions of localization and distribution of local agents have been introduced to reduce signaling overhead. Unfortunately today we witness difficulties in getting such protocols deployed, often leading to sub-optimal choices.

Moreover, the availability of multi-mode devices and the possibility of using several network interfaces simultaneously have motivated the development of more new protocol extensions. Deployment is further complicated with so many extensions.

Mobile users are, more than ever, consuming Internet content; such traffic imposes new requirements on mobile core networks for data traffic delivery. When the traffic demand exceeds available capacity, service providers need to implement new strategies such as selective traffic offload (e.g. 3GPP work items LIPA/SIPTO) through alternative access networks (e.g. WLAN). Moreover, the localization of content providers closer to the Mobile/Fixed Internet Service

Providers network requires taking into account local Content Delivery Networks (CDNs) while providing mobility services.

When demand exceeds capacity, both offloading and CDN techniques could benefit from the development of mobile architectures with fewer levels of routing hierarchy introduced into the data path by the mobility management system. This trend in network flattening is reinforced by a shift in users traffic behavior, aimed at increasing direct communications among peers in the same geographical area. Distributed mobility management in a truly flat mobile architecture would anchor the traffic closer to the point of attachment of the user and overcome the suboptimal routing issues of a centralized mobility scheme.

While deploying [Paper-Locating.User] today’s mobile networks, service providers face new challenges. More often than not, mobile devices remain attached to the same point of attachment. Specific IP mobility management support is not required for applications that launch and complete while the mobile device is connected to the same point of attachment. However, the mobility support has been designed to be always on and to maintain the context for each mobile subscriber as long as they are connected to the network. This can result in a waste of resources and ever-increasing costs for the service provider. Infrequent mobility and intelligence of many applications suggest that mobility can be provided dynamically, thus simplifying the context maintained in the different nodes of the mobile network.

The DMM charter addresses two complementary aspects of mobility management procedures: the distribution of mobility anchors to achieve a more flat design and the dynamic activation/deactivation of mobility protocol support as an enabler to distributed mobility management. The former has the goal of positioning mobility anchors (HA, LMA) closer to the user; ideally, these mobility agents could be collocated with the first hop router. The latter, facilitated by the distribution of mobility anchors, aims at identifying when mobility must be activated and identifying sessions that do not impose mobility management -- thus reducing the amount of state information to be maintained in the various mobility agents of the mobile network. The key idea is that dynamic mobility management relaxes some constraints so that it may avoid the establishment of non-optimal tunnels between two topologically distant anchors.

This document describes the motivations of distributed mobility management in Section 1. Section 3 compares distributed mobility management with centralized mobility management. The requirements to address these problems are given in Section 4.

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

2. 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].

2.1. 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 mobile node (MN), correspondent node (CN), home agent (HA), local mobility anchor (LMA), mobile access gateway (MAG), and context.

In addition, this draft introduces the following term.

Mobility context

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

3. Centralized versus distributed mobility management

Mobility management functions may be implemented at different layers of the network protocol stack. At the IP (network) layer, they may reside in the network or in the mobile node. In particular, a network-based solution resides in the network only. It therefore enables mobility for existing hosts and network applications which are already in deployment but lack mobility support.

At the IP layer, a mobility management protocol to achieve session continuity is typically based on the principle of distinguishing between identifier and routing address and maintaining a mapping between them. With Mobile IP, the home address serves as an identifier of the device whereas the care-of-address takes the role of routing address, and the binding between them is maintained at the mobility anchor, i.e., the home agent. If packets can be continuously delivered to a mobile device at its home address, then all sessions using that home address can be preserved even though the routing or care-of address changes.

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

3.1. Centralized mobility management

With centralized mobility management, the mapping information between the stable node identifier and the changing IP address of a mobile node (MN) is kept at a centralized mobility anchor. Packets destined to an MN are routed via this anchor. In other words, such mobility management systems are centralized in both the control plane and the data plane.

Many existing mobility management deployments make use of centralized mobility anchoring in a hierarchical network architecture, as shown in Figure 1. Examples of such centralized mobility anchors are the home agent (HA) and local mobility anchor (LMA) in Mobile IPv6 [RFC6275] and Proxy Mobile IPv6 [RFC5213], respectively. Current mobile networks such as the Third Generation Partnership Project (3GPP) UMTS networks, CDMA networks, and 3GPP Evolved Packet System (EPS) networks also employ centralized mobility management, with Gateway GPRS Support Node (GGSN) and Serving GPRS Support Node (SGSN) in the 3GPP UMTS hierarchical network and with Packet data network Gateway (P-GW) and Serving Gateway (S-GW) in the 3GPP EPS network.

```
          UMTS                3GPP SAE              MIP/PMIP
        +------+              +------+              +------+
        | GGSN |              | P-GW |              |HA/LMA|
        +------+              +------+              +------+
           /\                    /\                    /\
          /  \                  /  \                  /  \
         /    \                /    \                /    \
        /      \              /      \              /      \
       /        \            /        \            /        \
   +------+  +------+    +------+  +------+    +------+  +------+
   | SGSN |  | SGSN |    | S-GW |  | S-GW |    |MN/MAG|  |MN/MAG|
   +------+  +------+    +------+  +------+    +------+  +------+
```

Figure 1. Centralized mobility management.

3.2. Distributed mobility management

Mobility management functions may also be distributed to multiple locations in different networks as shown in Figure 2, so that a mobile node in any of these networks may be served by a closeby mobility function (MF).

```
+------+  +------+  +------+  +------+
|  MF  |  |  MF  |  |  MF  |  |  MF  |
+------+  +------+  +------+  +------+
                       |
                      ----
                     | MN |
                      ----
```

Figure 2. Distributed mobility management.

Mobility management may be partially distributed, i.e., only the data plane is distributed, or fully distributed where both the data plane and control plane are distributed. These different approaches are described in detail in [I-D.yokota-dmm-scenario].

[Paper-New.Perspective] discusses some initial steps towards a clear definition of what mobility management may be, to assist in better developing distributed architecture. [Paper-Characterization.Mobility.Management] analyses current mobility solutions and proposes an initial decoupling of mobility management into well-defined functional blocks, identifying their interactions, as well as a potential grouping, which later can assist in deriving more flexible mobility management architectures. According to the split functional blocks, this paper proposes three ways into which mobility management functional blocks can be grouped, as an initial way to consider a better distribution: location and handover management, control and data plane, user and access perspective.

A distributed mobility management scheme is proposed in [Paper-Distributed.Dynamic.Mobility] for future flat IP architecture consisting of access nodes. The benefits of this design over centralized mobility management are also verified through simulations in [Paper-Distributed.Centralized.Mobility].

Before designing new mobility management protocols for a future flat IP architecture, one should first ask whether the existing mobility management protocols that have already been deployed for the hierarchical mobile networks can be extended to serve the flat IP architecture. MIPv4 has already been deployed in 3GPP2 networks, and PMIPv6 has already been adopted in WiMAX Forum and in 3GPP standards. Using MIP or PMIP for both centralized and distributed architectures would ease the migration of the current mobile networks towards a flat architecture. It has therefore been proposed to adapt MIP or PMIPv6 to achieve distributed mobility management by using a distributed mobility anchor architecture.

In [Paper-Migrating.Home.Agents], the HA functionality is copied to many locations. The HoA of all MNs are anycast addresses, so that a packet destined to the HoA from any corresponding node (CN) from any network can be routed via the nearest copy of the HA. In addition, [Paper-Distributed.Mobility.SAE] proposes to distribute the function of HA into many mobility agents (MAs) each serving a portion of MNs using a distributed hash table structure. A lookup to the hash table will point to the MA serving an MN. In [Paper-Distributed.Mobility.PMIP] and [Paper-Distributed.Mobility.MIP], only the mobility routing (MR) function is duplicated and distributed in many locations. The location information for any MN that has moved to a visited network is still centralized and kept at a location management (LM) function in the home network of the MN. The LM function at different networks constitutes a distributed database system of all the MNs that belong to any of these networks and have moved to a visited network.

4. Requirements

After comparing distributed mobility management against centralized deployment in Section 3, this section states the requirements as follows:

4.1. Distributed deployment

REQ1: Distributed deployment

IP mobility, network access and routing solutions provided by DMM MUST enable a distributed deployment of mobility management of IP sessions so that the traffic can be routed in an optimal manner without traversing centrally deployed mobility anchors.

Motivation: The motivations of this requirement are to match mobility deployment with current trend in network evolution: more cost and resource effective to cache and distribute contents when combining distributed anchors with caching systems (e.g., CDN); improve scalability; avoid single point of failure; mitigate threats being focused on a centrally deployed anchor, e.g., home agent and local mobility anchor.

This requirement addresses the following problems PS1, PS2, PS3, and PS4.

PS1: Non-optimal routes

Routing via a centralized anchor often results in a longer route, and the problem is especially manifested when accessing a local or cache server of a Content Delivery Network (CDN).

PS2: Non-optimality in Evolved Network Architecture

The centralized mobility management can become non-optimal as a network architecture evolves and becomes more flattened.

PS3: Low scalability of centralized route and mobility context maintenance

Setting up such special routes and maintaining the mobility context for each MN is more difficult to scale in a centralized design with a large number of MNs. Distributing the route maintenance function and the mobility context maintenance function among different networks can be more scalable.

PS4: Single point of failure and attack

Centralized anchoring may be more vulnerable to single point of failure and attack than a distributed system.

4.2. Transparency to Upper Layers when needed

REQ2: Transparency to Upper Layers when needed

The DMM solutions MUST provide transparency above the IP layer when needed. Such transparency is needed, when the mobile hosts or entire mobile networks [RFC3963] change their point of attachment to the Internet, for the application flows that cannot cope with a change of IP address. Otherwise the support to maintain a stable home IP address or prefix during handover may be declined.

Motivation: The motivation of this requirement is to enable more efficient use of network resources and more efficient routing by not maintaining a stable home IP address when there is no such need.

This requirement addresses the problems PS5 as well as the other related problem O-PS1.

PS5: Wasting resources to support mobile nodes not needing mobility support

IP mobility support is not always required. For example, some applications do not need a stable IP address during handover, i.e., IP session continuity. Sometimes, the entire application session runs while the terminal does not change the point of attachment. In these situations that do not require IP mobility support, network resources are wasted when mobility context is set up.

O-PS1: Mobility signaling overhead with peer-to-peer communication

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

4.3. IPv6 deployment

REQ3: IPv6 deployment

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

Motivation: The motivation for this requirement is to be inline with the general orientation of IETF. Moreover, DMM deployment is foreseen in mid-term/long-term, hopefully in an IPv6 world. It is also unnecessarily complex to solve this problem for IPv4, as we will not be able to use some of the IPv6-specific features/tools.

4.4. Compatibility

REQ4: Compatibility

The DMM solution SHOULD be able to work between trusted administrative domains when allowed by the security measures deployed between these domains. Furthermore, the DMM solution MUST be able to co-exist with existing network deployment and end hosts so that the existing deployment can continue to be supported. For example, depending on the environment in which DMM is deployed, the DMM solutions may need to be compatible with other existing mobility protocols that are deployed in that environment or may need to be interoperable with the network or the mobile hosts/routers that do not support the DMM enabling protocol.

Motivation: The motivation of this requirement is to allow inter-domain operation if desired and to preserve backwards compatibility so that the existing networks and hosts are not affected and do not break.

This requirement addresses the following other related problem O-PS2.

O-PS2: Complicated deployment with too many variants and extensions of MIP

Deployment is complicated with many variants and extensions of MIP. When introducing new functions which may add to the complexity, existing solutions are more vulnerable to break.

4.5. Existing mobility protocols

REQ5: Existing mobility protocols

A DMM solution SHOULD first consider reusing and extending the existing mobility protocols before specifying new protocols.

Motivation: The purpose is to reuse the existing protocols first before considering new protocols.

4.6. Security considerations

REQ6: Security considerations

The protocol solutions for DMM MUST consider security, for example authentication and authorization mechanisms that allow a legitimate mobile host/router to access to the DMM service, protection of signaling messages of the protocol solutions in terms of authentication, data integrity, and data confidentiality, opt-in or opt-out data confidentiality to signaling messages depending on network environments or user requirements.

Motivation and problem statement: Mutual authentication and authorization between a mobile host/router and an access router providing the DMM service to the mobile host/router are required to prevent potential attacks in the access network of the DMM service. Otherwise, various attacks such as impersonation, denial of service, man-in-the-middle attacks, etc. are present to obtain illegitimate access or to collapse the DMM service.

Signaling messages are subject to various attacks since these messages carry context of a mobile host/router. For instance, a malicious node can forge and send a number of signaling messages to redirect traffic to a specific node. Consequently, the specific node is under a denial of service attack, whereas other nodes are not receiving their traffic. As signaling messages travel over the Internet, the end-to-end security is required.

5. Security Considerations

Distributed mobility management (DMM) requires two kinds of security considerations: 1) access network security that only allows a legitimate mobile host/router to access the DMM service; 2) end-to-end security that protects signaling messages for the DMM service. Access network security is required between the mobile host/router and the access network providing the DMM service. End-to-end security is required between nodes that participate in the DMM protocol.

It is necessary to provide sufficient defense against possible security attacks, or to adopt existing security mechanisms and protocols to provide sufficient security protections. For instance, EAP based authentication can be used for access network security, while IPsec can be used for end-to-end security.

6. IANA Considerations

None

7. Co-authors and Contributors

This problem statement document is a joint effort among the following participants. Each individual has made significant contributions to this work.

Dapeng Liu: liudapeng@chinamobile.com

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

Hidetoshi Yokota: yokota@kddilabs.jp

Charles E. Perkins: charliep@computer.org

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

Elena Demaria: elena.demaria@telecomitalia.it

Peter McCann: Peter.McCann@huawei.com

Tricci So: tso@zteusa.com

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

Jouni Korhonen: jouni.korhonen@nsn.com

Sri Gundavelli: sgundave@cisco.com

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

Marco Liebsch: Marco.Liebsch@neclab.eu

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

Georgios Karagiannis: g.karagiannis@utwente.nl

Julien Laganier: jlaganier@juniper.net

Wassim Michel Haddad: Wassam.Haddad@ericsson.com

Seok Joo Koh: sjkoh@knu.ac.kr

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

Ahmad Muhanna: amuhanna@awardsolutions.com

8. References

8.1. Normative References

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

8.2. Informative References

[I-D.ietf-netext-pd-pmip]
Zhou, X., Korhonen, J., Williams, C., Gundavelli, S., and C. Bernardos, "Prefix Delegation for Proxy Mobile IPv6", draft-ietf-netext-pd-pmip-02 (work in progress), March 2012.

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

[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, Feb 2011.", Proceedings of GlobeCom Workshop on Seamless Wireless Mobility, 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.

[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.

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

Author’s Address

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
France Telecom - Orange
4, rue du Clos Courtel, BP 91226, Cesson-Sevigne 35512, France
Email: pierrick.seite@orange-ftgroup.com
-
Hidetoshi Yokota
KDDI Lab
2-1-15 Ohara, Fujimino, Saitama, 356-8502 Japan
Email: yokota@kddilabs.jp
-
Charles E. Perkins
Huawei Technologies
Email: charliep@computer.org
-
Jouni Korhonen
Nokia Siemens Networks
Email: jouni.korhonen@nsn.com
-
Melia Telemaco
Alcatel-Lucent Bell Labs
Email: telemaco.melia@alcatel-lucent.com
-
Elena Demaria
Telecom Italia
via G. Reiss Romoli, 274, TORINO, 10148, Italy
Email: elena.demaria@telecomitalia.it
-
Jong-Hyouk Lee
RSM Department, Telecom Bretagne
Cesson-Sevigne, 35512, France
Email: jh.lee@telecom-bretagne.eu
-

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: PeterMcCann@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
-
Marco Liebsch
NEC Laboratories Europe
Email: liebsch@neclab.eu
-
Carl Williams
MCSR Labs
Email: carlw@mcsr-labs.org
-