Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 11, 2014

H. Chan (Ed.)
Huawei Technologies (more co-authors on P. 17)
D. Liu
China Mobile
P. Seite
Orange
H. Yokota
KDDI Lab
J. Korhonen
Renesas Mobile

November 7, 2013

Requirements for Distributed Mobility Management
draft-ietf-dmm-requirements-10

Abstract

This document defines the requirements for Distributed Mobility Management (DMM). The hierarchical structure in traditional wireless networks has led primarily to centralized deployment models. As some wireless networks are evolving away from the hierarchical structure, such as in moving the content delivery servers closer to the users, a distributed model for mobility management can be useful to them.

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 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 May 11, 2014.

Table of Contents

1. Introduction 4
2. Conventions used in this document 6
2.1. Terminology 6
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
5.1. Distributed processing 11
5.2. Transparency to Upper Layers when needed 11
5.3. IPv6 deployment 12
5.4. Existing mobility protocols 12
5.5. Co-existence 13
5.6. Security considerations 13
5.7. Multicast 14
6. Security Considerations 14
7. IANA Considerations 14
8. Co-authors and Contributors 14
9. References 15
9.1. Normative References 15
9.2. Informative References 15
Authors' Addresses 17

1. Introduction

In the past decade a fair number of mobility protocols have been standardized [RFC6275] [RFC5944] [RFC5380] [RFC6301] [RFC5213]. Although the 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.

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; such traffic imposes new requirements on mobile core networks for data traffic delivery. The presence of content providers closer to Internet Service Providers (ISP) network requires taking into account local Content Delivery Networks (CDNs) while providing mobility services. Moreover, when the traffic demand exceeds available capacity, service providers need to implement new strategies such as selective IPv4 traffic offload (e.g. [RFC6909], 3GPP work items LIPA/SIPTO [TS.23.401]) through alternative access networks (e.g. WLAN) [Paper-Mobile.Data.Offloading]. A gateway selection mechanism also takes the user proximity into account within EPC [TS.29303]. These mechanisms were not pursued in the past owing to charging and billing reasons. Assigning a gateway anchor node from a visited network in roaming scenario has until recently been done and are limited to voice services only. Charging and billing require solutions beyond the mobility protocol.

Both traffic offloading and CDN mechanisms 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 towards so-called "flat networks" works best for 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.

(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.

In addition, considerations in the study of DMM are in the following.

(1) 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 have stringent requirements in terms of delay. Notions of localization and distribution of local agents have been introduced to reduce signaling overhead at the centralized routing anchor point [Paper-Distributed.Centralized.Mobility]. Unfortunately, such protocols have not been deployed today.

(2) Most existing mobility protocols have not been designed for multiple-interface hosts which are capable to use multiple interfaces simultaneously. Retrofitting the required functionality can result in an unnecessary increase in the protocol complexity.

(3) IP multicast support, including optimizations, have been introduced as an effective transport method for multimedia data delivery, but by "patching-up" procedure after completing the design of reference mobility protocol, leading to network inefficiency and non-optimal routing.

The distributed mobility management (DMM) charter addresses two complementary aspects of mobility management procedures: the distribution of mobility anchors in the data-plane towards a more flat network and the selective activation/deactivation of mobility protocol support as an enabler to distributed mobility management. The former aims at positioning mobility anchors (e.g., HA, LMA) closer to the user; ideally, mobility agents could be collocated with

the first-hop router. The latter, facilitated by the distribution of mobility anchors, identifies when mobility support must be activated and when sessions do not require mobility management support -- thus reducing 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 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.

Flat mobile network

has few levels of routing hierarchy introduced into the data path by the mobility management system.

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 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 session identifier and routing address and maintaining a mapping between the two. In Mobile IP, the home address serves as the session identifier whereas the care-of-address (CoA) takes the role of the routing address. The binding between these two is maintained at the home agent (mobility anchor). If packets addressed to the home address of a mobile node can be continuously delivered to the node, then all sessions using that home address are unaffected even though the routing address (CoA) changes.

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

3.1. Centralized mobility management

In centralized mobility management, the mapping information between the session identifier and the locator IP address of a mobile node (MN) is kept at a single mobility anchor. At the same time, packets destined to the MN are routed 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 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 cellular networks such as the Third Generation Partnership Project (3GPP) GPRS networks, CDMA networks, and 3GPP Evolved Packet System (EPS) networks employ centralized mobility management too. In particular, the Gateway GPRS Support Node (GGSN), Serving GPRS

Support Node (SGSN) and Radio Network Controller (RNC) in the 3GPP GPRS hierarchical network, and the Packet Data Network Gateway (P-GW) and Serving Gateway (S-GW) in the 3GPP EPS network all act as anchors in a hierarchy.

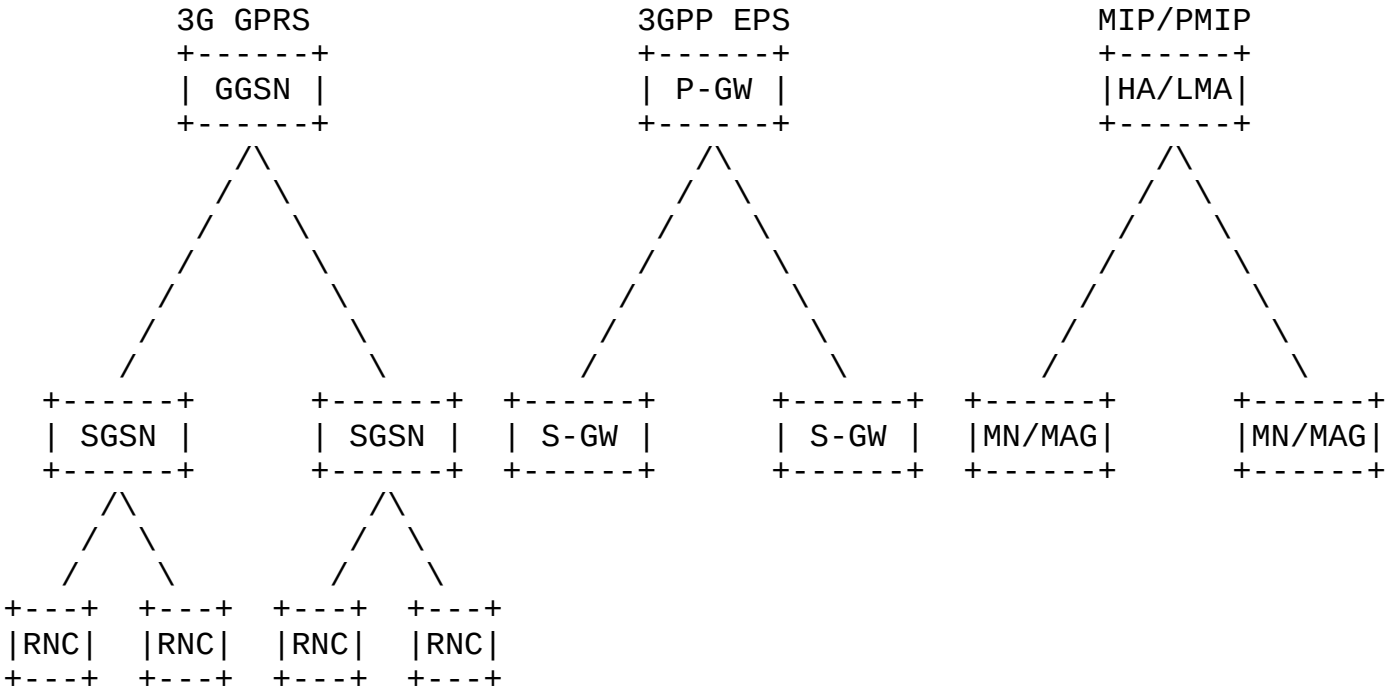

Figure 1. Centralized mobility management.

3.2. Distributed mobility management

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

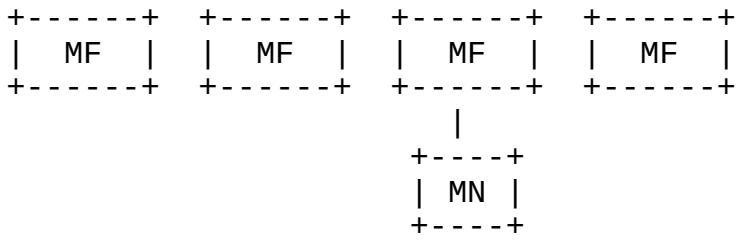

Figure 2. Distributed mobility management.

Mobility management may be partially or fully distributed [I-D.yokota-dmm-scenario]. In the former case only the data plane is

distributed, implicitly assuming separation of data and control planes as described in [I-D.wakikawa-netext-pmip-cp-up-separtion]. Fully distributed mobility management implies that both the data plane and the control plane are distributed. 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 flat mobile network of access nodes is proposed in [Paper-Distributed.Dynamic.Mobility]. Its benefits over centralized mobility management are shown through simulations in [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

Routing 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 CN are located in the PMIP domain and attached to a MAG, and is not applicable when the CN is outside the PMIP domain or does not behave like an MN.)

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

Centralized mobility management can become non-optimal with a flat network architecture.

PS3: Low 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 increase scalability.

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 nodes that do not need it

IP mobility support is not always required, and not every parameter of mobility context is always used. For example, some applications do not need a stable IP address during a handover to maintain session continuity. Sometimes, the entire application session runs while the terminal 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 more efficient to deactivate IP mobility support for such sessions.

PS6: (Related problem) 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. Peer-to-peer communications have particular traffic patterns that often do not benefit from mobility support from the network. Thus, the associated mobility support signaling (e.g., maintenance of the tunnel, keep alive signaling, etc.) wastes network resources for no application gain.

PS7: (Related problem) Deployment with multiple mobility solutions

There are already many variants and extensions of MIP. Deployment of new mobility management solutions can be challenging, and debugging difficult, when they must co-exist with solutions already 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, this section identifies the following requirements:

5.1. Distributed processing

REQ1: Distributed processing

IP mobility, network access and routing solutions provided by DMM MUST enable distributed processing for mobility management so that traffic can avoid traversing single mobility anchor far from the optimal route.

Motivation: This requirement is motivated by current trends in network evolution: (a) it is cost- and resource-effective to cache and distribute content by combining distributed mobility anchors with caching systems (e.g., CDN); (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.

5.2. Transparency to Upper Layers when needed

REQ2: Transparency to Upper Layers when needed

DMM solutions MUST provide transparent mobility support above the IP layer when needed. Such transparency is needed, for example, when, upon change of point of attachment to the

network, an application flow cannot cope with a change in the IP address. However, it is not always necessary to maintain a stable home IP address or prefix for every application or at all times for a mobile node.

Motivation: The motivation of this requirement is to enable more efficient routing 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 problem PS5 as well as the related problem PS6 stated in Section 4.

5.3. IPv6 deployment

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.

5.4. Existing mobility protocols

REQ4: Existing mobility protocols

A DMM solution SHOULD 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.

5.5. Co-existence

REQ5: Co-existence with deployed networks and hosts

The DMM solution MUST be able to co-exist with existing network deployments and end hosts. For example, depending on the environment in which DMM is deployed, DMM solutions may need to be compatible with other deployed mobility protocols or may need to co-exist with a network or mobile hosts/routers that do not support DMM protocols. The mobile node may also move between different access networks, where some of them may support neither DMM nor another mobility protocol. Furthermore, a DMM solution SHOULD work across different networks, possibly operated as separate administrative domains, when 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 related problem PS7 described in Section 4.

5.6. Security considerations

REQ6: Security considerations

A DMM solution MUST not introduce new security risks or amplify existing security risks against which the existing security mechanisms/protocols cannot offer sufficient protection.

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 is 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. can be used to protect the DMM entities as they are already used to protect against existing networks and existing mobility protocols defined in IETF.

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.

5.7. Multicast

REQ7: Multicast considerations

DMM SHOULD consider multicast early so that solutions can be developed not only to provide IP mobility support when it is needed, but also to avoid network inefficiency issues in multicast traffic delivery (such as duplicate multicast subscriptions towards the downstream tunnel entities). The multicast solutions should therefore avoid restricting the management of all IP multicast traffic to a single host through a dedicated (tunnel) interface on multicast-capable access routers.

Motivation: Existing multicast deployment have been introduced after completing the design of the reference mobility protocol, then optimization and extensions have been followed by "patching-up" procedure, thus leading to network inefficiency and non-optimal routing. The multicast solutions should therefore be required to consider efficiency nature in multicast traffic delivery.

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 5.6.

7. IANA Considerations

None

8. Co-authors and Contributors

This problem statement document is a joint effort among the numerous participants. Each individual has made significant contributions to this work and have been listed as co-authors.

9. References

9.1. Normative References

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

9.2. Informative References

[I-D.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., and S. Gundavelli, "Separation of Control and User Plane for Proxy Mobile IPv6", draft-wakikawa-netext-pmip-cp-up-separation-00 (work in progress), July 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-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.

[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.

[RFC3753] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[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.

[RFC5944] Perkins, C., "IP Mobility Support for IPv4, Revised", RFC 5944, November 2010.

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

[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.

[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 (more co-authors on P. 17)
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
Renesas Mobile
Porkkalankatu 24, FIN-00180 Helsinki, Finland
Email: jouni.korhonen@nsn.com
-
Charles E. Perkins
Huawei Technologies
Email: charliep@computer.org
-
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
Sangmyung University
Email: hurryon@gmail.com
-
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: 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
-
Sri Gundavelli
Cisco
sgundave@cisco.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
jlaganier@juniper.net
-
Wassim Michel Haddad
Ericsson
Wassam.Haddad@ericsson.com
-
Dirk von Hugo
Deutsche Telekom Laboratories
Dirk.von-Hugo@telekom.de
-
Ahmad Muhanna
Award Solutions
amuhanna@awardsolutions.com
-
Byoung-Jo Kim
ATT Labs
macsbug@research.att.com
-
Hassan Ali-Ahmad
Orange
hassan.aliahmad@orange.com
-
Alper Yegin
Samsung
alper.yegin@partner.samsung.com
-