

Internet Engineering Task Force (IETF)
Request for Comments: 7333
Category: Informational
ISSN: 2070-1721

H. Chan, Ed.
Huawei Technologies
D. Liu
China Mobile
P. Seite
Orange
H. Yokota
Landis+Gyr
J. Korhonen
Broadcom Communications
August 2014

Requirements for Distributed Mobility Management

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.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <http://www.rfc-editor.org/info/rfc7333>.

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. Introduction2
- 2. Conventions Used in This Document4
 - 2.1. Requirements Language4
 - 2.2. Terminology4
- 3. Centralized versus Distributed Mobility Management5
 - 3.1. Centralized Mobility Management6
 - 3.2. Distributed Mobility Management7
- 4. Problem Statement8
- 5. Requirements10
- 6. Security Considerations16
- 7. Contributors17
- 8. References20
 - 8.1. Normative References20
 - 8.2. Informative References21

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. Among other tasks that the anchor point performs, the anchor point 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 is 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-mentioned centralized deployment. The background behind the interest in studying DMM is primarily as follows.

- (1) More than ever, mobile users are 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 Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO) work items [TS.23.401]) through alternative access networks such as Wireless Local Area Networks (WLANs) [MOB-DATA-OFFLOAD]. In addition, a gateway selection mechanism takes user proximity into account within the Evolved Packet Core (EPC) [TS.29.303]. However, these mechanisms were not pursued in the past, owing to charging and billing considerations that 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 [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, IP mobility support is currently 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, e.g., as described in [DHCPv6-CLASS-BASED-PREFIX] and [IPv6-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. DMM can thus reduce the amount of state information that must be maintained in various mobility agents of the mobile network and can then avoid the unnecessary establishment of mechanisms to forward traffic from an old mobility anchor 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. Security considerations are mentioned in Section 6.

The problem statement and use cases [DMM-SCENARIO] can be found in [DIST-MOB-REVIEW].

2. Conventions Used in This Document

2.1. 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].

2.2. Terminology

All of the general mobility-related terms, and their acronyms as used in this document, are to be interpreted as defined in the Mobile IPv6 base specification [RFC6275], the Proxy Mobile IPv6 (PMIPv6) specification [RFC5213], and "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 document introduces the following terms:

Centrally deployed mobility anchors

refers 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 is 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 that are introduced into the data path by the mobility management system.

Flattening mobile network

refers to the hierarchical mobile network that 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 redirects them using the forwarding address to deliver to the session. Redirecting packets this way can result in long routes. An existing optimization routes directly, using the forwarding address of the host, and as 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 3GPP General Packet Radio System (GPRS) networks and 3GPP Evolved Packet System (EPS) networks, also employ centralized mobility management. 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.

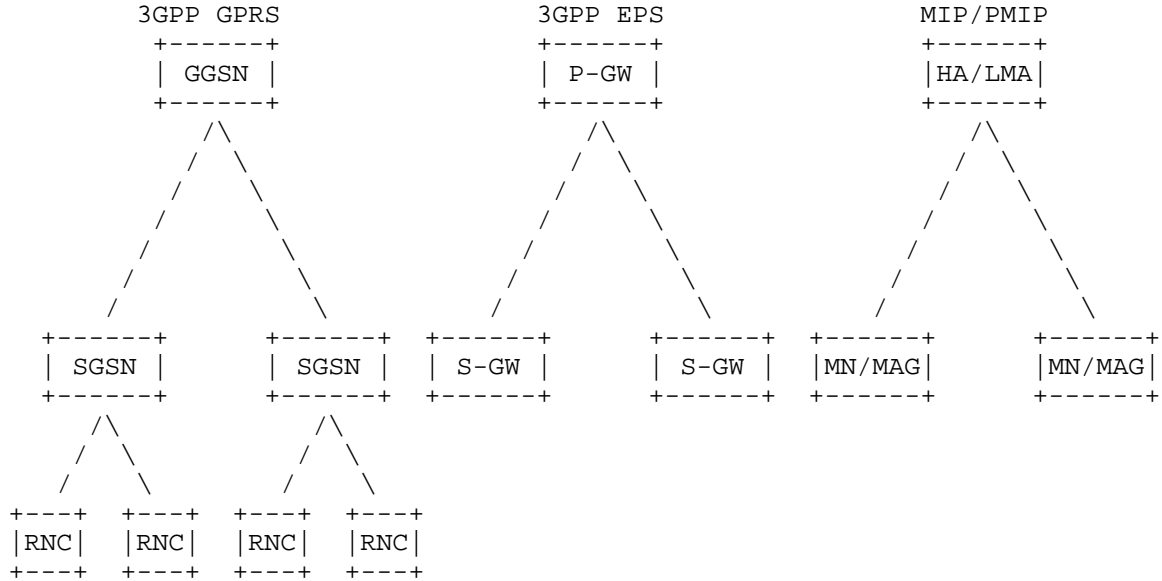


Figure 1: Centralized Mobility Management

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.

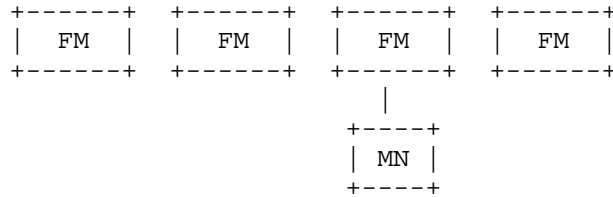


Figure 2: Distributed Mobility Management

DMM is distributed in the data plane, whereas the control plane may be either centralized or distributed [DMM-SCENARIO]. The former case implicitly assumes separation of data and control planes as described in [PMIP-CP-UP-SPLIT]. While mobility management can be distributed, it is not necessary for other functions such as subscription management, subscription databases, 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 [DIST-DYNAMIC-MOB]. Its benefits over centralized mobility management have been shown through simulations [DIST-CENTRAL-MOB]. Moreover, the (re)use and extension of existing protocols in the design of both fully distributed mobility management [MIGRATING-HAs] [DIST-MOB-SAE] and partially distributed mobility management [DIST-MOB-PMIP] [DIST-MOB-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 as follows:

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 packets 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 a single point of failure 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. However, 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

Resources may be wasted 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 as mobility solutions at other layers. Deployment of new mobility management solutions can be challenging, and debugging difficult, when they coexist 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., a 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

Now that distributed mobility management has been compared with centralized deployment (Section 3) and the problems have been described (Section 4), this section identifies the following requirements:

REQ1: Distributed mobility management

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

This requirement on distribution applies to 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 implied 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; and (d) threats against centrally deployed anchors, e.g., a home agent and a 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 solutions, and forwarding solutions provided by DMM MUST then provide 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, particularly 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 as "on the mid- to long-term horizon", when IPv6 is expected to be far more common than today.

This requirement avoids the unnecessarily complex solution of trying to provide the same level of functionality to both IPv4 and IPv6. Some of the IPv6-specific features are not available for IPv4.

REQ4: Existing mobility protocols

A DMM solution MUST first consider reusing and extending IETF standard 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 for development of new protocols and therefore their potential for 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 stacks. 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: to (a) 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, and 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) the Simple Network Management Protocol (SNMP) [RFC1157], with definitions of standardized management information base (MIB) objects for DMM that allow the monitoring of traffic steering in a consistent manner across different devices
- (b) the Network Configuration Protocol (NETCONF) [RFC6241], with definitions of standardized YANG [RFC6020] modules for DMM to achieve a standardized configuration
- (c) syslog [RFC5424], which is a one-way protocol allowing a device to report significant events to a log analyzer in a network management system
- (d) the 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 this requirements document to impose which management protocol(s) should be used. An inventory of the management protocols and data models is covered in [RFC6632].

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

A DMM solution MUST describe how, and in what types of environments, it can be scalably deployed and managed.

A DMM solution MUST support mechanisms to test whether 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 a 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 a 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 [RFC5424].

A DMM solution MUST provide fault management and monitoring mechanisms to manage situations where an 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 the 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 an indication of DMM performance, such as
 - (1) handover delay, which includes the time necessary to reestablish the forwarding path when the point of attachment changes

- (2) 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 encapsulation method used, and its overhead
 - (4) the security used at the 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 definitions of management information base (MIB) objects to the MIPv6 MIB [RFC4295] or the PMIPv6 MIB [RFC6475] that are 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 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 and 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 existing networks and existing mobility protocols defined in the IETF. However, if a candidate DMM solution is such that these existing security mechanisms/protocols are unable to provide sufficient security protection even when properly used, then 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 that make deployment infeasible, because platforms conforming to such 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 deployments 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. DMM should instead consider multicast early in the process, so that the multicast solutions can better consider the efficient nature of 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 REQ7 in Section 5.

7. Contributors

This requirements document is a joint effort among numerous participants working as a team. Valuable comments and suggestions in various reviews from the following area directors and IESG members have also contributed to many 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 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

8. References

8.1. 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.
- [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.
- [RFC5424] Gerhards, R., "The Syslog Protocol", RFC 5424, March 2009.
- [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.

8.2. Informative References

[DHCPv6-CLASS-BASED-PREFIX]

Bhandari, S., Halwasia, G., Gundavelli, S., Deng, H., Thiebaut, L., Korhonen, J., and I. Farrer, "DHCPv6 class based prefix", Work in Progress, July 2013.

[DIST-CENTRAL-MOB]

Bertin, P., Bonjour, S., and J-M. Bonnin, "Distributed or Centralized Mobility?", Proceedings of the 28th IEEE Conference on Global Telecommunications (GlobeCom), December 2009.

[DIST-DYNAMIC-MOB]

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.

[DIST-MOB-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.

[DIST-MOB-PMIP]

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

[DIST-MOB-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.

[DIST-MOB-SAE]

Fischer, M., Andersen, 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.

[DMM-SCENARIO]

Yokota, H., Seite, P., Demaria, E., and Z. Cao, "Use case scenarios for Distributed Mobility Management", Work in Progress, October 2010.

- [IPv6-PREFIX-PROPERTIES]
Korhonen, J., Patil, B., Gundavelli, S., Seite, P., and D. Liu, "IPv6 Prefix Properties", Work in Progress, July 2013.
- [LOCATING-USER]
Kirby, G., "Locating the User", Communications International, 1995.
- [MIGRATING-HAs]
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.
- [MOB-DATA-OFFLOAD]
Lee, K., Lee, J., Yi, Y., Rhee, I., and S. Chong, "Mobile Data Offloading: How Much Can WiFi Deliver?", Proceedings of the ACM SIGCOMM 2010 Conference, 2010.
- [PMIP-CP-UP-SPLIT]
Wakikawa, R., Pazhyannur, R., and S. Gundavelli, "Separation of Control and User Plane for Proxy Mobile IPv6", Work in Progress, July 2013.
- [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 TS 23.401 12.5.0, June 2014, <<http://www.3gpp.org/ftp/Specs/html-info/23401.htm>>.

[TS.29.303]

3GPP, "Domain Name System Procedures; Stage 3", 3GPP TS 29.303 12.3.0, June 2014, <<http://www.3gpp.org/ftp/Specs/html-info/29303.htm>>.

Authors' Addresses

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

EEmail: h.a.chan@ieee.org

Dapeng Liu
China Mobile
Unit 2, 28 Xuanwumenxi Ave, Xuanwu District
Beijing 100053
China

EEmail: liudapeng@chinamobile.com

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

EEmail: pierrick.seite@orange.com

Hidetoshi Yokota
Landis+Gyr

EEmail: hidetoshi.yokota@landisgyr.com

Jouni Korhonen
Broadcom Communications
Porkkalankatu 24
Helsinki FIN-00180
Finland

EEmail: jouni.nospam@gmail.com