

MULTIMOB Group
Internet-Draft
Expires: August 22, 2013

H. Asaeda
NICT
P. Seite
France Telecom
February 18, 2013

PMIPv6 Multicast Routing Optimization with PIM-SM
draft-asaeda-multimob-pmip6-ropt-with-pim-00

Abstract

This document describes IP multicast routing optimization with PIM-SM in Proxy Mobile IPv6 (PMIPv6) environment. The Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA) are the mobility entities defined in the PMIPv6 protocol and act as PIM-SM routers. The proposed protocol optimization addresses the tunnel convergence problem and cooperates with seamless handover mechanisms.

Status of this Memo

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

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

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

This Internet-Draft will expire on August 22, 2013.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	3
2. Conventions and Terminology	4
3. Overview	4
3.1. Multicast Communication in PMIPv6	4
3.2. Protocol Sequence for Multicast Channel Subscription	6
4. Multicast Tunnel (M-Tunnel)	7
4.1. Packet Encapsulation	7
4.2. M-Tunnels Connecting to Multiple PIM-SM Routers and ECMP Routing	8
5. Local Mobility Anchor Operation	9
6. Mobile Access Gateway Operation	10
7. Mobile Node Operation	10
8. Localized Multicast Routing	10
9. Smooth Handover	11
10. IANA Considerations	14
11. Security Considerations	14
12. Acknowledgements	14
13. References	14
13.1. Normative References	14
13.2. Informative References	15
Authors' Addresses	15

1. Introduction

Proxy Mobile IPv6 (PMIPv6) [1] enables network-based mobility for IPv6 mobile nodes (MNs) that do not implement any mobility protocols. The Local Mobility Anchor (LMA) is the topological anchor point to manages the mobile node's binding state. The Mobile Access Gateway (MAG) is an access router or gateway that manages the mobility-related signaling for an MN. An MN is attached to the Proxy Mobile IPv6 Domain (PMIPv6-Domain) that includes LMA and MAG(s), and is able to receive data coming from outside of the PMIPv6-Domain through LMA and MAG.

Network-based mobility support for unicast is addressed in [1], while multicast support in PMIPv6 is not discussed in it. Since LMA and MAG set up a bi-directional IPv6-in-IPv6 tunnel for each mobile node and forwards all mobile node's traffic according to [1], it highly wastes network resources when a large number of mobile nodes join/subscribe the same multicast sessions/channels, because independent data copies of the same multicast packet are delivered to the subscriber nodes in a unicast manner through MAG.

The base solution described in [12] provides options for deploying multicast listener functions in PMIPv6-Domains without modifying mobility and multicast protocol standards. However, in this specification, MAG MUST act as an MLD proxy [2] and hence MUST dedicate a tunnel link between LMA and MAG to an upstream interface for all multicast traffic. This limitation does not allow to use Protocol-Independent Multicast - Sparse Mode (PIM-SM) [3] native routing on MAG, and hence does not solve the tunnel convergence problem; MAG receives the same data from multiple LMAs when MAG attaches to them for mobile nodes and has subscribed the same multicast channel to them. It does not enable direct routing and does not optimize source mobility.

This document describes IP multicast routing optimization using PIM-SM in Proxy Mobile IPv6 (PMIPv6) environment. The Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA) are the mobility entities defined in the PMIPv6 protocol and act as PIM-SM routers. The proposed protocol optimization assumes that both LMA and MAG enable the Protocol-Independent Multicast - Sparse Mode (PIM-SM) multicast routing protocol [3]. The proposed optimization uses a dedicated GRE [4] tunnel for multicast, called M-Tunnel between MAG and PIM-SM router such as LMA. The proposed protocol optimization addresses the tunnel convergence problem and provides seamless handover. It can cooperate with localized routing and direct routing to deliver IP multicast packets for mobile nodes and source mobility. In this document, because multicast listener mobility is mainly focused on, the detail specification of source mobility is not

described.

This document does not require to change unicast communication methods or protocols defined in [1], and therefore both unicast and multicast communications for mobile nodes in PMIPv6-Domain are enabled if this extension is implemented.

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [5].

The following terms used in this document are to be interpreted as defined in the Proxy Mobile IPv6 specification [1]; Mobile Access Gateway (MAG), Local Mobility Anchor (LMA), Mobile Node (MN), Proxy Mobile IPv6 Domain (PMIPv6-Domain), LMA Address (LMAA), Proxy Care-of Address (Proxy-CoA), Mobile Node's Home Network Prefix (MN-HNP), Mobile Node Identifier (MN-Identifier), Proxy Binding Update (PBU), and Proxy Binding Acknowledgement (PBA).

3. Overview

3.1. Multicast Communication in PMIPv6

Required components to enable IP multicast are multicast routing protocols and host-and-router communication protocols. This document assumes PIM-SM [3] as the multicast routing protocol and Multicast Listener Discovery (MLD) as the host-and-router communication protocol. This document allows mobile nodes to participate in Any-Source Multicast (ASM) and Source-Specific Multicast (SSM) [6]. However, in order to explicitly participate in SSM, mobile nodes MUST support either MLDv2 [7] or Lightweight-MLDv2 (LW-MLDv2) [8].

The architecture of a Proxy Mobile IPv6 domain is shown in Figure 1. LMA and MAG are the core functional entities in PMIPv6-Domain. The entire PMIPv6-Domain appears as a single link from the perspective of each mobile node.

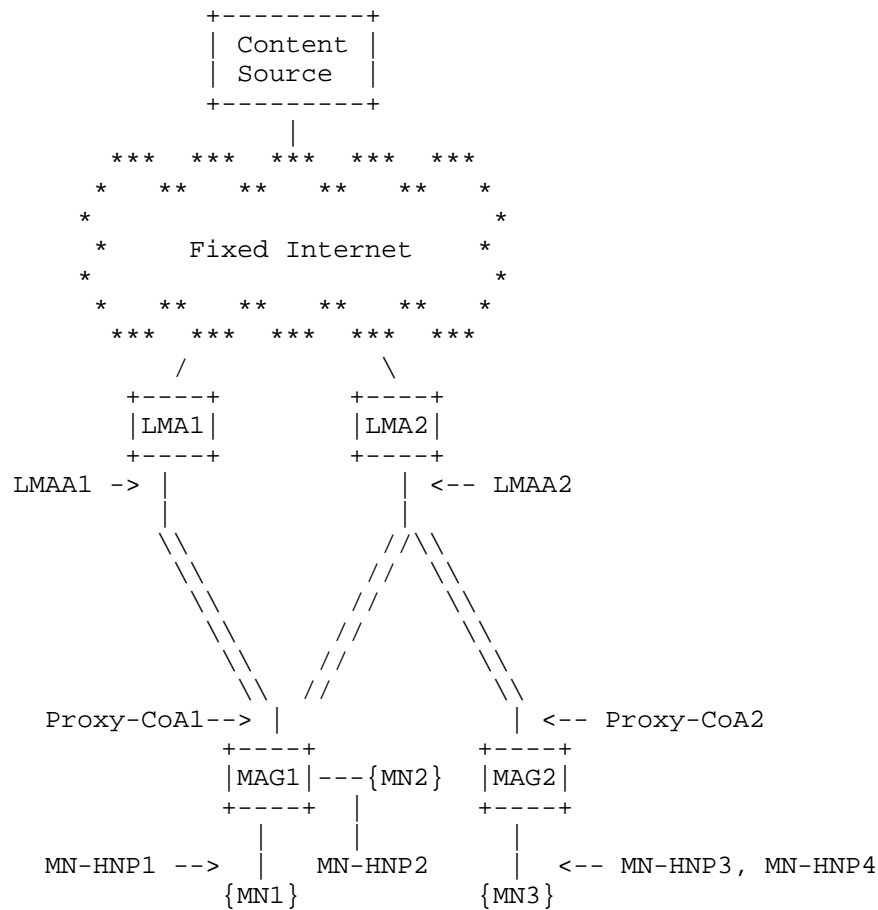


Figure 1: Proxy Mobile IPv6 Domain

When a mobile node wants to subscribe/unsubscribe a multicast channel, it sends MLD Report messages specifying sender and multicast addresses to the access link. The attached MAG detects this membership information and sends the PIM Join/Prune message to the corresponding LMA over a bi-directional GRE tunnel called M-Tunnel (described in Section 4) when the LMA is selected as the previous-hop router for the multicast channel, or sends the PIM Join/Prune message to the adjacent upstream multicast router for the multicast channel. When the LMA or the adjacent router receives the PIM Join/Prune message, it coordinates the corresponding multicast routing tree if necessary and starts forwarding the data.

When the MAG detects mobile node's handover, it can proceed the seamless handover procedures. Since both PMIPv6 and multicast

protocols (i.e., MLD and PIM-SM) do not have functions for multicast context transfer in their original protocol specifications, the external functions or protocols should be used for handover. One of the possible ways is the use of "mobile node's Policy Profile", as it could include "multicast channel information", which expresses mobile node's subscribing multicast channel list, as well as the mandatory fields of the Policy Profile specified in [1]. Mobile node's Policy Profile is provided by "policy store" whose definition is the same as of [1].

3.2. Protocol Sequence for Multicast Channel Subscription

A mobile node sends unsolicited MLD Report messages including source and multicast addresses when it subscribes a multicast channel. When the MAG operating as a PIM-SM router receives MLD Report messages from attached mobile nodes, it sends PIM Join messages to its neighboring routers (Figure 2) to join the multicast delivery tree (if not joined). When the upstream router for the requested channel is LMA (or a non-adjacent PIM router), the MAG sends the corresponding PIM Join messages to the LMA (or the non-adjacent PIM router) using M-Tunnel (see Section 4). When the upstream router for the requested channel is a directly attached adjacent router, the MAG sends the corresponding PIM Join messages to the adjacent upstream router natively. The LMA or such routers then join the multicast delivery tree and forward the packets to the downstream MAG.

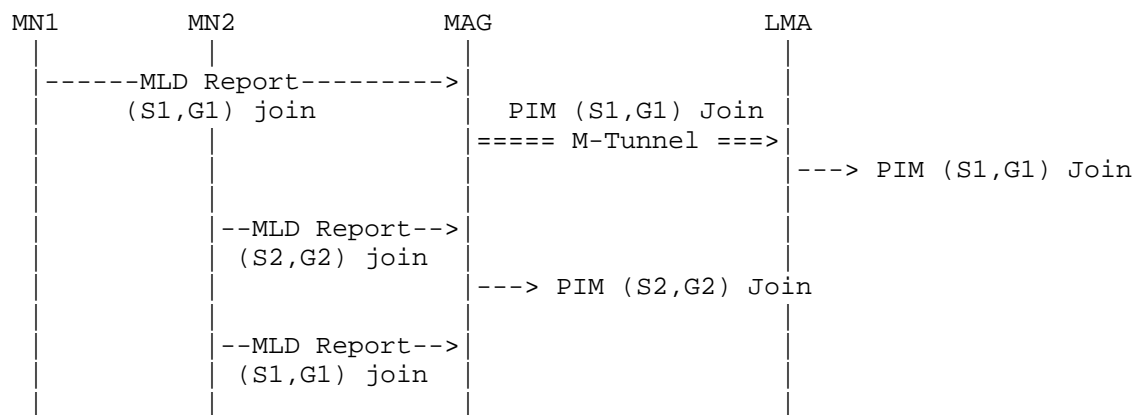


Figure 2: MLD Report and PIM Messages Transmission

PIM-SM relies on Multicast Routing Information Base (MRIB) to select a single upstream interface for each multicast channel by the Reverse Path Forwarding (RPF) algorithm. After all potential upstream interfaces including M-Tunnel are recognized in MRIB (as described in Section 4), the MAG enabling PIM-SM can select either M-Tunnel

interface or physical interface for a multicast channel by the Reverse Path Forwarding (RPF) algorithm. The proposed architecture for PMIPv6 with PIM-SM therefore does not cause the tunnel convergence problem, and hence duplicate packets are not forwarded to the MAG.

4. Multicast Tunnel (M-Tunnel)

4.1. Packet Encapsulation

M-Tunnel is a bi-directional GRE tunnel [4] dedicated for PIM messages and IP multicast data transmissions. The tunnel end-point of M-Tunnel is a MAG that is a PIM-SM capable router. Another tunnel end-point is also a PIM-SM capable router. The typical use case of M-Tunnel is to establish a bi-directional tunnel link between LMA and MAG; therefore LMA shall be another tunnel end-point. M-Tunnel can be established in a bootstrap phase of MAG (without detecting a multicast channel subscription request from a mobile node) and kept while the MAG enables PIM routing functions to forward multicast packets. An M-Tunnel is not set up per mobile node basis, but per MAG basis; it can be shared with mobile nodes attached to the MAG as seen in Figure 3.

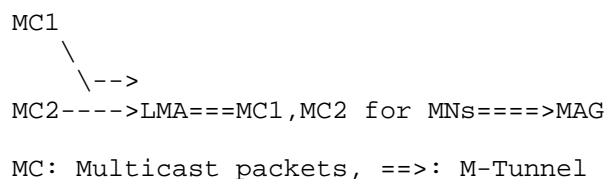


Figure 3: Multicast packet forwarding through M-Tunnel

In order for the PIM routing protocol to use an M-Tunnel for multicast forwarding, an M-Tunnel interface must be recognized by the PIM routing protocol as the upstream multicast interface for MAG. It is done by the configuration of static multicast routes, such as "ip mroute 0.0.0.0 0.0.0.0 gre0" or "ip mroute 1.1.1.0 255.255.255.0 gre0". By such configuration, MAG inserts the multicast forwarding paths using the M-Tunnel into its MRIB. MAG then selects the M-Tunnel interface as the corresponding RPF interface, and forwards the PIM Join/Prune messages over the M-Tunnel. If operators want to select other interface, e.g. a physical interface, as the upstream multicast interface for some specific source prefixes, e.g. sources inside the PMIPv6-Domain, they can *additionally* configure the specific multicast routes with longer prefixes. This configuration will be used for direct routing. Then the MAG selects as the appropriate upstream router according to the MRIB entry. Note that

the case having multiple M-Tunnels configured on MAG is described in Section 4.2.

The format of the tunneled multicast packet forwarded from LMA to MAG is shown below. "S" and "G" are the same notation used for (S,G) multicast channel.

```

IPv6 header (src= LMAA, dst= Proxy-CoA) /* Outer Header */
GRE header                               /* Encapsulation Header */
  IPv6 header (src= S, dst= G)           /* Inner Header */
  Upper layer protocols                 /* Packet Content */

```

Figure 4: Multicast packet format tunneled from LMA to MAG

When a PIM message is sent from MAG to LMA, the src and dst addresses of the outer tunnel header will be replaced to Proxy-CoA and LMAA, respectively. To convey a PIM message, the src address of the inner packet header is changed to either LMA's or MAG's link-local address. The dst address of the packet header is assigned based on the PIM's condition (see [3]).

In order to establish M-Tunnel, LMA and MAG need to negotiate GRE encapsulation and GRE keys for M-Tunnel. The GRE Key option to be used for the negotiation of GRE tunnel encapsulation mode and exchange of the uplink and downlink GRE keys is defined in [9]. It is also possible to use the static fixed GRE keys for M-Tunnel.

4.2. M-Tunnels Connecting to Multiple PIM-SM Routers and ECMP Routing

There can be multiple LMAs in a PMIPv6-Domain each serving a different group of mobile nodes. In that case, a MAG will connect to multiple LMAs with different M-Tunnels having different GRE keys. For example, in Figure 5, MAG1 establishes two M-Tunnels with LMA1 and LMA2, and MAG2 establishes one M-Tunnel with LMA2.

A MAG that has multiple M-Tunnels, such as MAG1 in Figure 5, must decide a single upstream M-Tunnel interface for an RP or a source address or prefix. There are two ways to decide a single upstream M-Tunnel for a MAG. One is only with static MRIB configuration by operation. For example, operators can configure each M-Tunnel interface as the RPF interface for specific source address(es) or prefix(es) one by one. Each M-Tunnel interface is then inserted into the MAG's MRIB and used for different source address(es) or prefix(es).

The other way to select a single upstream M-Tunnel interface is with PIM ECMP [13]. A MAG enabling PIM routing functions selects a path by the ECMP algorithm as described in [13]. The PIM ECMP function

chooses the PIM neighbor with the highest IP address or the best hash value over the destination and source addresses. The algorithm choosing a single interface is based on an operator's decision. When operators decide to use PIM ECMP to select a single upstream M-Tunnel from multiple M-Tunnels, both the MAG and the tunnel end-point PIM-SM routers (e.g., LMAs) MUST enable PIM ECMP.

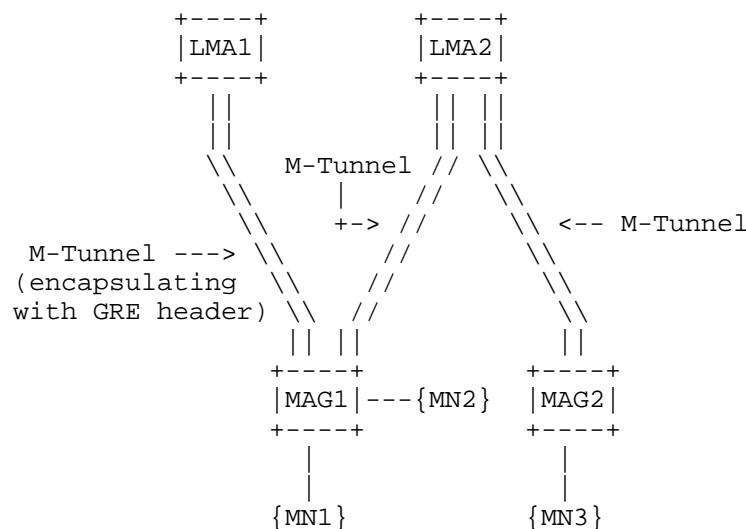


Figure 5: M-Tunnels established between LMA and MAG

5. Local Mobility Anchor Operation

The LMA is responsible for maintaining the mobile node's reachability state and is the topological anchor point for the mobile node's home network prefix(es). This document assumes that the LMA is capable of forwarding multicast packets to the MAG by enabling the PIM-SM multicast routing protocol [3]. The LMA acting as a PIM-SM multicast router may serve MAGs as downstream routers for some multicast channels when a mobile node is a multicast data receiver (or as upstream routers when a mobile node is a multicast data sender). The downstream (or upstream) MAG is connected to the LMA through the M-Tunnel for multicast communication.

When the LMA sets up the multicast state and joins the group as the MAG's upstream router, the multicast packets are tunneled to the MAG that requested to receive the corresponding multicast session. The MAG then forwards the packets to the mobile node according to the multicast listener state maintained in the MAG. [1] supports only point-to-point access link types for MAG and mobile node connection;

hence a mobile node and the MAG are the only two nodes on an access link, where the link is assumed to be multicast capable.

6. Mobile Access Gateway Operation

The MAG performs the mobility management on behalf of a mobile node. This document assumes that the MAG is PIM-SM capable and forwards multicast packets to the corresponding mobile nodes attached to MAG by enabling the PIM-SM multicast routing protocol. In addition, the MAG must maintain multicast membership status for the attached mobile nodes at the edge and forwards the multicast data to the member mobile nodes. This condition requires MAG to support MLDv2 [7] or LW-MLDv2 [8], as well.

When mobile nodes subscribe multicast channel(s), they send MLD Report messages with their link-local address to the MAG, and the MAG sends the corresponding PIM Join messages to the upstream router if the MAG has no multicast state for the requested channel(s). The upstream router is selected by the Reverse Path Forwarding (RPF) lookup algorithm, and that is either the LMA or an adjacent multicast router attached to the same link. If the LMA is the upstream router for the channel(s) for the MAG, the MAG encapsulates PIM Join messages using the M-Tunnel.

The optimal multicast routing path may not include the LMA, especially in localized routing as described in Section 6.10.3 of [1] and [10]. The localized routing option is designed to support node-to-node communication within PMIPv6-Domain where a local content source exists. Details are described in Section 8.

7. Mobile Node Operation

Mobile nodes attached to the MAG can behave as regular receiver hosts. A mobile node sends MLD report messages to the MAG when it wants to subscribe and unsubscribe IP multicast channels.

In order to subscribe/unsubscribe multicast channel(s) by unsolicited report messages and inform current membership state by solicited report messages, mobile nodes MUST support either MLDv1 [7], MLDv2 [7], or LW-MLDv2 [8], and SHOULD support MLDv2 or LW-MLDv2.

8. Localized Multicast Routing

Localized routing defined in [10] allows mobile nodes attached to the same or different MAGs to directly exchange unicast traffic by using

localized forwarding or a direct tunnel between the MAGs. Localized routing must be initiated both MAG and LMA. Localized routing is not persistent, and is initiated by two signaling messages, Localized Routing Initiation (LRI) and Local Routing Acknowledgment (LRA), sent by LMA or MAG.

To support localized multicast routing with PIM-SM capable LMA and MAG, both LMA and MAG MUST include the routes organized by the localized routing procedure specified in [10] into their MRIBs. The exact mechanism to do this is not specified in this document and is left open for implementations and specific deployments.

To support localized routing for the case that a source node and a receiver node are attached to different MAGs but the same LMA (as seen in Section 6 of [10]), these MAGs must use the same tunneling mechanism for the data traffic tunneled between them. M-Tunnel defined in this document corresponds to the concept; these MAGs establish M-Tunnel and enable localized multicast routing.

9. Smooth Handover

The MAG is responsible for detecting the mobile node's movements to and from the access link and for initiating binding registrations to the mobile node's LMA. In PMIPv6, it does not require for mobile nodes to initiate to re-subscribe multicast channels, and the MAG keeps multicast channel subscription status for mobile nodes even if they move to a different MAG (i.e., n-MAG) in PMIPv6-Domain.

The MAG needs to join the multicast delivery tree when an attached mobile node subscribes a multicast channel. When the mobile node changes the network, it seamlessly receives multicast data from the new MAG according to the multicast channel information stored in the "MN's Policy Profile" or by some handover mechanisms such as [14] and [15]. Whether the MN's Policy Profile or a handover mechanism mobile operators use depend on their policy or implementation.

Here, a handover procedure using the MN's Policy Profile is described as an example. When the multicast channel information subscribed by mobile nodes is maintained in "MN's Policy Profile" stored in a policy store [1], the MAG can use the channel information to provide seamless handover. The procedures are described as follows and illustrated in Figure 6;

1. Figure 6 shows the examples that a mobile node has received multicast data from an upstream multicast router via p-MAG (*1) and from LMA via p-MAG (*2).

2. Whenever the mobile node moves a new network and attaches to n-MAG, the n-MAG obtains the MN-Identifier (MN-ID) and learns multicast channel information described in Mobile Node's Policy Profile associated to this MN-Identifier. Describing the method how the n-MAG identifies the p-MAG is out of scope of this document, while using the same mechanism described in [16] would be one of the possible methods.
3. If there are multicast channels the mobile node has subscribed but the n-MAG has not yet subscribed, n-MAG joins the corresponding multicast channels by sending the PIM Join message to its upstream router. If the upstream router is the LMA, the PIM messages are encapsulated and transmitted over the M-Tunnel (*4); otherwise the PIM messages are sent natively to the adjacent upstream router (*3).
4. The multicast data is forwarded from the LMA through the M-Tunnel between the LMA and n-MAG (*4) or from the adjacent upstream router (*3).

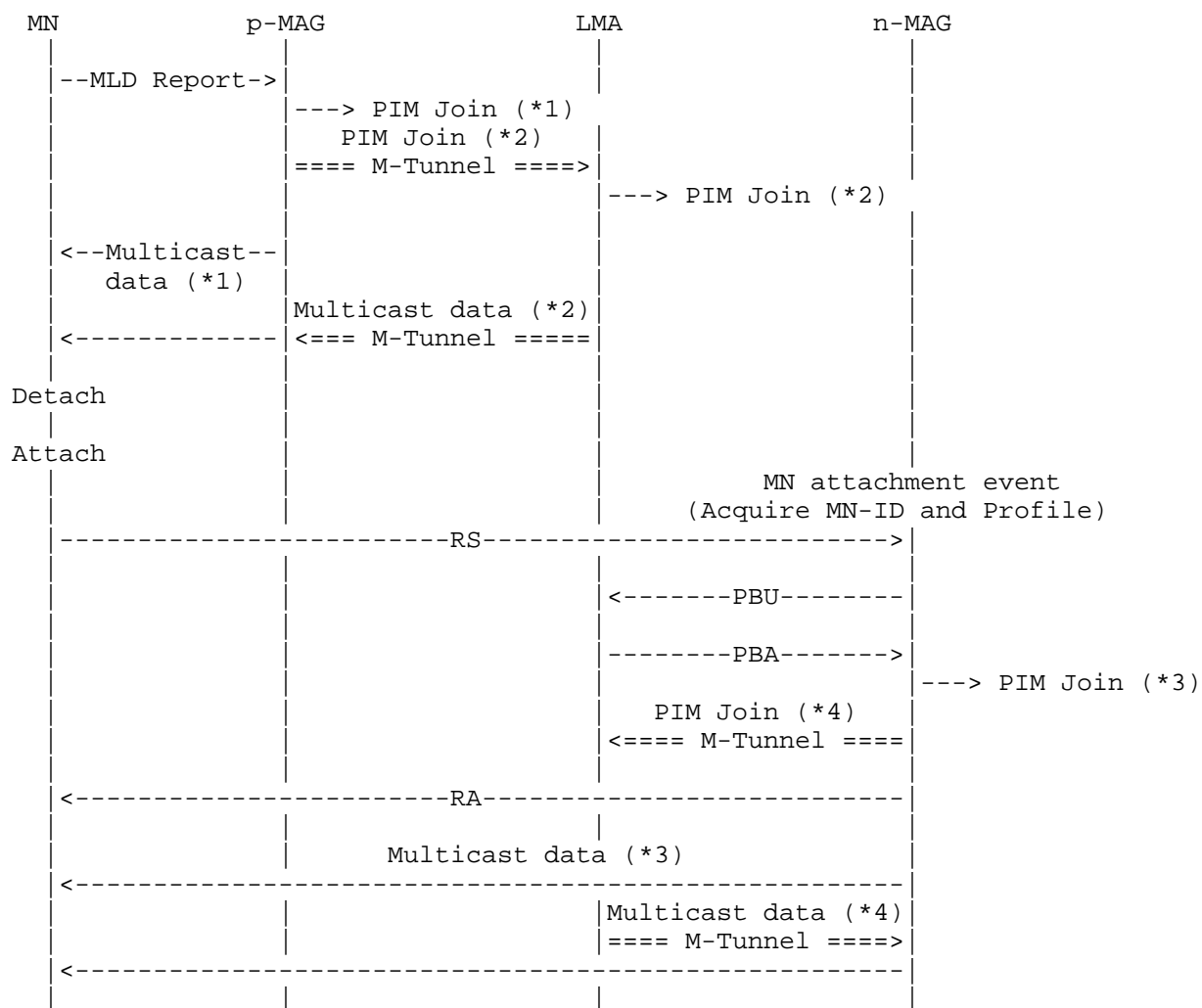


Figure 6: Handover with MN's Policy Profile

After MN attaches to n-MAG, the multicast data will be delivered to the MN immediately. MN's multicast membership state is maintained with MLD Query and Report messages exchanged by MN and n-MAG. If p-MAG thinks that the moving mobile node is the last member of multicast channel(s) (according to the membership record maintained by the explicit tracking function [17] or similar mechanism), p-MAG confirms it by sending MLD query. After the confirmation, p-MAG leaves the channel(s) by sending the PIM Prune message to its upstream router.

10. IANA Considerations

This document has no actions for IANA.

11. Security Considerations

TBD.

12. Acknowledgements

Many of the specifications described in this document are discussed and provided by the multimob mailing-list. Also, extensive comments were received from Sergio Figueiredo, Dirk von Hugo, and Stig Venaas.

13. References

13.1. Normative References

- [1] Gundavelli, S, Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [2] Fenner, B., He, H., Haberman, B., and H. Sandick, "Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")", RFC 4605, August 2006.
- [3] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.
- [4] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.
- [5] Bradner, S., "Key words for use in RFCs to indicate requirement levels", RFC 2119, March 1997.
- [6] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.
- [7] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.
- [8] Liu, H., Cao, W., and H. Asaeda, "Lightweight Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Version 2 (MLDv2) Protocols", RFC 5790,

February 2010.

- [9] Muhanna, A., Khalil, M., Gundavelli, S., and K. Leung, "Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6", RFC 5845, June 2010.
- [10] Krishnan, S., Koodli, R., Loureiro, P., Wu, Q., and A. Dutta, "Localized Routing for Proxy Mobile IPv6", RFC 6705, September 2012.
- [11] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

13.2. Informative References

- [12] Schmidt, T., Waehlich, M., and S. Krishnan, "Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains", RFC 6224, April 2011.
- [13] Thaler, D. and C. Hopps, "Multipath Issues in Unicast and Multicast Next-Hop Selection", RFC 2991, November 2000.
- [14] Contreras, LM., Bernardos, CJ., and I. Soto, "PMIPv6 multicast handover optimization by the Subscription Information Acquisition through the LMA (SIAL)", draft-ietf-multimob-handover-optimization-01.txt (work in progress), December 2012.
- [15] von Hugo, D. and H. Asaeda, "Context Transfer Protocol Extension for Multicast", draft-vonhugo-multimob-cxtp-extension-03.txt (work in progress), February 2013.
- [16] Yokota, H., Chowdhury, K., Koodli, R., Patil, B., and F. Xia, "Fast Handovers for Proxy Mobile IPv6", RFC 5949, September 2010.
- [17] Asaeda, H., "IGMP/MLD-Based Explicit Membership Tracking Function for Multicast Routers", draft-ietf-pim-explicit-tracking-04.txt (work in progress), January 2013.

Authors' Addresses

Hitoshi Asaeda
National Institute of Information and Communications Technology
4-2-1 Nukui-Kitamachi
Koganei, Tokyo 184-8795
Japan

Email: asaeda@nict.go.jp

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

Email: pierrick.seite@orange-ftgroup.com

MULTIMOB Working Group
INTERNET-DRAFT
Intended Status: Proposed Standard
Expires: April 18, 2013

Luis M. Contreras
Telefonica I+D
Carlos J. Bernardos
Universidad Carlos III de Madrid
Juan Carlos Zuniga
InterDigital
February 25, 2013

Extension of the MLD proxy functionality to support multiple
upstream interfaces
draft-contreras-multimob-multiple-upstreams-01

Abstract

This document presents different scenarios of applicability for an MLD proxy running more than one upstream interface. Since those scenarios impose different requirements on the MLD proxy with multiple upstream interfaces, it is important to ensure that the proxy functionality addresses all of them for compatibility.

The purpose of this document is to define the requirements in an MLD proxy with multiple interfaces covering a variety of applicability scenarios, and to specify the proxy functionality to satisfy all of them.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/lid-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>

Copyright and License Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1	Introduction	4
2.	Terminology	4
3.	Problem statement	4
4.	Scenarios of applicability	7
4.1	Fixed network scenarios	7
4.1.1	Multicast wholesale offer for residential services	7
4.1.1.1	Requirements	7
4.1.2	Multicast resiliency	8
4.1.2.1	Requirements	8
4.1.3	Load balancing for multicast traffic in the metro segment	8
4.1.3.1	Requirements	8
4.1.4	Summary of the requirements needed for mobile network scenarios	9
4.2	Mobile network scenarios	9
4.2.1	Applicability to multicast listener mobility	10
4.2.1.1	Single MLD proxy instance on MAG	10
4.2.1.1.1	Requirements	10
4.2.1.2	Remote and local multicast subscription	10
4.2.1.2.1	Requirements	11
4.2.1.3	Dual subscription to multicast groups during handover	11
4.2.1.3.1	Requirements	12
4.2.2	Applicability to multicast source mobility	12
4.2.2.1	Support of remote and direct subscription in basic source mobility	12
4.2.2.1.1	Requirements	13
4.2.2.2	Direct communication between source and listener associated with distinct LMAs but on the same MAG	13

4.2.2.3.1	Requirements	14
4.2.2.3	Route optimization support in source mobility for remote subscribers	14
4.2.2.3.1	Requirements	14
4.2.3	Summary of the requirements needed for mobile network scenarios	15
5	Functional specification of an MLD proxy with multiple interfaces	17
6	Security Considerations	17
7	IANA Considerations	17
8	Conclusions	17
9	Acknowledgements	17
10	References	17
10.1	Normative References	17
10.2	Informative References	17
	Appendix A. Basic support for multicast listener with PMIPv6	18
	Authors' Addresses	20

1 Introduction

The aim of this document is to define the functionality that an MLD proxy with multiple upstream interfaces should have in order to support different scenarios of applicability in both fixed and mobile networks. This compatibility is needed in order to simplify node functionality and to ensure an easier deployment of multicast capabilities in all the use cases described in this document.

2. Terminology

This document uses the terminology defined in [3]. Specifically, the definition of Upstream and Downstream interfaces, which are reproduced here for completeness.

Upstream interface:

A proxy device's interface in the direction of the root of the tree. Also called the "Host interface".

Downstream interface:

Each of a proxy device's interfaces that is not in the direction of the root of the tree. Also called the "Router interfaces".

3. Problem statement

The concept of MLD proxy with several upstream interfaces has emerged as a way of optimizing (and in some cases enabling) service delivery scenarios where separate multicast service providers are reachable through the same access network infrastructure. Figure 1 presents the conceptual model under consideration.

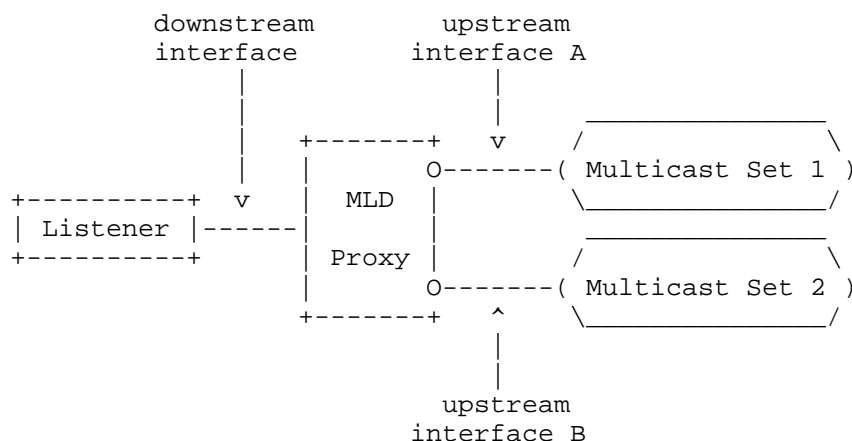


Figure 1. Concept of MLD proxy with multiple upstream interfaces

For illustrative purposes, two applications for fixed and mobile networks are here introduced. They will be elaborated later on the document.

In the case of fixed networks, multicast wholesale services in a competitive residential market require an efficient distribution of multicast traffic from different operators, i.e. the incumbent operator and a number of alternative ones, on the network infrastructure of the former. Existing proposals are based on the use of PIM routing from the metro network, and multicast traffic aggregation on the same tree. A different approach could be achieved with the use of an MLD proxy with multiple upstream interfaces, each of them pointing to a distinct multicast router in the metro border which is part of separated multicast trees deep in the network. Figure 2 graphically describes this scenario.

In the case of mobile networks, IP mobility services guarantee the continuity of the IP session while a Mobile Node (MN) changes its point of attachment. Proxy Mobile IPv6 (PMIPv6) [1] standardized a protocol that allows the network to manage the MN mobility without requiring specific support from the mobile terminal. The traffic to the MN is tunneled from the Home Network making use of two entities, one acting as mobility anchor, and the other as Mobility Access Gateway (MAG). Multicast support in PMIPv6 [2] implies the delivery of all the multicast traffic from the Home Network, via the mobility anchor. However, multicast routing optimization [4] could take advantage of an MLD proxy with multiple upstream interfaces by supporting the decision of subscribing a multicast content from the Home Network or from the local PMIPv6 domain if it is locally available. Figure 3 presents this scenario.

Informational text is provided in Appendix A summarizing how the basic solution for deploying multicast listener mobility with Proxy Mobile IPv6 works.

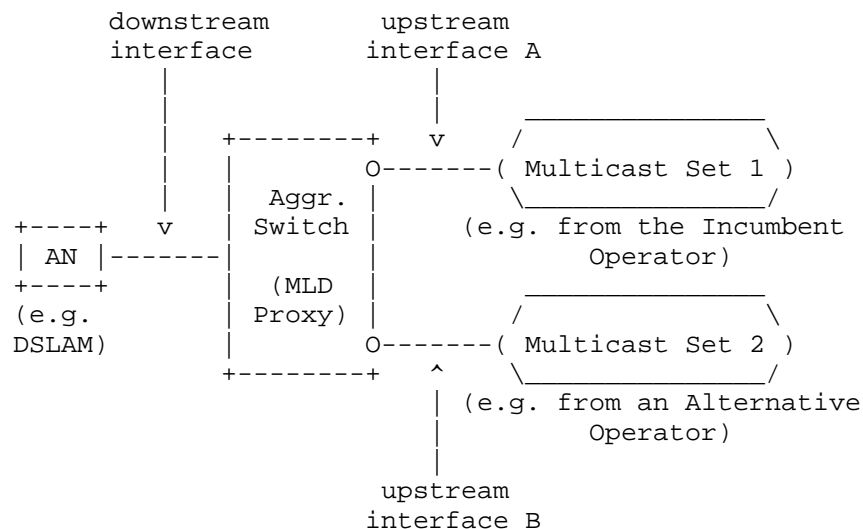


Figure 2. Example of usage of an MLD proxy with multiple upstream interfaces in a fixed network scenario

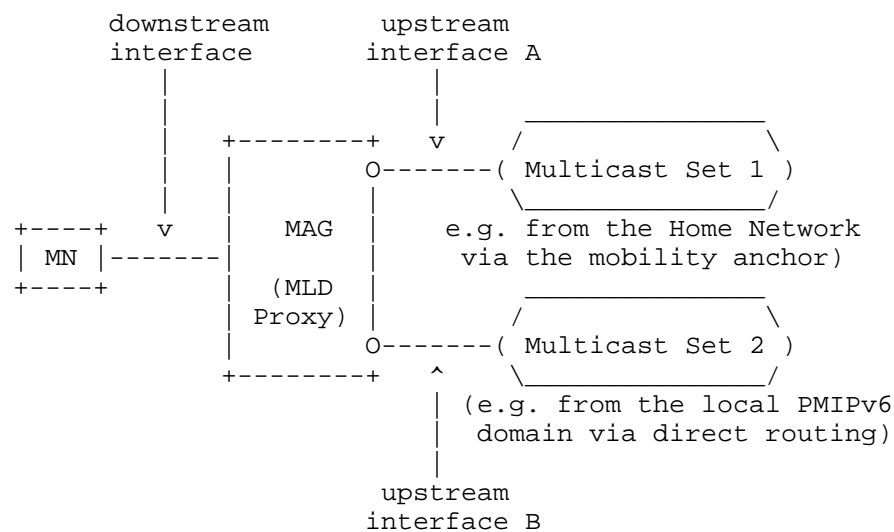


Figure 3. Example of usage of an MLD proxy with multiple upstream interfaces in a mobile network scenario

Since those scenarios can motivate distinct needs in terms of MLD proxy functionality, it is necessary to consider a comprehensive approach, looking at the possible scenarios, and establishing a minimum set of requirements which can allow the operation of a versatile MLD proxy with multiple upstream interfaces as a common entity to all of them (i.e., no different kinds of proxies depending on the scenario, but a common proxy applicable to all the potential scenarios).

4. Scenarios of applicability

This section describes in detail a number of scenarios of applicability of an MLD proxy with multiple upstream interfaces in place. A number of requirements for the MLD proxy functionality are identified from those scenarios.

4.1 Fixed network scenarios

Residential broadband users get access to multiple IP services through fixed network infrastructures. End user's equipment is connected to an access node, and the traffic of a number of access nodes is collected in aggregation switches.

For the multicast service, the use of an MLD proxy with multiple upstream interfaces in those switches can provide service flexibility in a lightweight and simpler manner if compared with PIM-routing based alternatives.

4.1.1 Multicast wholesale offer for residential services

This scenario has been already introduced in the previous section, and can be seen in Figure 2. There are two different operators, the one operating the fixed network where the end user is connected (e.g., typically an incumbent operator), and the one providing the Internet service to the end user (e.g., an alternative Internet service provider). Both can offer multicast streams that can be subscribed by the end user, independently of which provider contributes with the content.

Note that it is assumed that both providers offer distinct multicast groups. However, more than one subscription to multicast channels of different providers could take place simultaneously.

4.1.1.1 Requirements

- The MLD proxy should be able to deliver multicast control messages sent by the end user to the corresponding provider's multicast router.

- The MLD proxy should be able to deliver multicast control messages sent by each of the providers to the corresponding end user.

4.1.2 Multicast resiliency

In current PIM-based solutions, the resiliency of the multicast distribution relays on the routing capabilities provided by protocols like PIM and VRRP. A simpler scheme could be achieved by implementing different upstream interfaces on MLD proxies, providing path diversity through the connection to distinct leaves of a given multicast tree.

It is assumed that only one of the upstream interfaces is active in receiving the multicast content, while the other is up and in standby for fast switching.

4.1.2.1 Requirements

- The MLD proxy should be able to deliver multicast control messages sent by the end user to the corresponding active upstream interface.
- The MLD proxy should be able to deliver multicast control messages received in the active upstream to the end users, while ignoring the control messages of the standby upstream interface.
- The MLD proxy should be able of rapidly switching from the active to the standby upstream interface in case of network failure, transparently to the end user.

4.1.3 Load balancing for multicast traffic in the metro segment

A single upstream interface in existing MLD proxy functionality typically forces the distribution of all the channels on the same path in the last segment of the network. Multiple upstream interfaces could naturally split the demand, alleviating the bandwidth requirements in the metro segment.

4.1.3.1 Requirements

- The MLD proxy should be able to deliver multicast control messages sent by the end user to the corresponding multicast router which provides the channel of interest.
- The MLD proxy should be able to deliver multicast control messages sent by each of the multicast routers to the corresponding end user.
- The MLD proxy should be able to decide which upstream interface is selected for any new channel request according to defined criteria

(e.g., load balancing).

4.1.4 Summary of the requirements needed for mobile network scenarios

Following the analysis above, a number of different requirements can be identified by the MLD proxy to support multiple upstream interfaces in fixed network scenarios. The following table summarizes these requirements.

	Fixed Network Scenarios		
Functionality	Multicast Wholesale	Multicast Resiliency	Load Balancing
Upstream Control Delivery	X	X	X
Downstr. Control Delivery	X	X	X
Active / Standby Upstream		X	
Upstr i/f selection per group			X
Upstr i/f selection all group		X	

Table I. Functionality needed on MLD proxy with multiple upstream interfaces per application scenario in fixed networks

4.2 Mobile network scenarios

The mobile networks considered in this document are supposed to run PMIPv6 protocol for IP mobility management. A brief description of multicast provision in PMIPv6-based networks can be found in Appendix A.

The use of an MLD proxy supporting multiple upstream interfaces can improve the performance and the scalability of multicast-capable PMIPv6 domains.

4.2.1 Applicability to multicast listener mobility

Three sub-cases can be identified for the multicast listener mobility.

4.2.1.1 Single MLD proxy instance on MAG

The base solution for multicast service in PMIPv6 [2] assumes that any MN subscribed to multicast services receive the multicast traffic through the associated LMA, as in the unicast case. As standard MLD proxy functionality only supports one upstream interface, the MAG should implement several separated MLD proxy instances, one per LMA, in order to serve the multicast traffic to the MNs, according to any particular LMA-MN association.

A way of avoiding the multiplicity of MLD proxy instance in a MAG is to deploy a unique MLD proxy instance with multiple upstream interfaces, one per LMA, without any change in the multicast traffic distribution.

4.2.1.1.1 Requirements

- The MLD proxy should be able of delivering the multicast control messages sent by the MNs to the associated LMA.
- The MLD proxy should be able of delivering the multicast control messages sent by each of the connected LMAs to the corresponding MN.
- The MLD proxy should be able of routing the multicast data coming from different LMAs to the corresponding MNs according to the MN to LMA association.
- The MLD proxy should be able of maintaining a 1:1 association between an MN and LMA (or downstream to upstream).

4.2.1.2 Remote and local multicast subscription

This scenario has been already introduced in the previous section, and can be seen in Figure 3. Standard MLD proxy definition, with a unique upstream interface per proxy, does not allow the reception of multicast traffic from distinct upstream multicast routers. In other words, all the multicast traffic being sent to the MLD proxy in

downstream traverses a concrete, unique router before reaching the MAG. There are, however, situations where different multicast content could reach the MLD proxy through distinct next-hop routers.

For instance, the solution adopted to avoid the tunnel convergence problem in basic multicast PMIPv6 deployments [4] considers the possibility of subscription to a multicast source local to the PMIPv6 domain. In that situation, some multicast content will be accessed remotely, through the home network via the multicast tree mobility anchor, while some other multicast content will reach the proxy directly, via a local router in the domain.

4.2.1.2.1 Requirements

- The MLD proxy should be able of delivering the multicast control messages sent by the MNs to the associated upstream interface based on the location of the source, remote or local, for a certain multicast group.
- The MLD proxy should be able of delivering the multicast control messages sent either local or remotely to the corresponding MNs.
- The MLD proxy should be able of routing the multicast data coming from different upstream interfaces to a certain MN according to the MN subscription, either local or remote. Note that it is assumed that a multicast group can be subscribed either locally or remotely, but not simultaneously. However more than one subscription could happen, being local or remote independently.
- The MLD proxy should be able of maintaining a 1:N association between an MN and the remote and local multicast router (or downstream to upstream).
- The MLD proxy should be able of switching between local or remote subscription for per multicast group according to specific configuration parameters (out of the scope of this document).

4.2.1.3 Dual subscription to multicast groups during handover

In the event of an MN handover, once an MN moves from a previous MAG (pMAG) to a new MAG (nMAG), the nMAG needs to set up the multicast status for the incoming MN, and subscribe the multicast channels it was receiving before the handover event. The MN will then experience a certain delay until it receives again the subscribed content.

A generic solution is being defined in [5] to speed up the knowledge of the ongoing subscription by the nMAG. However, for the particular case that the underlying radio access technology supports layer-2

triggers (thus requiring extra capabilities on the mobile node), there could be inter-MAG cooperation for handover support if pMAG and nMAG are known in advance.

This could be the case, for instance for those contents not already arriving to the nMAG, where the nMAG temporally subscribes the multicast groups of the ongoing MN's subscription via the pMAG, while the multicast delivery tree among the nMAG and the mobility anchor is being established.

A similar approach is followed in [6] despite the solution proposed there differs from this approach (i.e., there is no consideration of an MLD proxy with multiple interfaces).

4.2.1.3.1 Requirements

- The MLD proxy should be able of delivering the multicast control messages sent by the MNs to the associated upstream interface based on the handover specific moment, for a certain multicast group.
- The MLD proxy should be able of delivering the multicast control messages sent either from pMAG or the multicast anchor to the corresponding MNs, based on the handover specific moment.
- The MLD proxy should be able of handle the incoming packet flows from the two simultaneous upstream interfaces, in order to not duplicate traffic delivered on the point-to-point link to the MN.
- The MLD proxy should be able of maintaining a 1:N association between an MN and both the remote multicast router and the pMAG (or downstream to upstream).
- The MLD proxy should be able of switching between local or remote subscription for all the multicast groups (from pMAG to multicast anchor) according to specific configuration parameters (out of the scope of this document).

4.2.2 Applicability to multicast source mobility

A couple of sub-cases can be identified for the multicast source mobility.

4.2.2.1 Support of remote and direct subscription in basic source mobility

In the basic case of source mobility, the multicast source is connected to one of the downstream interfaces of an MLD proxy. According to the standard specification [3] every packet sent by the

multicast source will be forwarded towards the root of the multicast tree.

However, linked to the mobility listener problem, there could be the case of simultaneous remote subscribers, subscribing to the multicast content through the home network, and local subscribers, requesting the contents directly via a multicast router residing on the same PMIPv6 domain where the source is attached to.

Then, in order to provide the co-existence of both types of subscribers, an MLD proxy with two upstream interfaces could simultaneously serve all kind of multicast subscribers.

Basic source mobility is being defined in [7] but the solution proposed there does not allow simultaneous co-existence of remote and local subscribers (i.e., the content sent by the source is either distributed locally to a multicast router in the PMIPv6 domain, or remotely by using the bi-directional tunnel towards the mobility anchor, but not both simultaneously).

4.2.2.1.1 Requirements

- The MLD proxy should be able of forwarding (replicating) the multicast content to both upstream interfaces, in case of simultaneous remote and local distribution.
- The MLD proxy should be able of handling control information incoming through any of the two upstream interfaces, providing the expected behavior for each of the multicast trees.
- The MLD proxy should be able of routing the multicast data towards different upstream interfaces for both remote and local subscriptions that could happen simultaneously.
- The MLD proxy should be able of maintaining a 1:N association between an MN and both the remote and local multicast router (or downstream to upstream).

4.2.2.2 Direct communication between source and listener associated with distinct LMAs but on the same MAG

In a certain PMIPv6 domain can be MNs associated to distinct LMAs using the same MAG to get access to their corresponding home networks. For multicast communication, according to the base solution [2], each MN <-> LMA association implies a distinct MLD proxy instance to be invoked in the MAG.

In these conditions, when a mobile source is serving multicast content to a mobile listener, both attached to the same MAG but each of them associated to different LMAs, the multicast flow must traverse the PMIPv6 domain from the MAG to the LMA where the source maintains an association, then from that LMA to the LMA where the listener is associated to, and finally come back to the same MAG from where the flow departed. This routing is extremely inefficient.

An MLD proxy with multiple upstream interfaces avoids this behavior since it allows to invoke a unique MLD proxy instance in the MAG. In this case, the multicast source can directly communicate with the multicast listener, without need for delivering the multicast traffic to the LMAs.

4.2.2.3.1 Requirements

- The MLD proxy should be able of forwarding (replicating) the multicast content to different upstream or downstream interfaces where subscribers are present.
- The MLD proxy should be able of handling control information incoming through any of the upstream or downstream interfaces requesting a multicast flow being injected in another downstream interface.
- The MLD proxy should be able of maintaining a 1:N association between an MN and any of the upstream or downstream interfaces demanding the multicast content.

4.2.2.3 Route optimization support in source mobility for remote subscribers

Even in a scenario of remote subscription, there could be the case where both the source and the listener are attached to the same PMIPv6-Domain (for instance, no possibility of direct routing within the PMIPv6, or source and listener pertaining to distinct home networks). In this situation there is a possibility of route optimization if inter-MAG communication is enabled, in such a way that the listeners in the PMIPv6 domain are served through the tunnels between MAGs, while the rest of remote listeners are served through the mobility anchor.

A multi-upstream MLD proxy would allow the simultaneous delivery of traffic to such kind of remote listeners.

A similar route optimization approach is proposed in [8].

4.2.2.3.1 Requirements

- The MLD proxy should be able of forwarding (replicating) the multicast content to both kinds of upstream interfaces, inter-MAG tunnel interfaces and MAG to mobility anchor tunnel interface.
- The MLD proxy should be able of handling control information incoming through any of the two types of upstream interfaces, providing the expected behavior for each of the multicast trees (e.g., no forwarding traffic on one inter-MAG link once there are not more listeners requesting the content).
- The MLD proxy should be able of routing the multicast data towards different upstream interfaces for both remote and route optimized subscriptions that could happen simultaneously.
- The MLD proxy should be able of maintaining a 1:N association between an MN and both the remote and local MAGs (or downstream to upstream).

4.2.3 Summary of the requirements needed for mobile network scenarios

After the previous analysis, a number of different requirements can be identified by the MLD proxy to support multiple upstream interfaces in mobile network scenarios. The following table summarizes these requirements.

Functionality	Mobile Network Scenarios					
	Multicast Listener			Multicast Source		
	Single MLD Proxy	Remote & local subscr.	Dual subscr. in HO	Direct & remote subscr.	Listener & source on MAG	Route optimi.
Upstream Control Delivery	X	X	X	X	X	X
Downstr. Control Delivery	X	X	X		X	
Upstream Data Delivery				X		X
Downstr. Data Delivery	X	X	X		X	
1:1 MN to upstream assoc.	X					
1:N MN to upstream assoc.		X	X	X	X	X
Upstr i/f selection per group		X				
Upstr i/f selection all group			X			
Upstream traffic replicat.				X		X

Table II. Functionality needed on MLD proxy with multiple upstream interfaces per application scenario in mobile networks

5 Functional specification of an MLD proxy with multiple interfaces

<To be completed>.

6 Security Considerations

<To be completed>.

7 IANA Considerations

<IANA considerations text>.

8 Conclusions

<To be completed>.

9 Acknowledgements

The authors thank Stig Venaas for his valuable comments and suggestions.

The research of Carlos J. Bernardos leading to these results has received funding from the European Community's Seventh Framework Programme (FP7-ICT-2009-5) under grant agreement n. 258053 (MEDIEVAL project), being also partially supported by the Ministry of Science and Innovation (MICINN) of Spain under the QUARTET project (TIN2009-13992-C02-01).

10 References

10.1 Normative References

- [1] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [2] T.C. Schmidt, M. Waehlich, and S. Krishnan, "A Minimal Deployment Option for Multicast Listeners in PMIPv6 Domains", RFC6224, April 2011.
- [3] B. Fenner, H. He, B. Haberman, and H. Sandick, "Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")", RFC 4605, August 2006.

10.2 Informative References

- [4] J.C. Zuniga, L.M. Contreras, C.J. Bernardos, S. Jeon, Y. Kim, "Multicast Mobility Routing Optimizations for Proxy Mobile IPv6", work in progress, draft-ietf-multimob-pmipv6-ropt-01, September 2012.
- [5] L.M. Contreras, C.J. Bernardos, I. Soto, "PMIPv6 multicast handover optimization by the Subscription Information Acquisition through the LMA (SIAL)", work in progress, draft-ietf-multimob-fast-handover-01, July 2012.
- [6] T.C. Schmidt, M. Waehlich, R. Koodli, G. Fairhurst, "Multicast Listener Extensions for MIPv6 and PMIPv6 Fast Handovers", work in progress, draft-schmidt-multimob-fmipv6-pfmipv6-multicast-06, May 2012
- [7] T.C. Schmidt, S. Gao, H. Zhang, M. Waehlich, "Mobile Multicast Sender Support in Proxy Mobile IPv6 (PMIPv6) Domains", work in progress, draft-ietf-multimob-pmipv6-source-01, July 2012.
- [8] J. Liu, W. Luo, "Routes Optimization for Multicast Sender in Proxy Mobile IPv6 Domain", work in progress, draft-liu-multimob-pmipv6-multicast-ro-02, July 2012.

Appendix A. Basic support for multicast listener with PMIPv6

This section briefly summarizes the operation of Proxy Mobile IPv6 [1] and how multicast listener support works with PMIPv6 as specified in [2].

Proxy Mobile IPv6 (PMIPv6) [1] is a network-based mobility management protocol which enables the network to provide mobility support to standard IP terminals residing in the network. These terminals enjoy this mobility service without being required to implement any mobility-specific IP operations. Namely, PMIPv6 is one of the mechanisms adopted by the 3GPP to support the mobility management of non-3GPP terminals in future Evolved Packet System (EPS) networks.

PMIPv6 allows a Media Access Gateway (MAG) to establish a distinct bi-directional tunnel with different Local Mobility Anchors (LMAs), being each tunnel shared by the attached Mobile Nodes (MNs). Each mobile node is associated with a corresponding LMA, which keeps track of its current location, that is, the MAG where the mobile node is attached. IP-in-IP encapsulation is used within the tunnel to forward traffic between the LMA and the MAG. Figure 4 (taken from [1]) shows the architecture of a PMIPv6 domain.

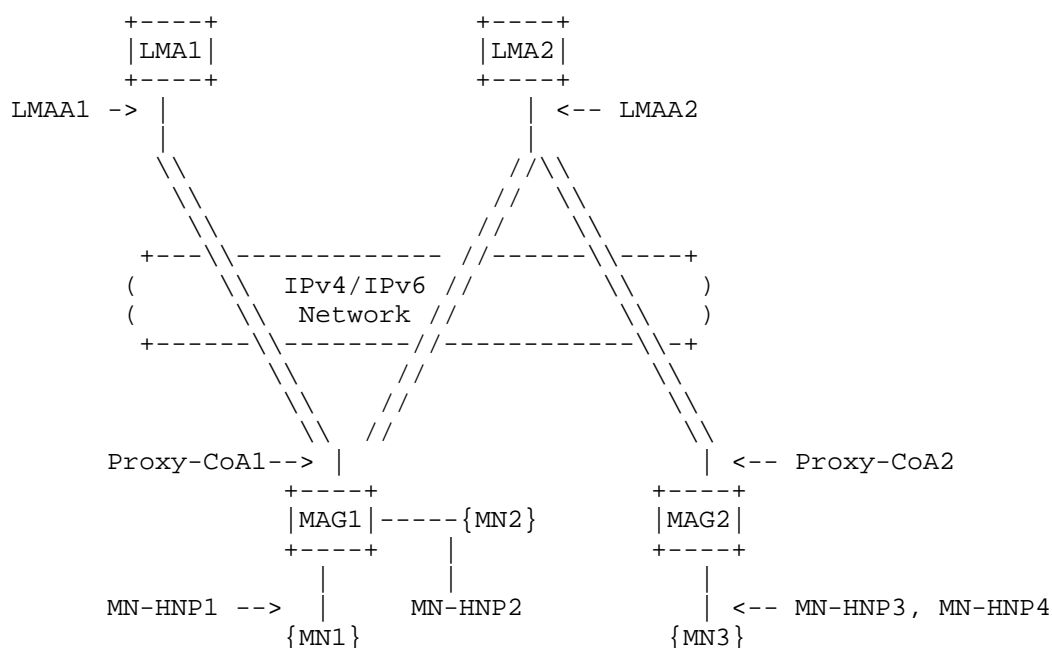


Figure 4. Proxy Mobile IPv6 Domain

The basic solution for the distribution of multicast traffic within a PMIPv6 domain [2] makes use of the bi-directional LMA-MAG tunnels. The base solution follows the so-called remote subscription model, in which the subscribed multicast content is delivered from the Home Network. By doing so, an individual copy of every multicast flow is delivered through the tunnel connecting the mobility anchor to any of the access gateways in the domain. In many cases, these individual copies traverse the same routers in the path towards the access gateways, incurring in an inefficient distribution, equivalent to the unicast distribution of the multicast content in the domain.

The reference scenario for multicast deployment in Proxy Mobile IPv6 domains is illustrated in Figure 5 (taken from [2]).

This fact leads to distribution inefficiencies and higher per-bit delivery costs, incurred by the PMIPv6 domain operator offering transport capabilities to the Home Network operator for serving their MNs when attached to the PMIPv6 domain. As long as the remotely subscribed multicast service is not affected, it seems worthy to explore more optimal ways of distributing such content within the PIMIPv6 domain.

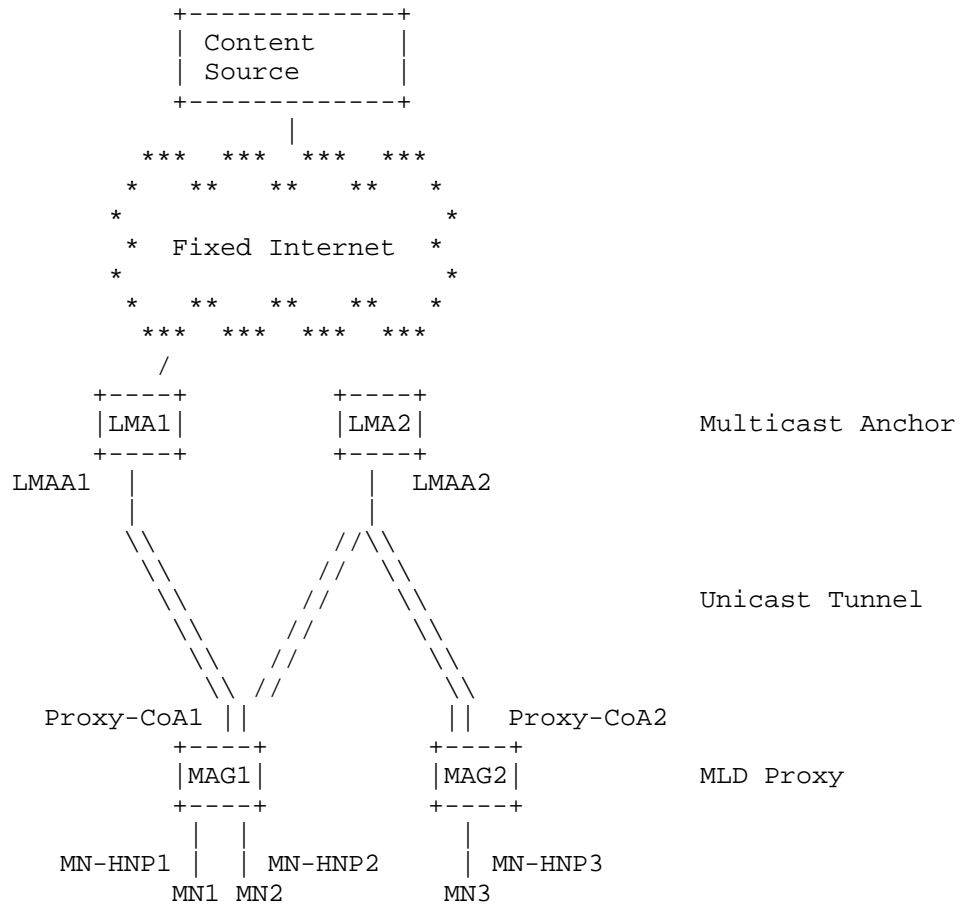


Figure 5. Reference Network for Multicast Deployment in PMIPv6

Authors' Addresses

Luis M. Contreras
 Telefonica I+D
 EMail: lmcm@tid.es

Carlos J. Bernardos
 Universidad Carlos III de Madrid
 EMail: cjbcb@it.uc3m.es

INTERNET DRAFT

MLD proxy with multiple upstream

February 25, 2012

Juan Carlos Zuniga
InterDigital Communications, LLC
EMail: JuanCarlos.Zuniga@InterDigital.com

Internet Area
Internet Draft
Intended status: Informational
Expires: Sep. 13, 2012

M.Hui
H.Deng
D.Liu
China Mobile
March 13, 2012

Fast Handover for Multicast in Proxy Mobile IPv6
draft-hui-multimob-fast-handover-04

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>

This Internet-Draft will expire on Jan 01, 2011.

Copyright Notice

Copyright (c) 2009 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.

Abstract

This document specifies the predictive fast handover mechanism to solve the problem of handover latency and packet loss in Proxy Mobile IPv6 Multicast. Necessary extensions are specified for Handover Initiate (HI) and Handover Acknowledgement (HAck) messages to support multicast handover procedure.

Table of Contents

1. Introduction.....	4
2. Problem Statement.....	5
3. Terminology.....	6
4. Protocol Operation.....	7
5. Message Format.....	11
6. Security Considerations.....	13
7. IANA Considerations.....	14
8. References.....	15
8.1. Normative References.....	15
8.2. Informative References.....	15
Author's Addresses.....	16

1. Introduction

Proxy Mobile IPv6 (PMIPv6) protocol provides local mobility management to a mobile node without requiring any modification of the mobile node. The Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG) perform the mobility management signaling on behalf of the mobile node. Extensions for LMA and MAG are specified in [1] to support IP multicast in PMIPv6. Nevertheless, the basic performance including handover latency and packet loss is not considered different from that of PMIPv6.

Fast handover for Mobile IPv6 is specified in [2]. [3] extends the FMIPv6 and applies it to the PMIPv6 in order to decrease handover latency and packet loss as well as transfer of network-resident contexts. However, IP multicast is not considered in fast handover for PMIPv6.

We propose a fast handover mechanism to support multicast for PMIPv6. Necessary extensions are specified in HI and HAcK message to transfer the multicast node's context information and deliver the multicast data before the set up of tunnel between n-MAG and LMA.

2. Problem Statement

The existing solution for PMIPv6 multicast [1] specifies that, only after the bi-directional tunnel is built between n-MAG and LMA using extended PBU (PBU-M) message, the multicast packet can be continuously delivered to MN. It inevitably causes the latency and loss of packet during handover process.

The solution presents two ways to acquire the MN's profile, which includes MN' ID and multicast state information. One way is to use the Context Transfer Protocol (CXTTP) [4] to transfer MN's profile from p-MAG to n-MAG. In the other way, if MN's profile is stored in a policy store [5], n-MAG obtains MN's multicast state by the same mechanism used to acquire MN' ID and profile during MN's attachment process [5].

In another PMIPv6 multicast solution [6], the author proposes normal handover and fast handover for proxy mobile multicast service. There is no any optimization in normal handover, the handover involves MN by running the MLDv2 [7] protocol with n-MAG to receive the related multicast packet. In the fast handover procedure, similar to the first method used in [1], the context transfer is used to provide multicast information. Although n-MAG can acquire the MN' multicast information before MN handovers to it, only after n-MAG joins the multicast group, it can receive the multicast data.

3. Terminology

This document refers to [1] [2] [3] for terminology. The following terms and abbreviations are additionally used in this document. The reference network is illustrated in Figure 1.

Previous Mobile Access Gateway (p-MAG):

The MAG that manages mobility related signaling for the MN before handover.

New Mobile Access Gateway (n-MAG):

The MAG that manages mobility related signaling for the MN after handover.

HO-Initiate:

A generic signaling that indicates the handover of the MN sent from the MN to the p-MAG. It is assumed that HO-Initiate can carry the information to identify the MN and to assist the p-MAG to resolve the n-MAG.

4. Protocol Operation

The architecture of fast handover for multicast in Proxy Mobile IPv6 is shown in Figure 1. A multicast tunnel is established to transfer the multicast data from p-MAG to n-MAG before the n-MAG joins the multicast group, so that whenever the MN handovers to the n-MAG, it can receive the multicast data from n-MAG.

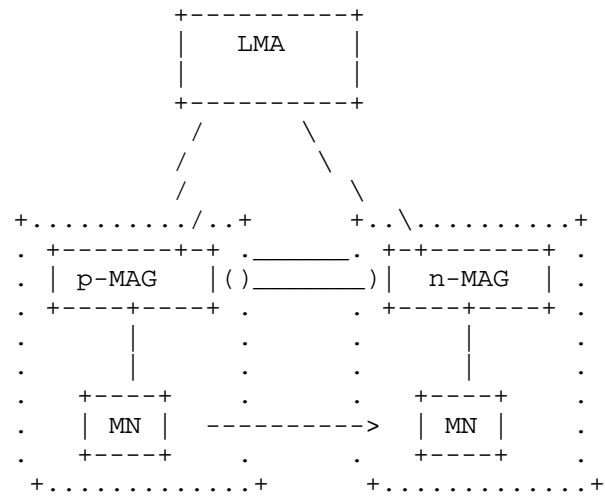


Figure 1: Reference network for fast handover

In order to decrease the handover latency and packet loss, this document specifies a bi-directional tunnel between the Previous MAG (p-MAG) and the New MAG (n-MAG). As the n-MAG needs the multicast node's context information to set up a bi-directional tunnel to continuous deliver multicast packet to mobile node, the HI and HAck messages are extended to support mobile multicast node's context transfer, in which parameters such as MN ID, MN Multicast State, are transferred from the p-MAG to the n-MAG. The sequence of events illustrating the fast handover for multicast is shown in Figure 2.

	MN	p-MAG	n-MAG	LMA
(1)	HO Initiate			
	--(MN ID,-->			

		n-MAG ID)			
(2)				HI	
				--(MN ID, -->	
				MN Multicast State)	
(3)				<---HACK---	
				(MN ID)	
				HI/HACK	
(4)				<----->	
(5)				M data	
				====tunnel====>	
(6)	~~~				
	~~~				
(7)		<=====M data=====			
(8)				-----PBU-M----->	
(9)				<-----PBA-----	
(10)				M data	
				<==bi-dir tunnel==>	

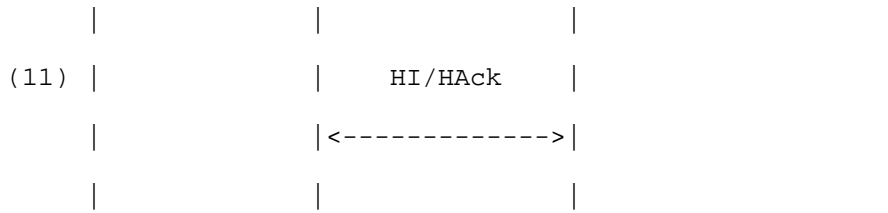


Figure 2: Fast handover for PMIPv6 multicast

The detailed descriptions are as follows:

- (1)The MN detects that a handover is imminent and reports the MN ID and n-MAG ID.
- (2)The p-MAG sends the HI to the n-MAG. The HI message includes MN ID and MN Multicast State.
- (3)The n-MAG sends the HAcK back to the p-MAG.
- (4)The n-MAG requests the p-MAG to forward multicast packets by setting F flags in the HI message.
- (5)A tunnel is established between the p-MAG and n-MAG and multicast packets destined for the MN are forwarded from the p-MAG to the n-MAG over this tunnel.
- (6)The MN undergoes handover to n-MAG.
- (7)The n-MAG starts to forward multicast packets destined for the MN.
- (8)The n-MAG sends the Proxy Binding Update with multicast extension (PBU-M)(proposed in [1]) to the LMA.
- (9)The LMA sends back the Proxy Binding Acknowledgment (PBA) to the n-MAG.
- (10)A bi-directional tunnel is set up for forwarding corresponding multicast data.

(11) Multicast packet forwarding is completed between p-MAG and n-MAG.



## 5. Message Format

This document defines new Mobility Header messages for the extended HI and HAcK and new mobility options for delivering context information.

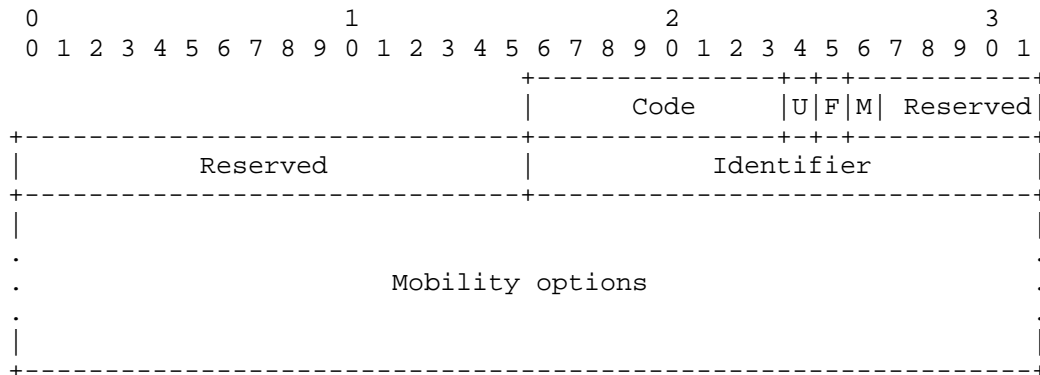
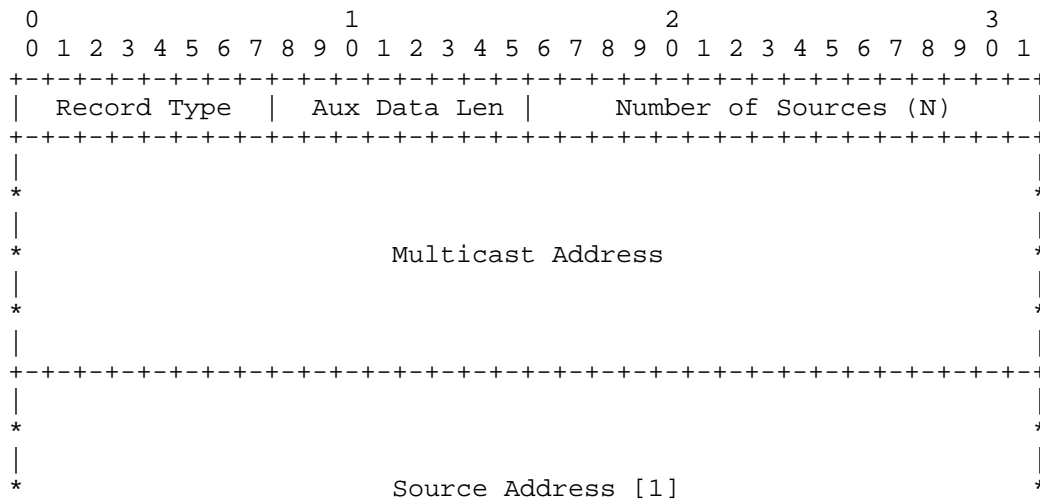
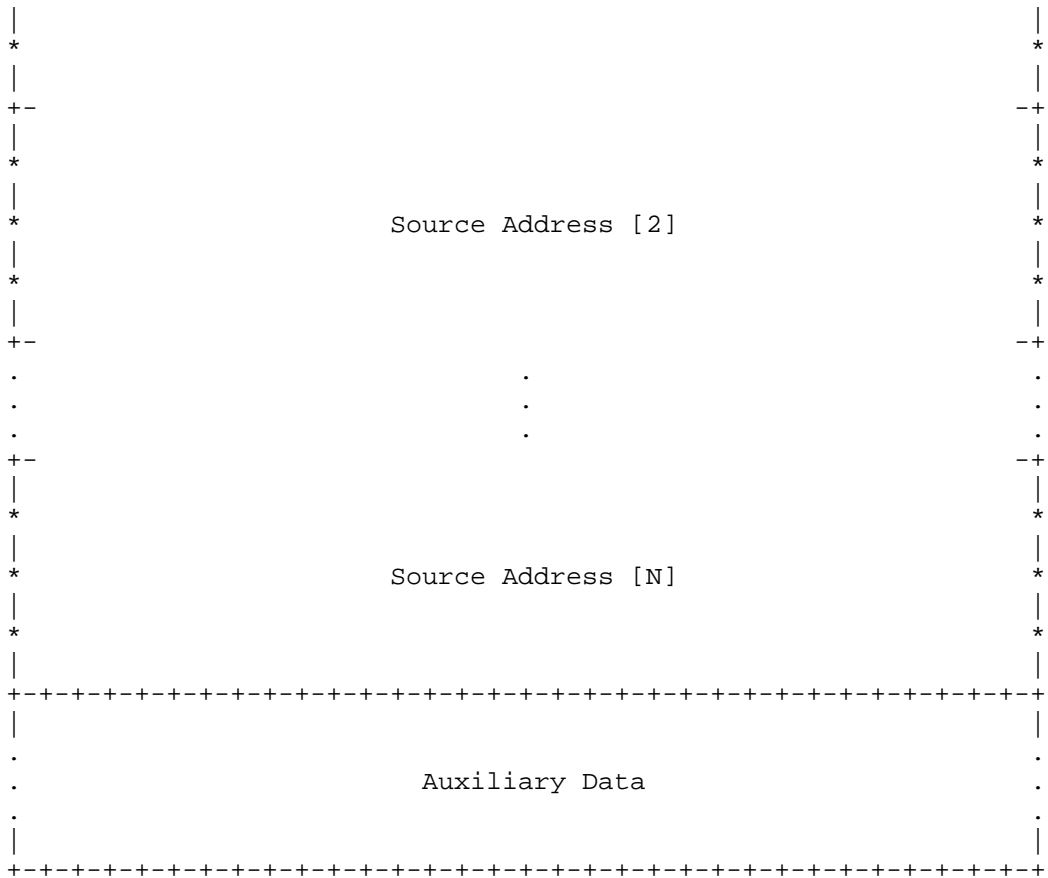


Figure 3: HI Mobility Header message with multicast extension

A new flag (M) is included in the HI Mobility Header message with multicast extension. The rest of the message format remains the same as defined in [3].

When (M) flag is specified in HI Mobility Header message, the mobility options field needs to be extended to include the multicast addresses.





## 6. Security Considerations

TBD.

## 7. IANA Considerations

This document does not require any IANA action.

## 8. References

### 8.1. Normative References

- [1] H. Asaeda, P. Seite, J. Xia, "PMIPv6 Extensions for Multicast", draft-asaeda-multimob-pmipv6-extension-01.txt (work in progress), July 2009.
- [2] Koodli, R., Ed., "Mobile IPv6 Fast Handovers", RFC 5268, June 2008.
- [3] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, F. Xia, "Fast Handovers for Proxy Mobile IPv6", draft-irtf-mipshop-pfmipv6-00.txt (work in progress), October 2008.
- [4] Loughney, Ed., J., Nakhjiri, M., Perkins, C., and R. Koodli, "Context Transfer Protocol (CXTP)", RFC 4067, July 2005.
- [5] Gundavelli, S, Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [6] Y K. ZHAO, P. Seite, "The Solution for Pmipv6 Multicast Service", draft-zhao-multimob-pmipv6-solution-02.txt (work in progress), November 2008.
- [7] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

### 8.2. Informative References

Author's Addresses

Min Hui  
China Mobile  
53A,Xibianmennei Ave.,  
Xuanwu District,  
Beijing 100053  
China  
Email: huimin.cmcc@gmail.com

Hui Deng  
China Mobile  
53A,Xibianmennei Ave.,  
Xuanwu District,  
Beijing 100053  
China  
Email: denghui02@gmail.com

Dapeng Liu  
China Mobile  
53A,Xibianmennei Ave.,  
Xuanwu District,  
Beijing 100053  
China  
EMail: liudapeng@chinamobile.com



MULTIMOB Group  
Internet-Draft  
Intended status: Experimental  
Expires: August 30, 2013

T C. Schmidt, Ed.  
HAW Hamburg  
M. Waehlich  
link-lab & FU Berlin  
R. Koodli  
Cisco Systems  
G. Fairhurst  
University of Aberdeen  
Dapeng. Liu  
China Mobile  
February 26, 2013

Multicast Listener Extensions for MIPv6 and PMIPv6 Fast Handovers  
draft-ietf-multimob-fmipv6-pfmipv6-multicast-01

## Abstract

Fast handover protocols for MIPv6 and PMIPv6 define mobility management procedures that support unicast communication at reduced handover latency. Fast handover base operations do not affect multicast communication, and hence do not accelerate handover management for native multicast listeners. Many multicast applications like IPTV or conferencing, though, are comprised of delay-sensitive real-time traffic and will benefit from fast handover execution. This document specifies extension of the Mobile IPv6 Fast Handovers (FMIPv6) and the Fast Handovers for Proxy Mobile IPv6 (PFMIPv6) protocols to include multicast traffic management in fast handover operations. This multicast support is provided first at the control plane by a management of rapid context transfer between access routers, second at the data plane by an optional fast traffic forwarding that may include buffering.

## Status of this Memo

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

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

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



This Internet-Draft will expire on August 30, 2013.

#### Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	4
2. Terminology . . . . .	5
3. Protocol Overview . . . . .	5
3.1. Multicast Context Transfer between Access Routers . . . . .	6
3.2. Protocol Operations Specific to FMIPv6 . . . . .	8
3.3. Protocol Operations Specific to PFMIPv6 . . . . .	10
4. Protocol Details . . . . .	13
4.1. Protocol Operations Specific to FMIPv6 . . . . .	13
4.1.1. Operations of the Mobile Node . . . . .	13
4.1.2. Operations of the Previous Access Router . . . . .	14
4.1.3. Operations of the New Access Router . . . . .	15
4.1.4. Buffering Considerations . . . . .	15
4.2. Protocol Operations Specific to PFMIPv6 . . . . .	16
4.2.1. Operations of the Mobile Node . . . . .	16
4.2.2. Operations of the Previous MAG . . . . .	16
4.2.3. Operations of the New MAG . . . . .	17
4.2.4. IPv4 Support Considerations . . . . .	18
5. Message Formats . . . . .	18
5.1. Multicast Indicator for Proxy Router Advertisement (PrRtAdv) . . . . .	18
5.2. Extensions to Existing Mobility Header Messages . . . . .	19
5.3. New Multicast Mobility Option . . . . .	19
5.4. New Multicast Acknowledgement Option . . . . .	21
5.5. Length Considerations: Number of Records and Addresses . . . . .	22
5.6. MLD (IGMP) Compatibility Aspects . . . . .	22
6. Security Considerations . . . . .	22
7. IANA Considerations . . . . .	23
8. Acknowledgments . . . . .	23
9. References . . . . .	24
9.1. Normative References . . . . .	24
9.2. Informative References . . . . .	24
Appendix A. Change Log . . . . .	25
Authors' Addresses . . . . .	26

## 1. Introduction

Mobile IPv6 [RFC3775] defines a network layer mobility protocol involving participation by mobile nodes, while Proxy Mobile IPv6 [RFC5213] provides a mechanism without requiring mobility protocol operations at a Mobile Node (MN). Both protocols introduce traffic disruptions on handovers that may be intolerable in many real-time application scenarios such as gaming or conferencing. Mobile IPv6 Fast Handovers (FMIPv6) [RFC5568], and Fast Handovers for Proxy Mobile IPv6 (PFMIPv6) [RFC5949] improve these handover delays for unicast communication to the order of the maximum delay needed for link switching and signaling between Access Routers (ARs) or Mobile Access Gateways (MAGs) [FMIPv6-Analysis].

No dedicated treatment of seamless multicast data reception has been proposed by any of the above protocols. MIPv6 only roughly defines multicast for Mobile Nodes using a remote subscription approach or a home subscription through bi-directional tunneling via the Home Agent (HA). Multicast forwarding services have not been specified at all in [RFC5213], but are subject to current specification [RFC6224]. It is assumed throughout this document that mechanisms and protocol operations are in place to transport multicast traffic to ARs. These operations are referred to as 'JOIN/LEAVE' of an AR, while the explicit techniques to manage multicast transmission are beyond the scope of this document.

Mobile multicast protocols need to serve applications such as IPTV with high-volume content streams to be distributed to potentially large numbers of receivers, and therefore should preserve the multicast nature of packet distribution and approximate optimal routing [RFC5757]. It is undesirable to rely on home tunneling for optimizing multicast. Unencapsulated, native multicast transmission requires establishing forwarding state, which will not be transferred between access routers by the unicast fast handover protocols. Thus multicast traffic will not experience expedited handover performance, but an MN - or its corresponding MAG in PFMIPv6 - can perform remote subscriptions in each visited network.

This document specifies extensions to FMIPv6 and PFMIPv6 that include multicast traffic management for fast handover operations. The solution common to both underlying protocols defines the per-group transfer of multicast contexts between ARs or MAGs. The protocol defines corresponding message extensions necessary for carrying group context information independent of the particular handover protocol. ARs or MAGs are then enabled to treat multicast traffic according to fast unicast handovers and with similar performance. No protocol changes are introduced that prevent a multicast unaware node from performing fast handovers with multicast aware ARs or MAGs.

The specified mechanisms apply when a mobile node has joined and maintains one or several multicast group subscriptions prior to undergoing a fast handover. It does not introduce any requirements on the multicast routing protocols in use, nor are the ARs or MAGs assumed to be multicast routers. It assumes network conditions, though, that allow native multicast reception in both, the previous and new access network. Methods to bridge regions without native multicast connectivity are beyond the scope of this document.

## 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119]. The use of the term, "silently ignore" is not defined in RFC 2119. However, the term is used in this document and can be similarly construed.

This document uses the terminology of [RFC5568], [RFC5949], [RFC3775], and [RFC5213]. In addition, the following terms are introduced:

## 3. Protocol Overview

This section provides an informative overview of the protocol mechanisms without normative elements.

The reference scenario for multicast fast handover is illustrated in Figure 1.

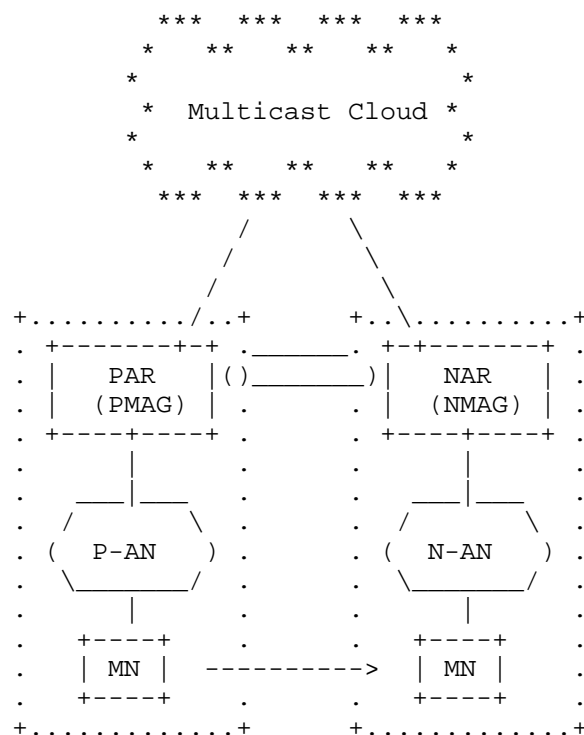


Figure 1: Reference Network for Fast Handover

### 3.1. Multicast Context Transfer between Access Routers

In a fast handover scenario (cf. Figure 1), ARs/MAGs establish a mutual binding and provide the capability to exchange context information concerning the MN. This context transfer will be triggered by detecting the forthcoming movement of an MN to a new AR and assist the MN to immediately resume communication on the new subnet link using its previous IP address. In contrast to unicast, multicast flow reception does not primarily depend on address and binding cache management, but requires distribution trees to adapt so that traffic follows the movement of the MN. This process may be significantly slower than fast handover management [RFC5757]. Multicast listeners at handover may offer the twofold advantage of including the multicast groups under subscription in context transfer. First, the NAR can proactively join the subscribed groups as soon as it gains knowledge of them. Second, multicast flows can be included in traffic forwarding via the tunnel established from PAR to NAR.

There are two modes of operation in FMIPv6 and in PFMIPv6. The

predictive mode allows for AR-binding and context transfer prior to an MN handover, while in the reactive mode, these steps are executed after detection that the MN has re-attached to NAR. Details of the signaling schemes differ between FMIPv6 and PFMIPv6 and are outlined in Section 3.2 and Section 3.3.

In a predictive fast handover, the access router (i.e., PAR (PMAG) in Figure 1) learns about the impending movement of the MN and simultaneously about the multicast group context as specified in Section 3.2 and Section 3.3. Thereafter, the PAR will initiate an AR-binding and context transfer by transmitting a HI message to NAR (NMAG). HI is extended by multicast group states carried in mobility header options as defined in Section 5.3. On reception of the HI message, NAR returns a multicast acknowledgement in its HACK answer that indicates its ability to support each requested group (see Section 5.4). NAR (NMAG) expresses its willingness to receive multicast traffic from forwarding by PAR using standard MLD signaling. There are several reasons to waive forwarding, e.g., the NAR could already have a native subscription for the group(s), or capacity constraints can hinder decapsulation of additional streams. At the previous network, there may be policy of capacity constraints that make it undesirable to forward the multicast traffic. The PAR can add the tunnel interface to its multicast forwarding database for those groups the MN wishes to receive, so that multicast flows can be forwarded in parallel to the unicast traffic. The NAR implements an MLD proxy [RFC4605] providing host-side behaviour on behalf of the upstream PAR. The proxy will submit an MLD report to the upstream tunnel interface to indicate the set of groups to be forwarded. It will terminate multicast forwarding from the tunnel when the group is natively received. In parallel, NAR joins all groups that are not already under subscription using its native multicast upstream interface. While the MN has not arrived at a downstream interface of the NAR, multicast subscriptions on behalf of the MN are associated with Loopback as a downstream interface. Reception of the Join at the NAR enables downstream native multicast forwarding of the subscribed group(s).

In a reactive fast handover, the PAR will learn about the movement of the MN, after the latter has re-associated with the new access network. Also from the new link, it will be informed about the multicast context of the MN. As group membership information are present at the new access network prior to context transfer, MLD join signaling can proceed in parallel to HI/HACK exchange. Following the context transfer, multicast data can be forwarded to the new access network using the PAR-NAR tunnel of the fast handover protocol. Depending on the specific network topology though, multicast traffic for some groups may natively arrive before it is forwarded from PAR.

In both modes of operation, it is the responsibility of the PAR (PMAG) to properly apply multicast state management when an MN leaves. Depending on the link type and MLD parameter settings, methods for observing the departure of an MN need to be applied (cf., [RFC5757]). While considering subscriptions of the remaining nodes and from the tunnel interfaces, the PAR uses normal multicast forwarding rules to determine whether multicast traffic can be pruned.

This method allows an MN to participate in multicast group communication with a handover performance that is comparable to unicast handover.

### 3.2. Protocol Operations Specific to FMIPv6

ARs that provide multicast support in FMIPv6 will advertise this general service by setting an indicator bit (M-bit) in its PrRtAdv message as defined in Section 5.1. Additional details about the multicast service support, e.g., flavors and groups, will be exchanged within HI/HACK dialogs later at handovers.

An MN operating FMIPv6 will actively initiate the handover management by submitting a fast binding update (FBU). The MN, which is aware of the multicast groups it wishes to maintain, will attach mobility options containing its group states (see Section 5.3) to the FBU, and thereby inform ARs about its multicast context. ARs will use these multicast context options for inter-AR context transfer.

In predictive mode, FBU is issued on the previous link and received by PAR as displayed in Figure 2. PAR will extract the multicast context options and append them to its HI message. From the HACK message, PAR will redistribute the multicast acknowledgement by adding the corresponding mobility options to its FBACK message. From receiving FBACK, the MN will learn about a per group multicast support in the new access network. If some groups or a multicast flavour are not supported, it MAY decide on taking actions to compensate the missing service. Note that the proactive multicast context transfer may proceed successfully, even if the MN misses the FBACK message on the previous link.

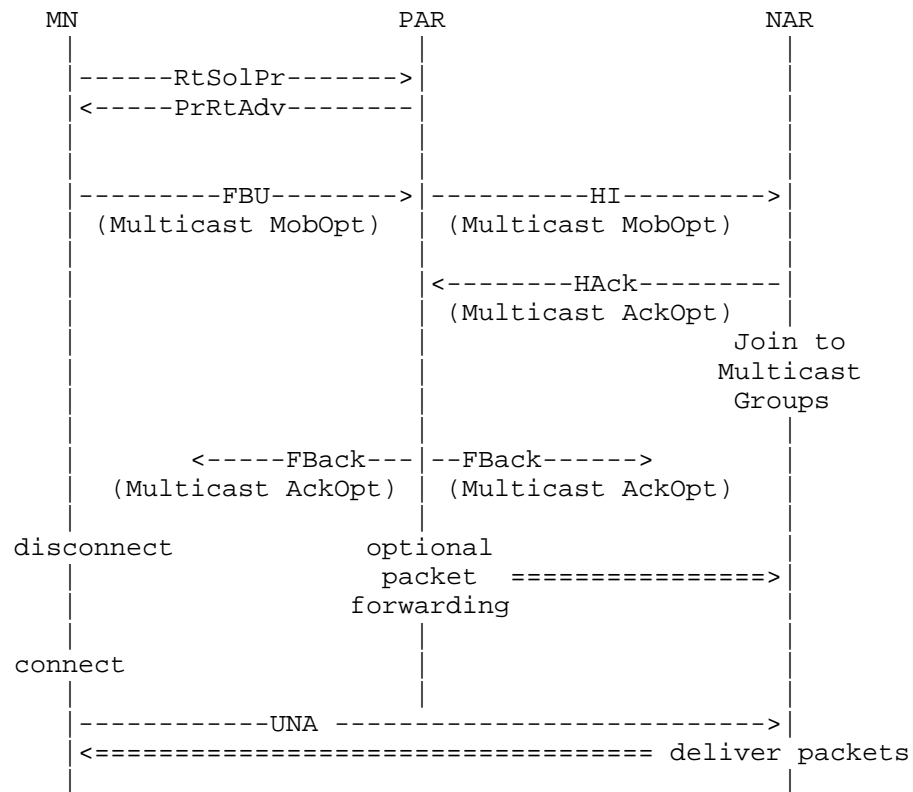


Figure 2: Predictive Multicast Handover for FMIPv6

The call flow for reactive mode is visualized in Figure 3. After attaching to the new access link and performing an unsolicited neighbor advertisement (UNA), the MN issues an FBU which NAR forwards to PAR without processing. At this time, the MN is able to re-join all subscribed multicast groups without relying on AR assistance. Nevertheless, multicast context options are exchanged in the HI/HACK dialog to facilitate intermediate forwarding of requested flows. Note that group traffic possibly already arrives from a MN's subscription at the time NAR receives the HI message. Such multicast flows may be transparently excluded from forwarding by setting an appropriate multicast acknowledge option. In any case, NAR MUST ensure that not more than one flow of the same group is forwarded to the MN.



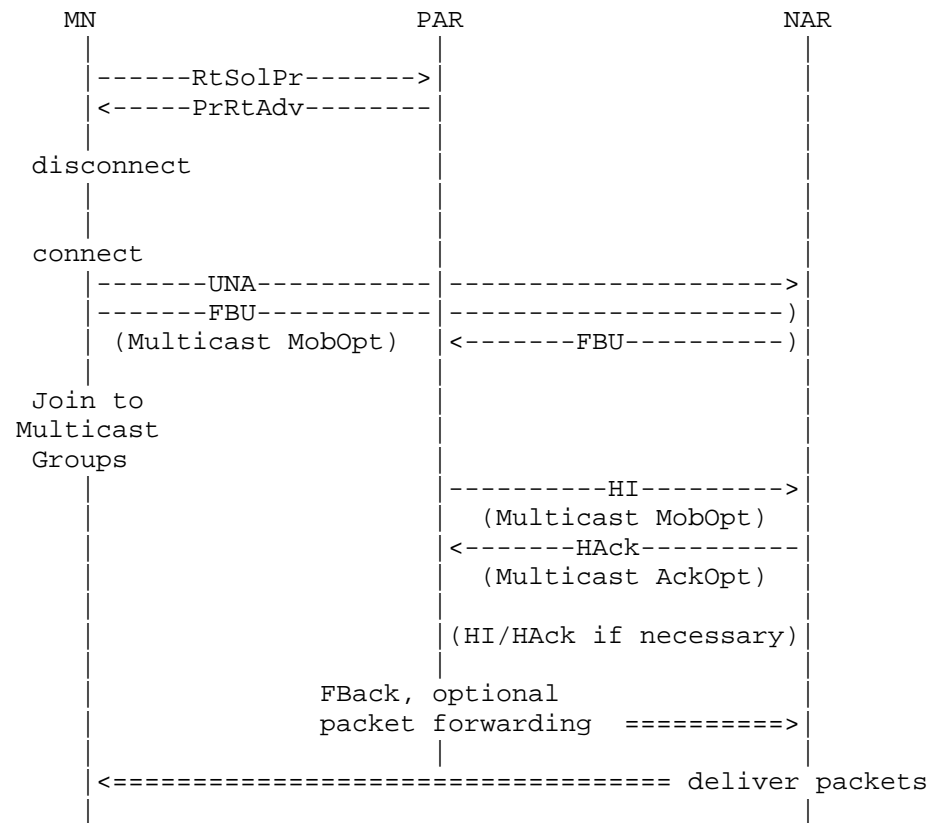


Figure 3: Reactive Multicast Handover for FMIPv6

### 3.3. Protocol Operations Specific to PFMIPv6

In a proxy mobile IPv6 environment, the MN remains agnostic of network layer changes, and fast handover procedures are operated by the access routers or MAGs. The handover initiation, or the re-association respectively are managed by the access networks. Consequently, access routers need to be aware of multicast membership state at the mobile node. There are two ways to obtain record of MN's multicast membership. First, MAGs MAY perform an explicit tracking (cf., [RFC4605], [RFC6224]) or extract membership status from forwarding states at node-specific point-to-point links. Second, routers can perform general queries at handovers. Both methods are equally applicable. However, a router that does not operate explicit tracking MUST query its downstream links subsequent to handovers. In either case, the PAR will become knowledgeable about multicast group subscriptions of the MN.

In predictive mode, the PMAG (PAR) will learn about the upcoming movement of the mobile node. Without explicit tracking, it will immediately submit a general MLD query and learn about the multicast groups under subscription. As displayed in Figure 4, it will initiate binding and context transfer with the NMAG (NAR) by issuing a HI message that is augmented by multicast contexts in the mobility options defined in Section 5.3. NAR will extract multicast context information and act as described in Section 3.1.

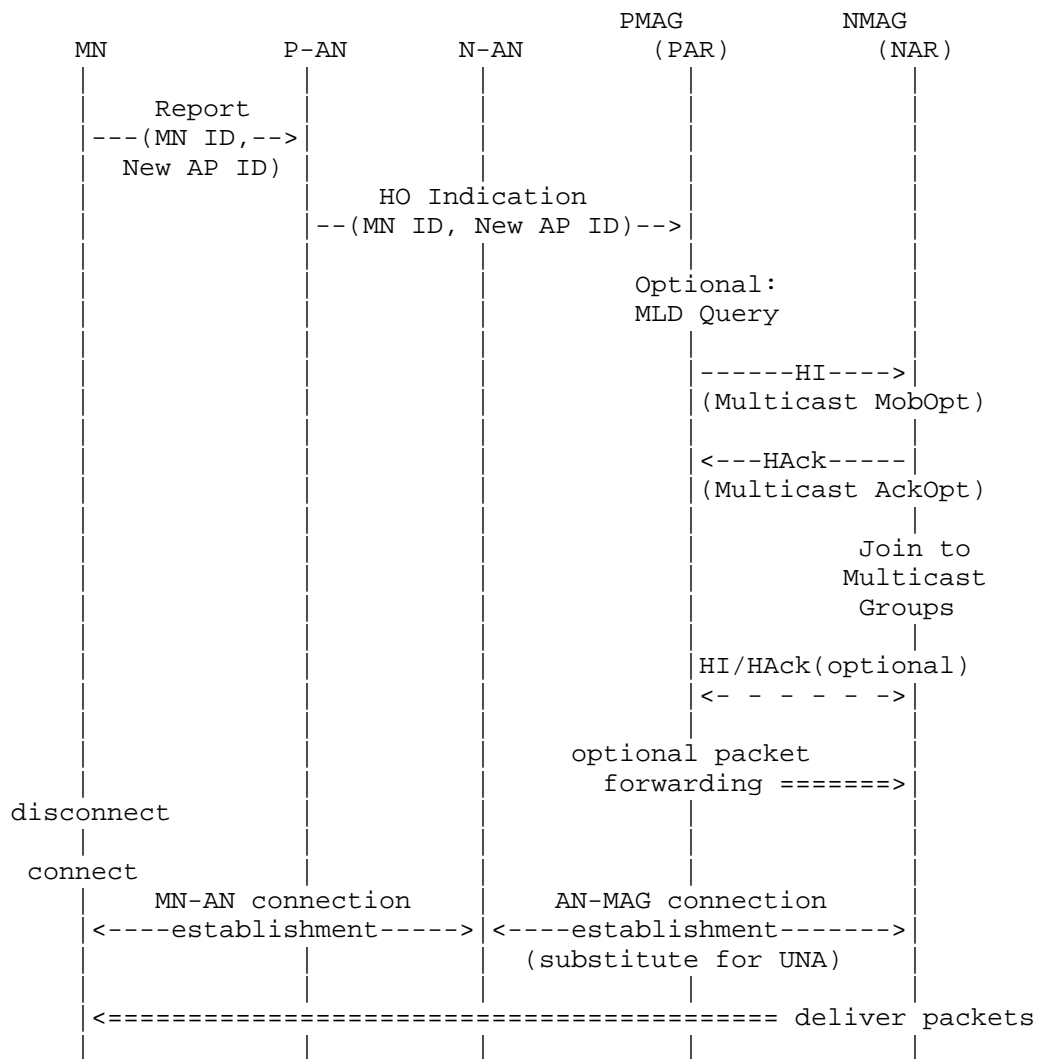


Figure 4: Predictive Multicast Handover for PFMIPv6

In reactive mode, the NMAG (NAR) will learn about MN's attachment to the N-AN and establish connectivity by means of PMIPv6 protocol operations. However, it will have no knowledge about multicast state at the MN. Triggered by a MN attachment, the NMAG will send a general MLD query and thereafter join the requested groups. In the case of a reactive handover, the binding is initiated by NMAG, and the HI/HACK message semantic is inverted (see [RFC5949]). For multicast context transfer, the NMAG attaches to its HI message those group identifiers it requests to be forwarded from PMAG. Using the identical syntax in its multicast mobility option headers as defined in Section 5.4, PMAG acknowledges those requested groups in its HACK answer that it is willing to forward. The corresponding call flow is displayed in Figure 5.

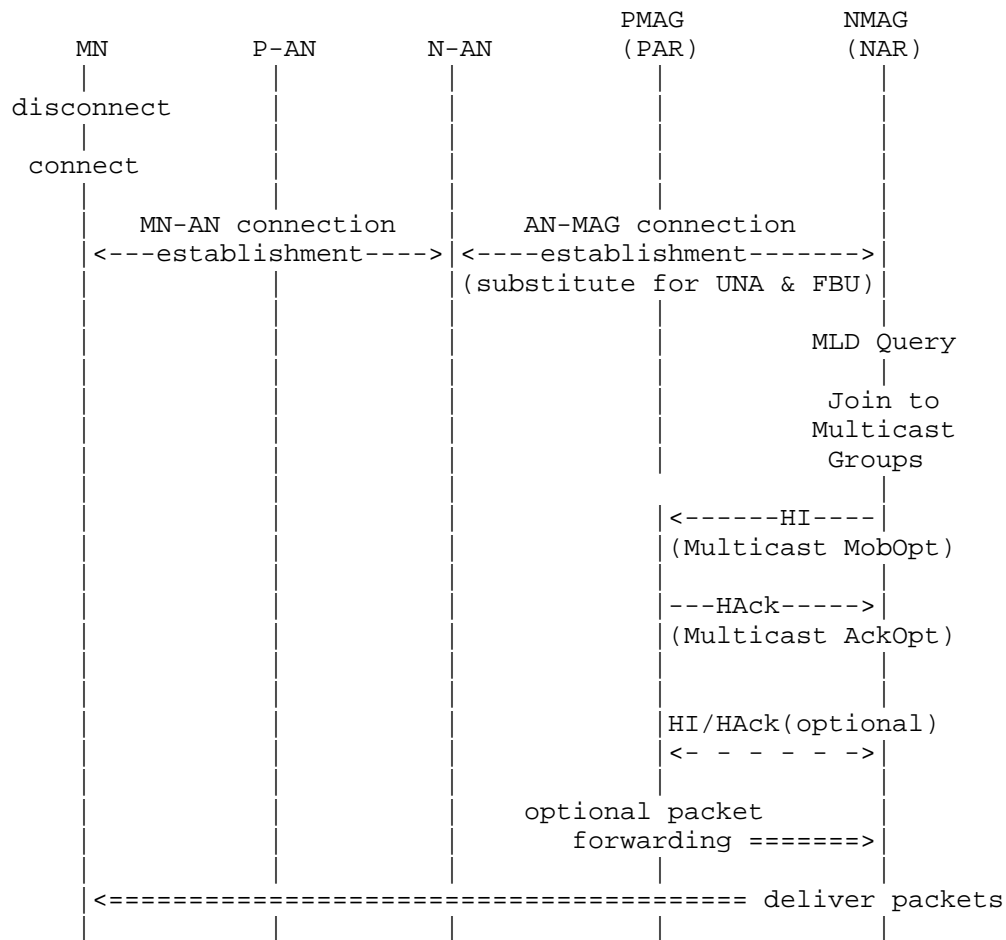


Figure 5: Reactive Multicast Handover for PFMIPv6

#### 4. Protocol Details

##### 4.1. Protocol Operations Specific to FMIPv6

###### 4.1.1. Operations of the Mobile Node

A Mobile Node willing to manage multicast traffic within fast handover operations will inform about its MLD listener state records within handover signaling.

When sensing a handover in predictive mode, an MN will build a

Multicast Mobility Option as described in Section 5.3 that contains the MLD (IGMP) multicast listener state and append it to the Fast Binding Update (FBU) prior to signaling with PAR. It will receive the Multicast Acknowledgement Option(s) as part of Fast Binding Acknowledge (FBack) (see Section 5.4) and learn about unsupported or prohibited groups at the NAR. The MN MAY take appropriate actions like home tunneling to bridge missing multicast services in the new access network. No multicast-specific operation is required by the MN when re-attaching in the new network besides standard FMIPv6 signaling.

In reactive mode, the MN appends an identical Multicast Mobility Option to FBU sent after its reconnect. In response, it will learn about the Multicast Acknowledgement Option(s) from FBACK and expect corresponding multicast data. Concurrently it joins all subscribed multicast groups (channels) directly on its newly established access link.

#### 4.1.2. Operations of the Previous Access Router

A PAR will advertise its multicast support by setting the M-bit in PrRtAdv.

In predictive mode, a PAR will receive the multicast listener state of a MN prior to handover from the Multicast Mobility Option appended to the FBU. It will forward these records to NAR within HI messages and will expect Multicast Acknowledgement Option(s) in HACK, which itself is returned to the MN as an appendix to FBACK. In performing multicast context exchange, the AR is instructed to include the PAR-to-NAR tunnel obtained from unicast handover management in its multicast downstream interfaces and await MLD listener reports from NAR. In response to receiving multicast subscriptions, PAR will normally forward group data acting as a regular multicast router or proxy. However, NAR MAY refuse to forward some or all of the multicast flows.

In reactive mode, PAR will receive the FBU augmented by the Multicast Mobility Option from the new network, but will continue with an identical multicast record exchange in the HI/HACK dialog. As in the predictive case, it will configure the PAR-to-NAR tunnel for multicast downstream and forward data according to MLD reports obtained from NAR, if capable of forwarding.

In both modes, PAR will interpret the first of the two events, the departure of the MN or the reception of the Multicast Acknowledgement Option(s) as a multicast LEAVE message of the MN and react according to the signaling scheme deployed in the access network (i.e., MLD querying, explicit tracking).

#### 4.1.3. Operations of the New Access Router

NAR will advertise its multicast support by setting the M-bit in PrRtAdv.

In predictive mode, a NAR will receive the multicast listener state of an expected MN from the Multicast Mobility Option appended to the HI message. It will extract the MLD/IGMP records from the message and intersect the request subscription with its multicast service offer. Further on it will adjoin the supported groups (channels) to the MLD listener state using loopback as downstream interface. This will lead to suitable regular subscriptions on its native multicast upstream interface without additional forwarding. Concurrently, NAR builds a Multicast Acknowledgement Option(s) (see Section 5.4) listing those groups (channels) unsupported on the new access link and returns them within HACK. As soon as the bidirectional tunnel from PAR to NAR is operational, NAR joins the groups subscribed for forwarding on the tunnel link.

In reactive mode, NAR will learn about the multicast listener state of a new MN from the Multicast Mobility Option appended to HI at a time, when the MN has already performed local subscriptions of the multicast service. Thus NAR solely determines the intersection of requested and supported groups (channels) and issues the join requests for group forwarding on the PAR-NAR tunnel interface.

In both modes, NAR MUST send a LEAVE message to the tunnel immediately after forwarding of a group (channel) becomes unneeded, e.g., after native multicast traffic arrives or group membership of the MN terminates.

#### 4.1.4. Buffering Considerations

Multicast packets may be lost during handover. For example, in predictive mode as illustrated by figure 2, although the NAR can forward the multicast traffic before the MN attaches to it, the multicast packets still will be lost after the MN disconnects from PAR and before it attaches to the NAR. In reactive mode as illustrated by figure 3, the situation may be worse since there will be a delay for joining the multicast group after the MN attaches to the NAR. The multicast packets will be lost during this time. Buffering the multicast packets at the PAR can ease the multicast packet loss problem. It should be noted that many multicast traffic is video/audio which is sensitive to delay, the buffering mechanism at the PAR should be optimized to meet the specific application's delay requirement.

## 4.2. Protocol Operations Specific to PFMIPv6

### 4.2.1. Operations of the Mobile Node

A Mobile Node willing to participate in multicast traffic will join, maintain and leave groups as if located in the fixed Internet. It will cooperate in handover indication as specified in [RFC5949] and required by its access link-layer technology. No multicast-specific mobility actions nor implementations are required at the MN in a PMIPv6 domain.

### 4.2.2. Operations of the Previous MAG

A MAG receiving a handover indication for one of its MNs follows the predictive fast handover mode as a PMAG. It MUST issue an MLD General Query immediately on its corresponding link unless it performs an explicit tracking on that link. After gaining knowledge of the multicast subscriptions of the MN, the PMAG builds a Multicast Mobility Option as described in Section 5.3 that contains the MLD (IGMP) multicast listener state. If not empty, this Mobility Option is appended to the regular fast handover HI messages, or - in the case of unicast HI message being submitted prior to multicast state detection - sent in an additional HI message to the NMAG. PMAG then waits for receiving the Multicast Acknowledgement Option(s) with HACK (see Section 5.4) and the creation of the bidirectional tunnel with NMAG. Thereafter PMAG will add the tunnel to its downstream interfaces in the multicast forwarding database. For those groups (channels) reported in the Multicast Acknowledgement Option(s), i.e., not supported in the new access network, PMAG normally takes appropriate actions (e.g., forwarding, termination) in concordance with the network policy. It SHOULD start forwarding traffic down the tunnel interface for those groups it receives an MLD listener report message from NMAG. However, it MAY deny forwarding service. After the departure of the MN and on the reception of LEAVE messages for groups/channels, PMAG MUST terminate forwarding of the specific groups and update its multicast forwarding database. Correspondingly it issues a group/channel LEAVE to its upstream link, if no more listeners are present on its downstream links.

A MAG receiving a HI message with Multicast Mobility Option for a currently attached node follows the reactive fast handover mode as a PMAG. It will return Multicast Acknowledgement Option(s) (see Section 5.4) within HACK listing those groups/channels unsupported at NMAG. It will add the bidirectional tunnel with NMAG to its downstream interfaces and will start forwarding multicast traffic for those groups it receives an MLD listener report message from NMAG. At the reception of LEAVE messages for groups (channels), PMAG MUST terminate forwarding of the specific groups and update its multicast

forwarding database. According to its multicast forwarding states, it MAY need to issue a group/channel LEAVE to its upstream link, if no more listeners are present on its downstream links.

In both modes, PMAG will interpret the departure of the MN as a multicast LEAVE message of the MN and react according to the signaling scheme deployed in the access network (i.e., MLD querying, explicit tracking).

#### 4.2.3. Operations of the New MAG

A MAG receiving a HI message with Multicast Mobility Option for a currently unattached node follows the predictive fast handover mode as NMAG. It will decide on those multicast groups/channels it wants forwarded from the PMAG and builds a Multicast Acknowledgement Option (see Section 5.4) that enumerates only unwanted groups/channels. This Mobility Option is appended to the regular fast handover HACK messages, or - in the case of unicast HACK message being submitted prior to multicast state acknowledgement - sent in an additional HACK message to the PMAG. Immediately thereafter, NMAG SHOULD update its MLD listener state by the new groups/channels obtained from the Multicast Mobility Option. Until the MN re-attaches, NMAG uses its loopback interface for downstream and does not forward traffic to the potential link of the MN. NMAG SHOULD issue JOIN messages for those newly selected groups to its regular multicast upstream interface. As soon as the bidirectional tunnel with PMAG is established, NMAG additionally joins those groups/channels on the tunnel interface that it wants to receive by forwarding from PMAG. NMAG MUST send a LEAVE message to the tunnel immediately after forwarding of a group/channel becomes unneeded, e.g., after native multicast traffic arrives or group membership of the MN terminates.

A MAG experiencing a connection request for a MN without prior reception of a corresponding Multicast Mobility Option is operating in the reactive fast handover mode as NMAG. Following the re-attachment, it immediately issues an MLD General Query to learn about multicast subscriptions of the newly arrived MN. Using standard multicast operations, NMAG joins the missing groups (channels) on its regular multicast upstream interface. Concurrently, it selects groups (channels) for forwarding from PMAG and builds a Multicast Mobility Option as described in Section 5.3 that contains the MLD (IGMP) multicast listener state. If not empty, this Mobility Option is appended to the regular fast handover HI messages with the F flag set, or - in the case of unicast HI message being submitted prior to multicast state detection - sent in an additional HI message to the PMAG. Upon reception of the Multicast Acknowledgement Option and upcoming of the bidirectional tunnel, NMAG additionally joins those groups/channels on the tunnel interface that it wants to receive by



forwarding from PMAG. When multicast flows arrive, the NMAG forwards data to the appropriate downlink(s). NMAG MUST send a LEAVE message to the tunnel immediately after forwarding of a group/channel becomes unneeded, e.g., after native multicast traffic arrives or group membership of the MN terminates.

#### 4.2.4. IPv4 Support Considerations

An MN in a PMIPv6 domain may use an IPv4 address transparently for communication as specified in [RFC5844]. For this purpose, LMAs can register IPv4-Proxy-CoAs in its Binding Caches and MAGs can provide IPv4 support in access networks. Correspondingly, multicast membership management will be performed by the MN using IGMP. For multiprotocol multicast support on the network side, IGMPv3 router functions are required at both MAGs (see Section 5.6 for compatibility considerations with previous IGMP versions). Context transfer between MAGs can transparently proceed in HI/HACK message exchanges by encapsulating IGMP multicast state records within Multicast Mobility Options (see Section 5.3 and Section 5.4 for details on message formats).

It is worth mentioning the scenarios of a dual-stack IPv4/IPv6 access network, and the use of GRE tunneling as specified in[RFC5845]. Corresponding implications and operations are discussed in the PMIP Multicast Base Deployment document, cf., [RFC6224].

## 5. Message Formats

### 5.1. Multicast Indicator for Proxy Router Advertisement (PrRtAdv)

An FMIPv6 AR will indicate its multicast support by activating the M-bit in its Proxy Router Advertisements (PrRtAdv). The message extension has the following format.

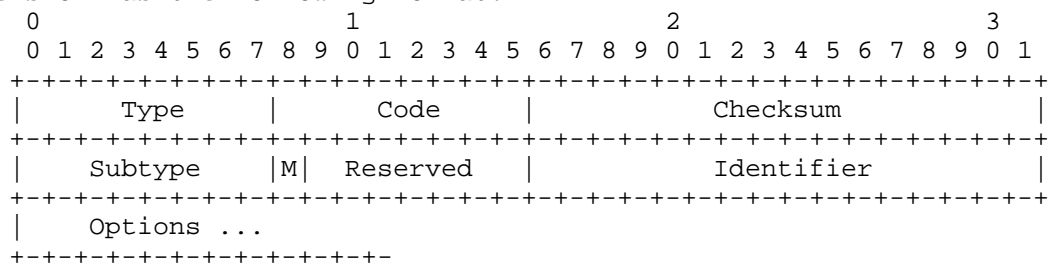


Figure 6: Multicast Indicator Bit for Proxy Router Advertisement (PrRtAdv) Message

## 5.2. Extensions to Existing Mobility Header Messages

The fast handover protocols use a new IPv6 header type called Mobility Header as defined in [RFC3775]. Mobility headers can carry variable Mobility Options.

Multicast listener context of an MN is transferred in fast handover operations from PAR/PMAG to NAR/NMAG within a new Multicast Mobility Option, and acknowledged by a corresponding Acknowledgement Option. Depending on the specific handover scenario and protocol in use, the corresponding option is included within the mobility option list of HI/HACK only (PFMIPv6), or of FBU/FBACK/HI/HACK (FMIPv6).

## 5.3. New Multicast Mobility Option

The Multicast Mobility Option contains the current listener state record of the MN obtained from the MLD Report message, and has the format displayed in Figure 7.

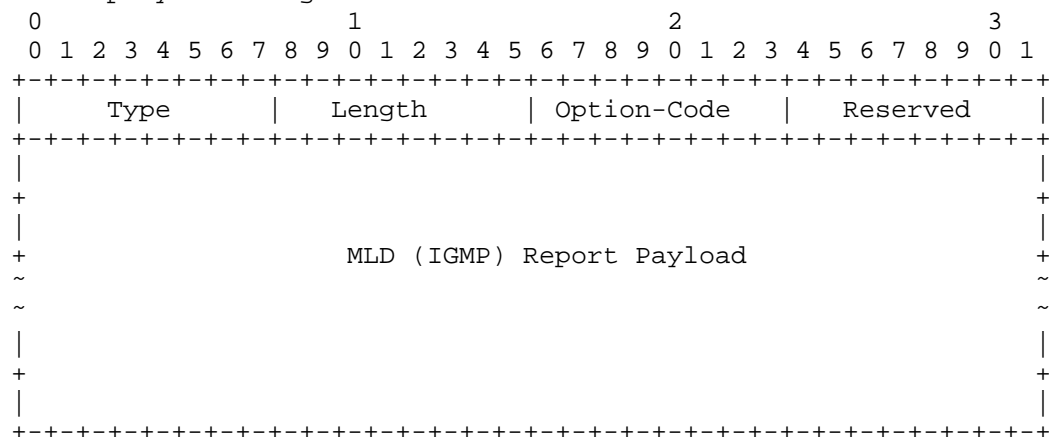


Figure 7: Mobility Header Multicast Option

Type: TBD

Length: 8-bit unsigned integer. The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code:

1: IGMPv3 Payload Type

2: MLDv2 Payload Type

### 3: IGMPv3 Payload Type from IGMPv2 Compatibility Mode

#### 4: MLDv2 Payload Type from MLDv1 Compatibility Mode

Reserved: MUST be set to zero by the sender and MUST be ignored by the receiver.

MLD (IGMP) Report Payload: this field is composed of the MLD (IGMP) Report message after stripping its ICMP header. Corresponding message formats are defined for MLDv2 in [RFC3810], and for IGMPv3 in [RFC3376].

Figure 8 shows the Report Payload for MLDv2, while the payload format for IGMPv3 is defined corresponding to the IGMPv3 payload format (see Section 5.2. of [RFC3810], or Section 4.2 of [RFC3376]) for the definition of Multicast Address Records).

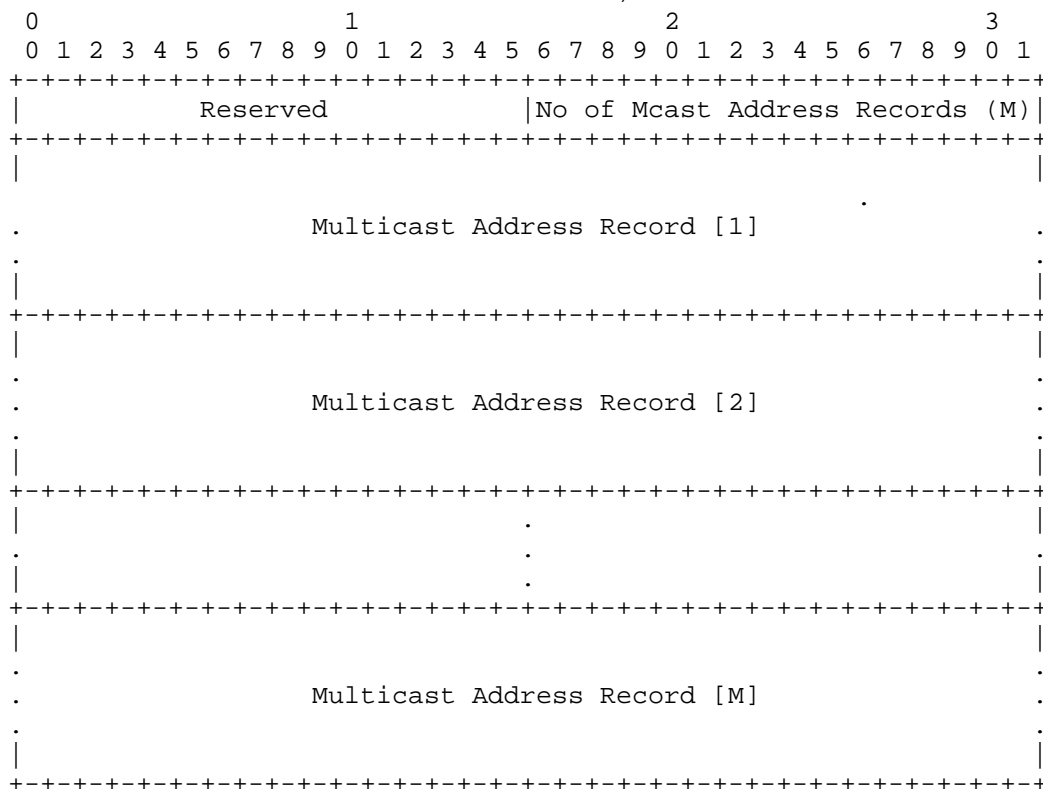


Figure 8: MLDv2 Report Payload

5.4. New Multicast Acknowledgement Option

The Multicast Acknowledgement Option reports the status of the context transfer and contains the list of state records that could not be successfully transferred to the next access network. It has the format displayed in Figure 9.

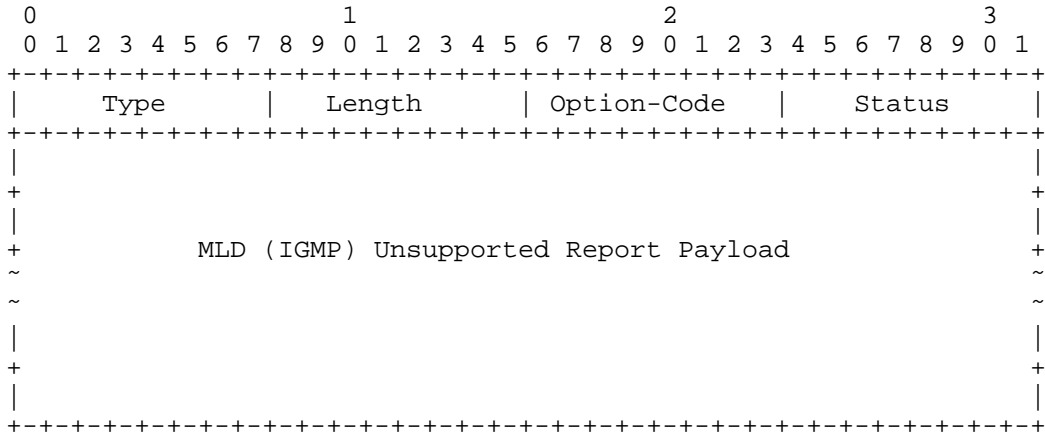


Figure 9: Mobility Header Multicast Acknowledgement Option

Type: TBD

Length: 8-bit unsigned integer. The size of this option is 8 octets. The length is 1 when the MLD (IGMP) Unsupported Report Payload field contains no Mcast Address Record.

Option-Code: 0

Status:

- 1: Report Payload type unsupported
- 2: Requested group service unsupported
- 3: Requested group service administratively prohibited

Reserved: MUST be set to zero by the sender and MUST be ignored by the receiver.

MLD (IGMP) Unsupported Report Payload: this field is syntactically identical to the MLD (IGMP) Report Payload field described in Section 5.3, but is only composed of those multicast address records that are not supported or prohibited in the new access network. This field MUST always contain the first header line (reserved field and

No of Mcast Address Records), but MUST NOT contain any Mcast Address Records, if the status code equals 1.

Note that group subscriptions to specific sources may be rejected at the destination network, and thus the composition of multicast address records may differ from initial requests within an MLD (IGMP) Report Payload option.

#### 5.5. Length Considerations: Number of Records and Addresses

Mobility Header Messages exchanged in HI/HACK and FBU/FBACK dialogs impose length restrictions on multicast context records. The maximal payload length available in FBU/FBACK messages is the PATH-MTU - 40 octets (IPv6 Header) - 6 octets (Mobility Header) - 6 octets (FBU/FBACK Header). For example, on an Ethernet link with an MTU of 1500 octets, not more than 72 Multicast Address Records of minimal length (without source states) may be exchanged in one message pair. In typical handover scenarios, this number reduces further according to unicast context and Binding Authorization data. A larger number of MLD Report Payloads MAY be sent within multiple HI/HACK or FBU/FBACK message pairs. In PFMIPv6, context information can be fragmented over several HI/HACK messages. However, a single MLDv2 Report Payload MUST NOT be fragmented. Hence, for a single Multicast Address Record on an Ethernet link, the number of source addresses is limited to 89.

#### 5.6. MLD (IGMP) Compatibility Aspects

Access routers (MAGs) MUST support MLDv2 (IGMPv3). To enable multicast service for MLDv1 (IGMPv2) listeners, the routers MUST follow the interoperability rules defined in [RFC3810] ([RFC3376]) and appropriately set the Multicast Address Compatibility Mode. When the Multicast Address Compatibility Mode is MLDv1 (IGMPv2), a router internally translates the following MLDv1 (IGMPv2) messages for that multicast address to their MLDv2 (IGMPv2) equivalents and uses these messages in the context transfer. The current state of Compatibility Mode is translated into the code of the Multicast Mobility Option as defined in Section 5.3. A NAR (nMAG) receiving a Multicast Mobility Option during handover will switch to the minimum obtained from its previous and newly learned value of MLD (IGMP) Compatibility Mode for continued operation.

### 6. Security Considerations

Security vulnerabilities that exceed issues discussed in the base protocols of this document ([RFC5568], [RFC5949], [RFC3810], [RFC3376]) are identified as follows.

Multicast context transfer at predictive handovers implements group states at remote access routers and may lead to group subscriptions without further validation of the multicast service requests. Thereby a NAR (nMAG) is requested to cooperate in potentially complex multicast re-routing and may receive large volumes of traffic. Malicious or inadvertent multicast context transfers may result in a significant burden of route establishment and traffic management onto the backbone infrastructure and the access router itself. Rapid re-routing or traffic overload can be mitigated by a rate control at the AR that restricts the frequency of traffic redirects and the total number of subscriptions. In addition, the wireless access network remains protected from multicast data injection until the requesting MN attaches to the new location.

## 7. IANA Considerations

This document defines new flags and status codes in the HI and HACK messages as well as two new mobility options. The Type values for these mobility options are assigned from the same numbering space as allocated for the other mobility options defined in [RFC3775]. Those for the flags and status codes are assigned from the corresponding numbering space defined in [RFC5568], or [RFC5949] and requested to be created as new tables in the IANA registry (marked with asterisks). New values for these registries can be allocated by Standards Action or IESG approval [RFC5226].

## 8. Acknowledgments

Protocol extensions to support multicast in Fast Mobile IPv6 have been loosely discussed since several years. Repeated attempts have been taken to define corresponding protocol extensions. The first draft [fmcast-mip6] was presented by Suh, Kwon, Suh, and Park already in 2004.

This work was stimulated by many fruitful discussions in the MobOpts research group. We would like to thank all active members for constructive thoughts and contributions on the subject of multicast mobility. Comments, discussions and reviewing remarks have been contributed by (in alphabetical order) Carlos J. Bernardos, Luis M. Contreras, Dirk von Hugo, Marco Liebsch, Behcet Sarikaya, Stig Venaas and Juan Carlos Zuniga.

## 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.
- [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5568] Koodli, R., "Mobile IPv6 Fast Handovers", RFC 5568, July 2009.
- [RFC5949] Yokota, H., Chowdhury, K., Koodli, R., Patil, B., and F. Xia, "Fast Handovers for Proxy Mobile IPv6", RFC 5949, September 2010.
- [RFC1112] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, August 1989.
- [RFC4605] Fenner, B., He, H., Haberman, B., and H. Sandick, "Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")", RFC 4605, August 2006.
- [RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.
- [RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.
- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

### 9.2. Informative References

- [RFC5757] Schmidt, T., Waehlich, M., and G. Fairhurst, "Multicast Mobility in Mobile IP Version 6 (MIPv6): Problem Statement and Brief Survey", RFC 5757, February 2010.
- [fmcast-mip6] Suh, K., Kwon, D., Suh, Y., and Y. Park, "Fast Multicast Protocol for Mobile IPv6 in the fast handovers environments", draft-suh-mipshop-fmcast-mip6-00 (work in progress), July 2004.

## [FMIPv6-Analysis]

Schmidt, TC. and M. Waehlich, "Predictive versus Reactive - Analysis of Handover Performance and Its Implications on IPv6 and Multicast Mobility", Telecommunication Systems Vol 33, No. 1-3, pp. 131-154, November 2005.

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

[RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.

[RFC5845] Muhanna, A., Khalil, M., Gundavelli, S., and K. Leung, "Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6", RFC 5845, June 2010.

## Appendix A. Change Log

The following changes have been made from  
draft-ietf-multimob-fmipv6-pfmipv6-multicast-00.

1. Buffering text added from new co-author Dapeng.
2. Several editorial improvements.

The following changes have been made from  
draft-schmidt-multimob-fmipv6-pfmipv6-multicast-04.

1. Following working group feedback, multicast traffic forwarding is now a two-sided option between PAR (PMAG) and NAR (NMAG): Either access router can decide on its contribution to the data plane.
2. Several editorial improvements.

The following changes have been made from  
draft-schmidt-multimob-fmipv6-pfmipv6-multicast-03.

1. References updated.

The following changes have been made from  
draft-schmidt-multimob-fmipv6-pfmipv6-multicast-02.

1. Detailed operations on PFMIPv6 entities completed.
2. Some editorial improvements & clarifications.



### 3. References updated.

The following changes have been made from  
draft-schmidt-multimob-fmipv6-pfmipv6-multicast-01.

1. First detailed operations on PFMIPv6 added.
2. IPv4 support considerations for PFMIPv6 added.
3. Section on length considerations for multicast context records corrected.
4. Many editorial improvements & clarifications.
5. References updated.

The following changes have been made from  
draft-schmidt-multimob-fmipv6-pfmipv6-multicast-00.

1. Editorial improvements & clarifications.
2. Section on length considerations for multicast context records added.
3. Section on MLD/IGMP compatibility aspects added.
4. Security section added.

### Authors' Addresses

Thomas C. Schmidt (editor)  
HAW Hamburg  
Dept. Informatik  
Berliner Tor 7  
Hamburg, D-20099  
Germany

Email: schmidt@informatik.haw-hamburg.de

Matthias Waehlich  
link-lab & FU Berlin  
Hoenower Str. 35  
Berlin D-10318  
Germany

Email: mw@link-lab.net

Rajeev Koodli  
Cisco Systems  
30 International Place  
Xuanwu District,  
Tewksbury MA 01876  
USA

Email: rkoodli@cisco.com

Godred Fairhurst  
University of Aberdeen  
School of Engineering  
Aberdeen AB24 3UE  
UK

Email: gorry@erg.abdn.ac.uk

Dapeng Liu  
China Mobile

Phone: +86-123-456-7890  
Email: liudapeng@chinamobile.com



MULTIMOB Working Group  
Internet-Draft  
Intended status: Experimental  
Expires: August 29, 2013

LM. Contreras  
Telefonica I+D  
CJ. Bernardos  
I. Soto  
UC3M  
February 25, 2013

PMIPv6 multicast handover optimization by the Subscription Information  
Acquisition through the LMA (SIAL)  
draft-ietf-multimob-handover-optimization-02

Abstract

This document specifies a multicast handover optimization mechanism for Proxy Mobile IPv6 to accelerate the delivery of multicast traffic to mobile nodes after handovers. The mechanism is based on speeding up the acquisition of mobile nodes' multicast context by the mobile access gateways. To do that, extensions to the current Proxy Mobile IPv6 protocol are proposed. These extensions are not only applicable to the base solution for multicast support in Proxy Mobile IPv6, but they can also be applied to other solutions being developed to avoid the tunnel convergence problem. Furthermore, they are also independent of the role played by the mobile access gateway within the multicast network (either acting as multicast listener discovery proxy or multicast router).

Status of this Memo

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

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

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

This Internet-Draft will expire on August 29, 2013.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	4
1.1. Handover optimization requirements . . . . .	5
2. Terminology . . . . .	6
3. Overview . . . . .	7
4. PMIPv6 extensions . . . . .	9
4.1. New mobility option . . . . .	9
4.1.1. Active Multicast Subscription mobility option . . . . .	9
4.1.1.1. Option application rules . . . . .	9
4.1.1.2. Option format . . . . .	9
4.1.1.3. Backward compatibility with MLDv1 . . . . .	10
4.2. New flags . . . . .	11
4.2.1. Multicast Signaling flag on PBU/PBA message headers . . . . .	11
4.2.1.1. Flag application rules . . . . .	11
4.2.1.1.1. Registration process . . . . .	11
4.2.1.1.2. De-registration process . . . . .	12
4.2.1.2. New format of conventional PBU/PBA messages . . . . .	13
4.2.1.2.1. Proxy Binding Update message . . . . .	13
4.2.1.2.2. Proxy Binding Acknowledgement Message . . . . .	13
4.2.2. Multicast Active flag in the LMA Binding Cache and (optionally) on the MN's policy store . . . . .	14
4.2.2.1. Flag application rules . . . . .	14
4.3. New messages . . . . .	15
4.3.1. Messages for active multicast subscription query . . . . .	15
4.3.1.1. Subscription Query message . . . . .	15
4.3.1.1.1. Message application rules . . . . .	15
4.3.1.1.2. Message format . . . . .	15
4.3.1.2. Subscription Response message . . . . .	16
4.3.1.2.1. Message application rules . . . . .	16
4.3.1.2.2. Message format . . . . .	16
4.3.2. Messages for active multicast subscription indication . . . . .	17
4.3.2.1. Multicast Activity Indication message . . . . .	18
4.3.2.1.1. Message application rules . . . . .	18
4.3.2.1.2. Message format . . . . .	18
4.3.2.2. Multicast Activity Indication Acknowledge	

message . . . . .	19
4.3.2.2.1. Message application rules . . . . .	19
4.3.2.2.2. Message format . . . . .	19
4.4. New PBA timer in the LMA . . . . .	20
5. Signaling processes description . . . . .	20
5.1. Multicast Activity signaling . . . . .	20
5.1.1. Multicast Activity set to ON (A=1) . . . . .	21
5.1.2. Multicast Activity set to OFF (A=0) . . . . .	22
5.2. Handover signaling procedures . . . . .	23
5.2.1. Handover of proactive type . . . . .	23
5.2.1.1. Rationale . . . . .	23
5.2.1.2. Message flow description . . . . .	23
5.2.2. Handover of reactive type . . . . .	25
5.2.2.1. Rationale . . . . .	25
5.2.2.2. Message flow description . . . . .	26
5.2.2.3. Further considerations for the reactive handover signaling . . . . .	29
5.2.3. LMA decision process . . . . .	30
5.2.3.1. LMA processing of S flag on reception of PBU messages . . . . .	30
5.2.3.1.1. Proactive handover . . . . .	30
5.2.3.1.2. Reactive handover . . . . .	31
5.2.3.2. LMA set-up of S flag in PBA messages . . . . .	32
5.2.4. Prevention of large delays of the binding acknowledgement for unicast traffic . . . . .	33
6. IPv4 support . . . . .	36
6.1. Active Multicast Subscription for IPv4 . . . . .	36
6.2. Signaling procedures for IPv4 support . . . . .	37
6.3. Binding Cache extensions for IPv4 support . . . . .	38
7. Co-existence with PMIPv6 multicast architectural evolutions . . . . .	38
8. Security Considerations . . . . .	38
9. IANA Considerations . . . . .	40
10. Contributors . . . . .	40
11. Acknowledgments . . . . .	40
12. References . . . . .	41
12.1. Normative References . . . . .	41
12.2. Informative References . . . . .	41
Appendix A. Performance comparison with base solution . . . . .	42
A.1. Delay characterization of the base solution . . . . .	43
A.2. Delay characterization of the SIAL solution . . . . .	43
A.3. Performance comparison . . . . .	44
Appendix B. Change Log . . . . .	46
Authors' Addresses . . . . .	47

## 1. Introduction

The base solution describing how continuous multicast service delivery can be provided in Proxy Mobile IPv6 domains is described in [RFC6224]. It specifies the basic functionality needed in the Proxy Mobile IPv6 [RFC5213] entities to provide a multicast service, and supports the continuous delivery of multicast traffic by obtaining, after a handover, the on-going multicast subscription information directly from the mobile node. When a mobile node attaches to a new mobile access gateway, the mobile node is queried by the mobile access gateway through a multicast listener discovery General Query, which is sent just after any new link is set up, to get knowledge of any existing subscription, as specified in [RFC2710].

However, as highlighted by [I-D.von-hugo-multimob-future-work], the base solution needs to be improved to meet some performance requirements, especially those referred to the user perceived service quality, which is seriously affected by the disruption of multicast content forwarding to the mobile node during handovers.

A mobile node with an active multicast subscription, moving from one point of attachment to another within a Proxy Mobile IPv6 domain, experiences a certain delay until it resumes receiving again the multicast content that it was receiving at the previous location. Such delay causes a gap in the content reception. Two different actions can help to mitigate such reception gap. One of them is to buffer at the previous mobile access gateway the traffic with destination at the mobile node and forward it to the new mobile access gateway, in order to deliver that traffic to the mobile node. The other possible (complementary) action is to reduce the time needed by the new mobile access gateway to get knowledge of the active multicast subscription of the mobile node (i.e., the multicast context), so the new mobile access gateway can subscribe to the multicast group(s) on behalf of the mobile node as soon as possible.

While the first mechanism could potentially be accomplished by using some adaptation of [RFC5949] to multicast traffic (despite being only applicable in the case the underlying radio access technology supports layer-2 triggers, thus requiring additional support on the mobile node), there is no generic standard solution for the accelerated acquisition of the on-going multicast subscription of the mobile node.

The approach followed by the base solution [RFC6224] to get knowledge of an existing multicast subscription relies on the behavior of the IGMP/MLD protocols. Both protocols send multicast membership query messages when a new link is up. The response to such a message reports any existing multicast subscription by the mobile node.

While this is a straightforward approach, it also causes that the mobile access gateway can incur in a non-negligible delay in receiving the corresponding MLD Report message. This delay is caused by the time needed for the detection of the attachment in the new link and the re-establishment of the data plane after the handover, the radio transfer delays associated with the signaling to the mobile node, and the MLD query response interval time required by this procedure (whose default value is 10 seconds as defined in [RFC2710], or between 5 and 10 seconds as considered in the best case wireless link scenario in [RFC6636]).

This document extends the Proxy Mobile IPv6 signaling protocol defined in the base protocol [RFC5213] by including a new multicast information option to update Proxy Mobile IPv6 entities during the registration and de-registration processes, and new messages to trigger the transfer of multicast information. No extension is required in any of the multicast-related protocols in use (IGMP/MLD or PIM protocols). Furthermore, this specification does not substitute the standard procedures defined in [RFC6224] (e.g., the mobile access gateway will continue sending an MLD Query to the entering MN as soon as the point-to-point link is set up), but complements them for accelerating the acquisition of the multicast content by the mobile access gateway of the new point-of-attachment.

This document provides a signaling method internal to the network to speed up the subscription information acquisition by the mobile access gateway, in order to accelerate the multicast delivery to the mobile node after having completed a handover. By doing so, the knowledge by the mobile access gateway of the currently active multicast subscription becomes independent of the underlying radio technology dynamics and relaxes the requirement of a rapid response from the mobile node in processing MLD control messages. Issues like radio framing, radio access contention, channel reliability, MN's capabilities (i.e., layer-2 triggering support), IGMP/MLD timers optimization for wireless environments, etc, will not impact on the observed multicast performance during handovers.

The solution described in this document can also be applied to the solutions described in [I-D.ietf-multimob-pmipv6-ropt]. Furthermore, it is also independent of the role played by the mobile access gateway within the multicast network (either acting as MLD proxy or multicast router).

### 1.1. Handover optimization requirements

A basic solution for providing support of multicast in a network-based mobility management environment has been specified in [RFC6224] without introducing changes on the original PMIPv6 specification



[RFC5213]. The focus of this specification is on improving the efficiency of the base solution regarding handover performance.

One of the critical aspects of the base solution is the expected delay in which the nMAG is informed about the on-going multicast subscription of the entering MN, mainly due to the fact that the mechanisms provided in the base solution rely on the original MLD procedures, with long timing interactions not conceived for mobile environments. Then, the requirements to be covered by a handover optimization solution can be established in the following manner:

- o The solution has to be applicable to any kind of MN, in such a way that any type of MN in a PMIPv6 domain being served with multicast traffic can benefit from the optimized solution.
- o The solution should be integrated as part of the PMIPv6 suite of protocols to ensure a smooth introduction of the new functionality in the network.
- o The solution does not have impact on existing multicast protocols.
- o The solution should optimize the handover performance respect to the performance achieved with the base solution for any kind of handover process (i.e., for proactive and reactive handovers).
- o The solution should minimize the number and extent of additional support required in the network, aiming at an easier deployment.

The present specification addresses all these requirements, as described in the following sections.

## 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [RFC2119].

This document uses the terminology referring to PMIPv6 components as defined in [RFC5213].

Additionally, the following terms are defined.

pMAG: The previous MAG or pMAG is the MAG where the MN is initially registered in a handover event.

nMAG: The new MAG or nMAG is the MAG where the MN is registered at the end of the handover event.

Reactive Handover: A reactive handover is a handover event in which the LMA receives the MN registration from the nMAG without having previously received the MN de-registration from the pMAG.

Proactive handover: A proactive handover is a handover event where the MN is firstly de-registered on the LMA by the pMAG, and later on it is registered by the nMAG as consequence of changing the point of attachment.

Multicast Membership Context: Along this document, multicast membership context makes reference to the information relative to the currently active multicast subscription of a MN in a handover event which is transferred between the PMIPv6 entities to support the handover optimization.

### 3. Overview

The LMA is a key element within the PMIPv6 infrastructure, which traces the MN reachability along the PMIPv6 domain. Therefore the LMA is the best element to maintain the MNs' multicast subscription information updated and to forward it to the rest of PMIPv6 entities (i.e., to the MAGs) as needed when MNs move within the domain. The LMA has timely knowledge of the MNs' location, especially during handover events, and it is therefore able to quickly provide information to the new one point of attachment (querying the previous one if required). Figure 1 shows this idea.

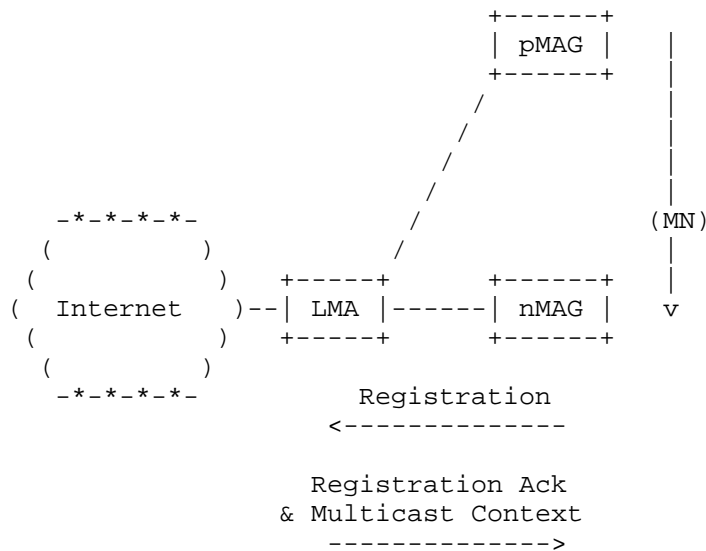


Figure 1: High level solution description

The LMA only obtains the detailed subscription information or multicast context during a handover event. There is no need of continuously informing the LMA about MNs' multicast state while the mobile nodes remain attached to the same mobile access gateway. Such a continuous updating procedure would significantly increase the signaling load within the PMIPv6 domain without a clear benefit. The multicast context is only critical during handovers, neither after nor before. Indicating the active subscription while the handover is ongoing guarantees that such information will be up-to-date, ready to be transferred to the new MAG where the MN has just attached. However it should be noted that some signaling is needed to differentiate what MNs are maintaining active subscriptions in order to restrict the optimization procedure to them in case of handover.

To be able to transfer the multicast subscription information between PMIPv6 entities during a handover, this document extends the PMIPv6 protocol in several ways. First of all, a new mobility option is defined to carry the multicast context of the current subscription. Furthermore, additional messages are defined to manage the interchange of the multicast information among PMIPv6 entities. Finally, some flags are defined to govern the process.

Next sections provide the details of these Proxy Mobile IPv6 protocol extensions.

#### 4. PMIPv6 extensions

This section outlines the extensions proposed to the PMIPv6 protocol specified in [RFC5213].

##### 4.1. New mobility option

###### 4.1.1. Active Multicast Subscription mobility option

###### 4.1.1.1. Option application rules

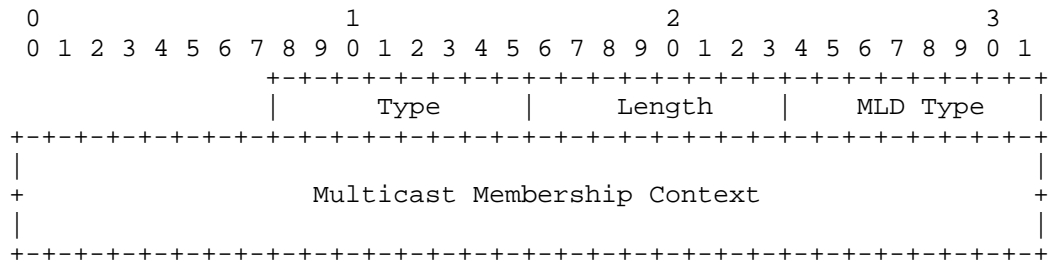
A new TLV-encoded mobility option, "Active Multicast Subscription" option is defined for use with the PBU (Proxy Binding Update) and PBA (Proxy Binding Acknowledge) messages exchanged between an LMA and a MAG to transfer the multicast subscription information. This option is used for exchanging the multicast membership context. This information is carried by using directly the format defined in the original MLD specifications. There can be multiple "Active Multicast Subscription" options present in the message, one for each active subscription maintained by the MN when the handover is taking place (i.e., one per multicast membership context).

This new option will be also used, with the same aim, by the new message Subscription Response described later in this document.

MLDv2 is the primary objective for the definition of the option format. MLDv1 is also considered for backward compatibility.

###### 4.1.1.2. Option format

The format of this new option is as follows:



The alignment requirement of this option is  $8n+1$ .

Type:

To be defined by IANA, for indication of an IPv6 Active Multicast Subscription option.

Length:

8-bit unsigned integer indicating the length of the option in octets, excluding the type and length fields.

MLD type:

Field used to identify the IPv6 multicast membership protocol in use, and the corresponding format of the next Multicast Membership Context information field. This field maps the type codification used in the original MLD specifications for the Report message. For MLDv2, the MLD Type value is 0x143.

Multicast Membership Context:

Multicast subscription information corresponding to a single subscribed multicast address. For MLDv2, the format of this field follows the Multicast Address Record format as defined in [RFC3810].

#### 4.1.1.3. Backward compatibility with MLDv1

The following values are adopted when MLDv1 is used.

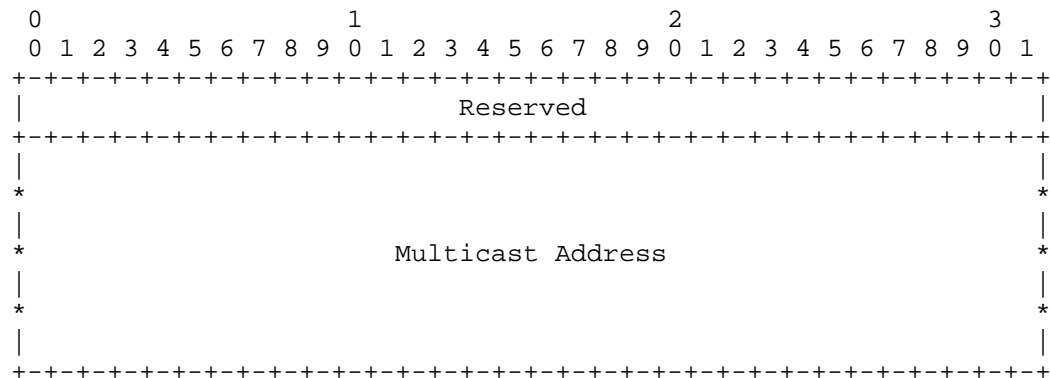
MLD type:

For MLDv1, the MLD Type value is 0x131.

Multicast Membership Context:

For MLDv1, the relevant information for multicast context is simply given, according to [RFC2710], by the multicast address of the subscribed content.

In consequence, the Multicast Membership Context is defined as a 4-octet reserved field and the Multicast Address of the subscribed content as in [RFC2710], in the following manner:



## 4.2. New flags

Two new flags are defined and used to handle the forwarding of multicast subscription information.

#### 4.2.1. Multicast Signaling flag on PBU/PBA message headers

#### 4.2.1.1. Flag application rules

A new flag S is added in both PBU and PBA message headers to advise about the MAG and the LMA capabilities of processing multicast-related signaling for the MN that caused the message.

This flag will govern the multicast-related signaling between the LMA and the MAG. As a general rule, the value of the flag in the PBA message SHOULD be a copy of the value received in the PBU message. Specific rules are described in next sub-sections.

#### 4.2.1.1.1. Registration process

During handover, the entities involved in this process are the nMAG and the LMA. These rules also apply for the Initial Binding registration process.

- o PBU message

- * S=0, it indicates that the MAG sending the PBU message does not accept multicast-related signaling for the MN being attached. This can be used to discriminate PMIPv6 nodes which are not multicast enabled, for backward compatibility reasons.
- * S=1, it indicates that the MAG sending the PBU message accepts multicast-related signaling for the MN being attached. Depending on the type of handover (reactive or proactive) the

- * S=1, it indicates that the MAG sending the PBU message accepts multicast-related signaling for the MN being attached. Depending on the type of handover (reactive or proactive) the

LMA will take some actions, described later in this document.

- o PBA message
  - * If S=0 in the corresponding PBU message, the value of the flag in the PBA message SHOULD be a copy of the value received in the PBU message (thus S=0), without any further meaning.
  - * If S=1 in the corresponding PBU message, two sub-cases can happen
    - + S=1 and "Active Multicast Subscription" mobility option in the PBA message. When the MN maintains an active multicast session, if the LMA is able to provide the multicast subscription information during registration, the PBA message will include the "Active Multicast Subscription" mobility option. If the LMA is not able to provide such information during registration, the PBA message will not include the "Active Multicast Subscription" mobility option. This case is useful to decouple unicast and multicast signaling for an MN being registered at nMAG. A way for obtaining later active multicast-subscription information is described later in this document.
    - + S=0 in the PBA message if the MN does not maintain an active multicast subscription (note that for backward compatibility reasons an LMA not supporting multicast related signaling would always send S=0).

#### 4.2.1.1.2. De-registration process

During handover, the entities involved in this process are the pMAG and the LMA. These rules apply for the Binding De-registration process

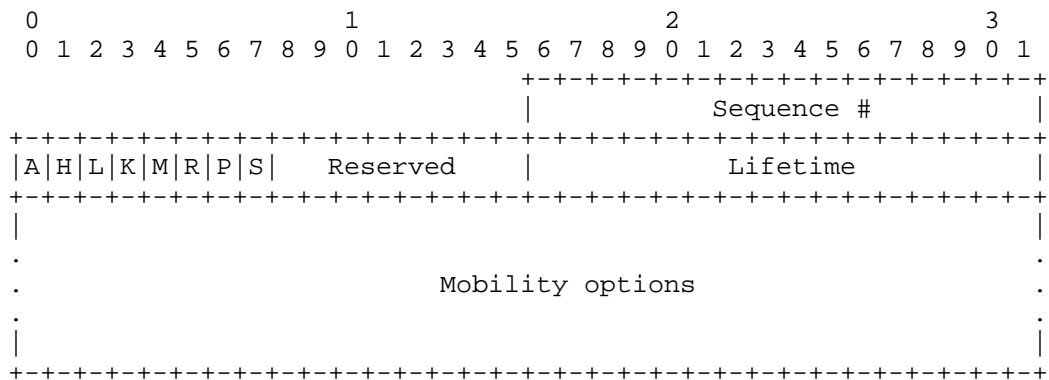
- o PBU message
  - * S=0, it indicates that the MN has no active multicast session (note that for backward compatibility reasons a pMAG not supporting multicast related signaling would always send S=0).
  - * S=1, it indicates that the MN has an active multicast session, and the multicast context is transported in the "Active Multicast Subscription" mobility option.
- o PBA message

- * The value of the flag in the PBA message SHOULD be 0, without any further meaning (note that for backward compatibility reasons an LMA not supporting multicast related signaling would always send S=0).

#### 4.2.1.2. New format of conventional PBU/PBA messages

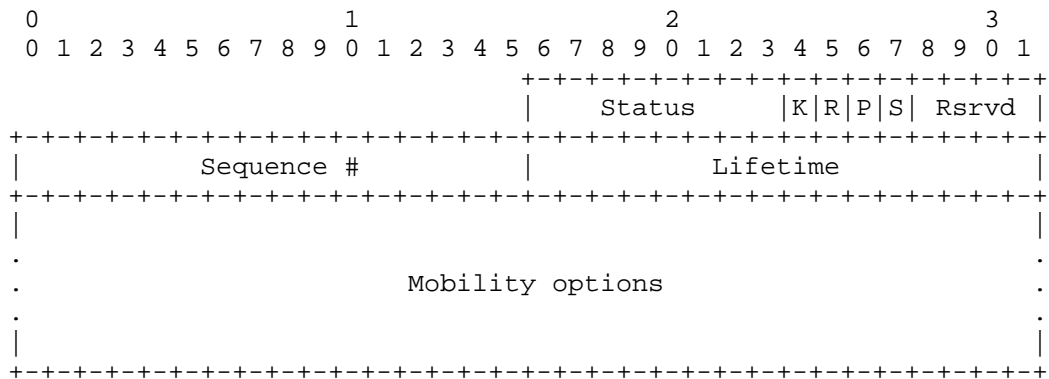
##### 4.2.1.2.1. Proxy Binding Update message

As result of the new defined flag, the PBU message results as follows:



##### 4.2.1.2.2. Proxy Binding Acknowledgement Message

As result of the new defined flag, the PBA message results as follows:





#### 4.2.2. Multicast Active flag in the LMA Binding Cache and (optionally) on the MN's policy store

##### 4.2.2.1. Flag application rules

A new flag A is added in the LMA Binding Cache to retain the knowledge that the registered MN maintains or not an active multicast subscription. The basic use of this flag is to restrict the query of the pMAG only to the cases in which the MN certainly is maintaining an active subscription. The algorithm which is followed by the LMA to query or not the pMAG (after receiving a PBU message from the nMAG) is as follows:

- o Flag S=0 & flag A=0: this situation represents the case where the nMAG does not support multicast-related signaling for the MN being registered, and, additionally, the LMA is not aware of any active multicast subscription on-going. Then, the LMA does not query the pMAG, and registers the MN as attached to the nMAG as usual.
- o Flag S=0 & flag A=1: this situation represents the case where the nMAG does not support multicast-related signaling for the MN being registered, but the LMA is aware of one or more on-going MN's active multicast subscriptions. Due to the fact that multicast signaling is not supported by the nMAG for that MN, the LMA does not query the pMAG, and registers the MN as attached to the nMAG as usual.
- o Flag S=1 & flag A=0: this situation represents the case where the nMAG supports multicast-related signaling for the MN being registered, but the LMA is not aware of any active multicast subscription. Then, the LMA does not query the pMAG, and registers the MN as attached to the nMAG as usual.
- o Flag S=1 & flag A=1: this situation represents the case where the nMAG supports multicast-related signaling for the MN being registered, and, additionally, the LMA is aware of one or more on-going MN's active multicast subscriptions. Then, the LMA queries the pMAG to obtain the multicast context details previously to complete the registration of the MN attached to the nMAG.

The flag A SHOULD be initialized to the value 0.

Optionally, this flag can be also added to the MN's policy store, and dynamically updated by the LMA to signal that the MN has (or not) an active multicast subscription. By introducing this flag in the MN's policy profile, the nMAG can know in advance the existence of an active multicast session by the incoming MN.

#### 4.3. New messages

##### 4.3.1. Messages for active multicast subscription query

A new pair of messages is defined for interrogating entities about the active multicast subscription of the MN when the handover is of reactive type.

These messages are sent using the Mobility Header as defined in [RFC6275].

###### 4.3.1.1. Subscription Query message

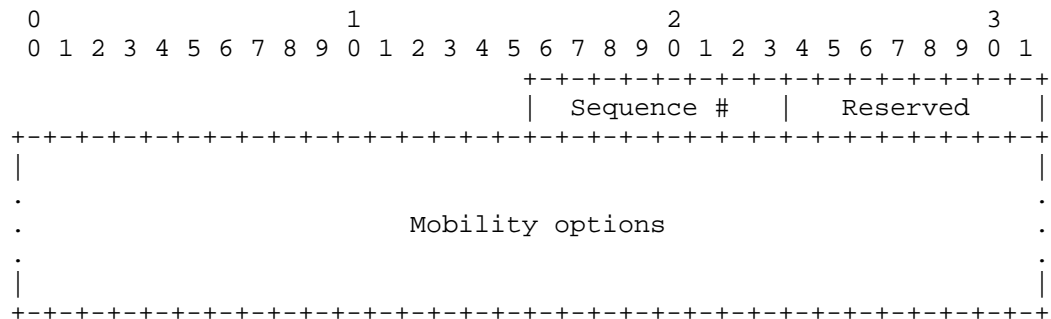
###### 4.3.1.1.1. Message application rules

The Subscription Query message is sent by the LMA towards the pMAG to query it about any existing multicast subscription of the MN which is being registered by the nMAG. This message is generated in case that the handover is of reactive type.

Additionally, this message is sent by the nMAG towards the LMA to query it about the existing multicast subscription of the MN when the LMA acknowledges the PBU sent by the nMAG but the multicast context is not provided (in detail, when the PBU messages has set the flag S to 1, and the PBA message has set the flag S to 1 but the multicast context is missing).

###### 4.3.1.1.2. Message format

The Subscription Query message has the following format.



Sequence Number:

The Sequence Number field establishes the order of the messages sent in the Subscription Query / Subscription Response dialogue between the LMA and the MAG for a certain MN. The initial

Sequence Number will be determined by the entity which creates the message (either LMA or MAG, depending on the scenario), which will be responsible of managing this counter.

Reserved:

This field is unused for now. The value MUST be initialized to 0.

Mobility options:

This message will carry one or more TLV-encoded mobility options. The valid mobility options for this message are the following:

- * Mobile Node Identifier option (mandatory)
- * Home Network Prefix option (optional)

There can be one or more instances of the Home Network Prefix option, but only one instance of the Mobile Node Identifier option.

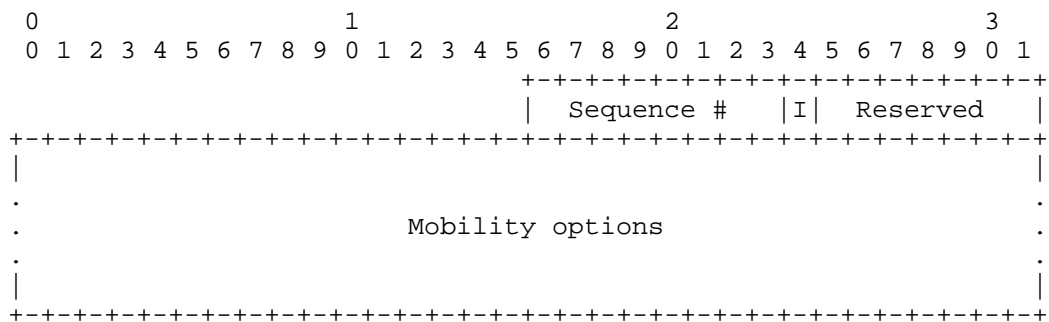
#### 4.3.1.2. Subscription Response message

##### 4.3.1.2.1. Message application rules

The Subscription Response message is sent by the pMAG towards the LMA, or by the LMA towards the nMAG, to answer a previously received Subscription Query message, as described above.

##### 4.3.1.2.2. Message format

The Subscription Response message has the following format.



Sequence Number:

The value of the Sequence Number field in the Subscriber Response message MUST be a copy of the Sequence Number received in the Subscription Query message.

Multicast Information (I):

The multicast Information flag I specifies if there is multicast subscription information available for the MN or not. The meaning is the following:

I=0: there is no multicast subscription information available for the MN identified by the Mobile Node Identifier option in this message.

I=1: there is multicast subscription information available for the MN identified by the Mobile Node Identifier option in this message. The multicast subscription information is carried on one or more instances of the Active Multicast Subscription option in this message (one instance for each active subscription).

Reserved:

This field is unused for now. The value MUST be initialized to 0.

Mobility options:

This message will carry one or more TLV-encoded mobility options. The valid mobility options for this message are the following:

- * Mobile Node Identifier option (mandatory)
- * Active Multicast Subscription option (mandatory) only when flag I=1, not present in any other case
- * Home Network Prefix option (optional)

There can be one or more instances of the Home Network Prefix option (in all cases) and the Active Multicast Subscription option (only when I=1), but only one instance of the Mobile Node Identifier option.

4.3.2. Messages for active multicast subscription indication

A new pair of messages is defined for setting up and down the optional A flag defined above.

These messages are sent using the Mobility Header as defined in

[RFC6275].

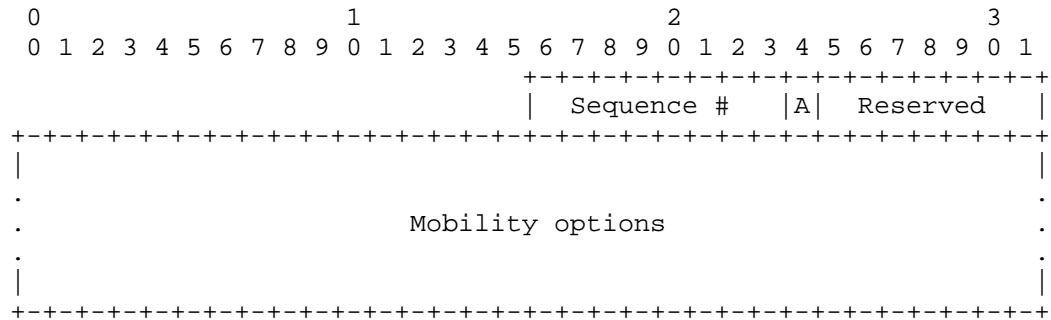
#### 4.3.2.1. Multicast Activity Indication message

##### 4.3.2.1.1. Message application rules

The Multicast Activity Indication message is sent by a MAG towards the LMA to set to 1 or 0 the A flag either to indicate the start or the complete cease of any multicast subscription by the MN. Through the use of this message, the LMA becomes aware that one or more multicast flows are being forwarded to a MN. This information is useful for the LMA during a handover to discriminate if the pMAG needs to be asked or not about multicast information corresponding to the MN being registered at the nMAG, in case that the handover is of reactive type.

##### 4.3.2.1.2. Message format

The Multicast Activity Indication message has the following format.



##### Sequence Number:

The Sequence Number field establishes the order of the messages sent in the Activity Indication / Activity Indication Ack dialogue between the MAG and the LMA for a certain MN. The initial Sequence Number will be determined by the MAG, which will be responsible of managing this counter.

##### Activity indicator (A):

The Activity indicator flag A specifies if the MN multicast activity is on, that is, if the MN maintains one or more active multicast subscriptions at the MAG. The meaning is the following:

A=0: the multicast activity of the MN (identified by the Mobile Node Identifier option in this message) is OFF.

A=1: the multicast activity of the MN (identified by the Mobile Node Identifier option in this message) is ON.

Reserved:

This field is unused for now. The value MUST be initialized to 0.

Mobility options:

This message will carry one or more TLV-encoded mobility options. The valid mobility options for this message are the following:

- * Mobile Node Identifier option (mandatory)
- * Home Network Prefix option (optional)

There can be one or more instances of the Home Network Prefix option, but only one instance of the Mobile Node Identifier option.

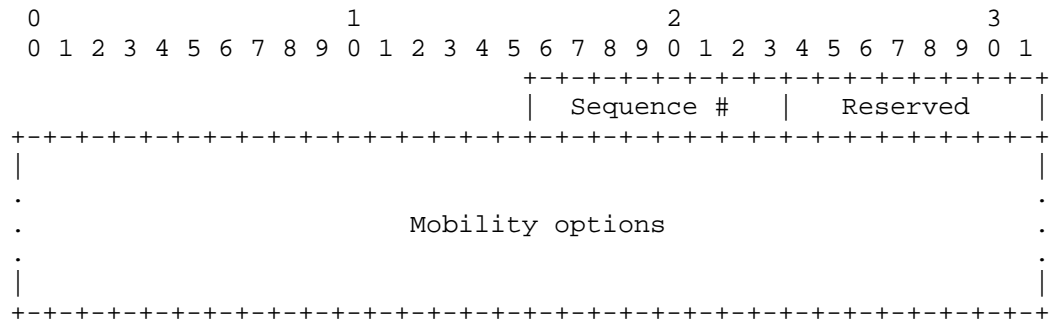
#### 4.3.2.2. Multicast Activity Indication Acknowledge message

##### 4.3.2.2.1. Message application rules

The Multicast Activity Indication Acknowledge message is sent by the LMA towards a MAG to confirm the reception of a previously sent Multicast Activity Indication message.

##### 4.3.2.2.2. Message format

The Multicast Activity Indication message has the following format.



Sequence Number:

The value of the Sequence Number field in the Activity Indication Ack message MUST be a copy of the Sequence Number received in the

Activity Indication message.

Reserved:

This field is unused for now. The value MUST be initialized to 0.

Mobility options:

This message will carry one or more TLV-encoded mobility options. The valid mobility options for this message are the following:

- * Mobile Node Identifier option (mandatory)
- * Home Network Prefix option (optional)

There can be one or more instances of the Home Network Prefix option, but only one instance of the Mobile Node Identifier option.

#### 4.4. New PBA timer in the LMA

A new timer named "PBA timer" is used in the LMA to define the maximum waiting time before the PBA message is sent to the nMAG in case the multicast subscription information relative to the MN is not yet available. The aim of this timer is to prevent potential large delays in the forwarding of unicast traffic towards the MN being registered at the nMAG. This timer allows decoupling the unicast signaling from the multicast one.

This timer SHOULD be upper bounded by the constant defined in [RFC6275] INIT_BINDACK_TIMEOUT, whose default value is 1 s. This constant sets the time when the nMAG will retry the MN registration by sending again the PBU message. The "PBA timer" has to ensure that the nMAG does not enter the retry mode.

### 5. Signaling processes description

A number of new signaling processes are introduced with this solution. Next sections describe these new processes in detail.

#### 5.1. Multicast Activity signaling

This solution makes use of the flag A to keep track of existing multicast activity in a certain MN. The idea behind this is to define a mechanism which helps the LMA to decide whether to query or not the pMAG about potential subscription information.

This signaling message is used to allow the LMA to distinguish among MNs with on-going multicast subscription, and MN without active multicast status. This differentiation further allows to apply the optimization procedure only to those MNs with active multicast subscription (no actions are taken for MN without active multicast subscription).

#### 5.1.1. Multicast Activity set to ON (A=1)

Figure 2 summarizes this process.

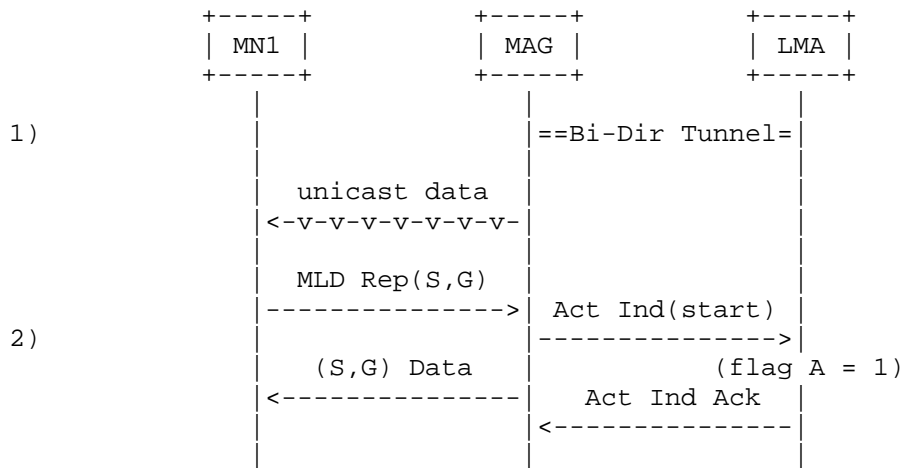


Figure 2: Multicast Activity set to ON

The sequence of messages is the following:

1. An MN, named MN1, is attached to the MAG. The MN is a multicast-enabled node, and it is only receiving unicast traffic as usual in PMIPv6 domains, with no multicast subscription yet. At some point in time, the MN1 requests to the MAG to be subscribed to the content identified by the IP addresses (S,G), by sending a standard MLD report from the MN to the MAG. The MAG will keep the multicast status state of the point-to-point link with the MN. In case the MAG has not already subscribed to the multicast flow (S,G) it joins the content on behalf of MN. Multicast flow (S,G) is subsequently forwarded by the MAG to the MN1.
2. Due to this initial multicast subscription for the MN1, the MAG triggers the multicast Activity Indication message towards the LMA, to indicate that the MN1 multicast activity is ON. The LMA will set the flag A to 1. Afterwards, the LMA sends an Activity Indication Ack message to the MAG to acknowledge the previous



indication.

#### 5.1.2. Multicast Activity set to OFF (A=0)

Figure 3 presents the corresponding flow.

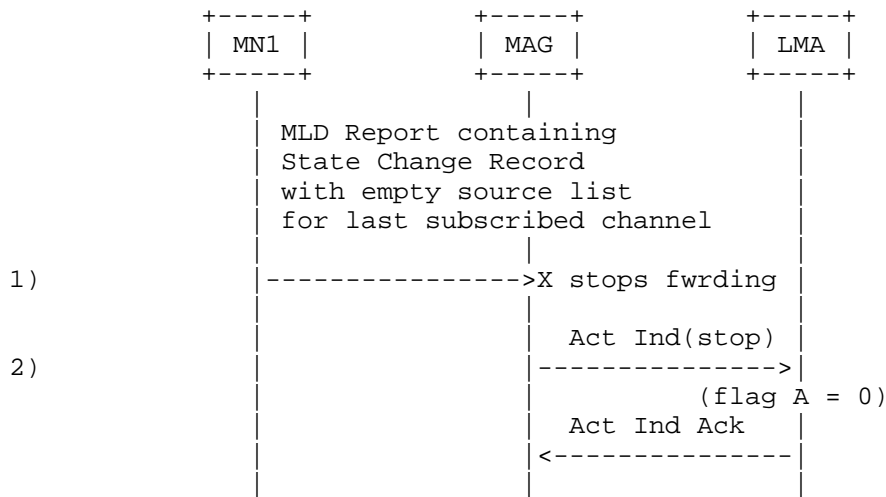


Figure 3: Multicast Activity set to OFF

The message flow is as follows:

1. Some time later, the MN1 decides to totally stop all the active multicast subscriptions that it maintains. The MN1 will send an MLD Report message (containing an State Change Record for the last subscribed multicast group with a filter change record mode indicating INCLUDE mode and an empty source list) to the MAG to request the cease of the multicast traffic delivery. As a consequence, the MAG will stop all the multicast traffic forwarding to the MN1.
2. After removing the active subscriptions for the MN1, the MAG sends a multicast Activity Indication message to the LMA indicating that the MN1 multicast activity is OFF. The LMA will set the flag A to 0, its default value. Afterwards, the LMA sends an Activity Indication Ack message to the MAG to acknowledge the previous indication.

## 5.2. Handover signaling procedures

As the MN moves from one access gateway to another, the mobility-related signaling due to the handover event is carried out independently by the pMAG and the nMAG. That signaling process is not synchronized and, thus, two scenarios need to be considered depending on the order in which the LMA receives notification of the MN registration and de-registration in the nMAG and the pMAG respectively.

### 5.2.1. Handover of proactive type

#### 5.2.1.1. Rationale

In the proactive case, the MN is firstly de-registered by the pMAG, and later on it is registered by the nMAG as consequence of changing the point of attachment.

Only for those MNs which maintain an active multicast subscription, the pMAG will include, as part of the PBU message (with flag S set to 1), the new TLV-encoded mobility option "Active Multicast Subscription" carrying the multicast context of the MN at that moment.

The LMA will store that information in the corresponding binding cache. If, later on, the MN attaches to a nMAG, this information will be sent (using the same TLV option) to the nMAG as part of the PBA confirmation of the registration process (the PBU message sent by the nMAG SHOULD set the flag S to 1). On the other hand, if no further registration happens, the multicast information will be removed together with the rest of binding database for that MN.

After receiving the multicast context, the nMAG can subscribe to the multicast flow(s) on behalf of the MN if there is no other MN receiving it already at the nMAG. The multicast status can be also set in advance for the point-to-point link towards the MN.

Note that the solution described here does not prevent benefiting from extended support in the mobile node/network that facilitates the proactive mode operation of the solution, e.g., based on layer-2 capabilities.

#### 5.2.1.2. Message flow description

Figure 4 summarizes this process.

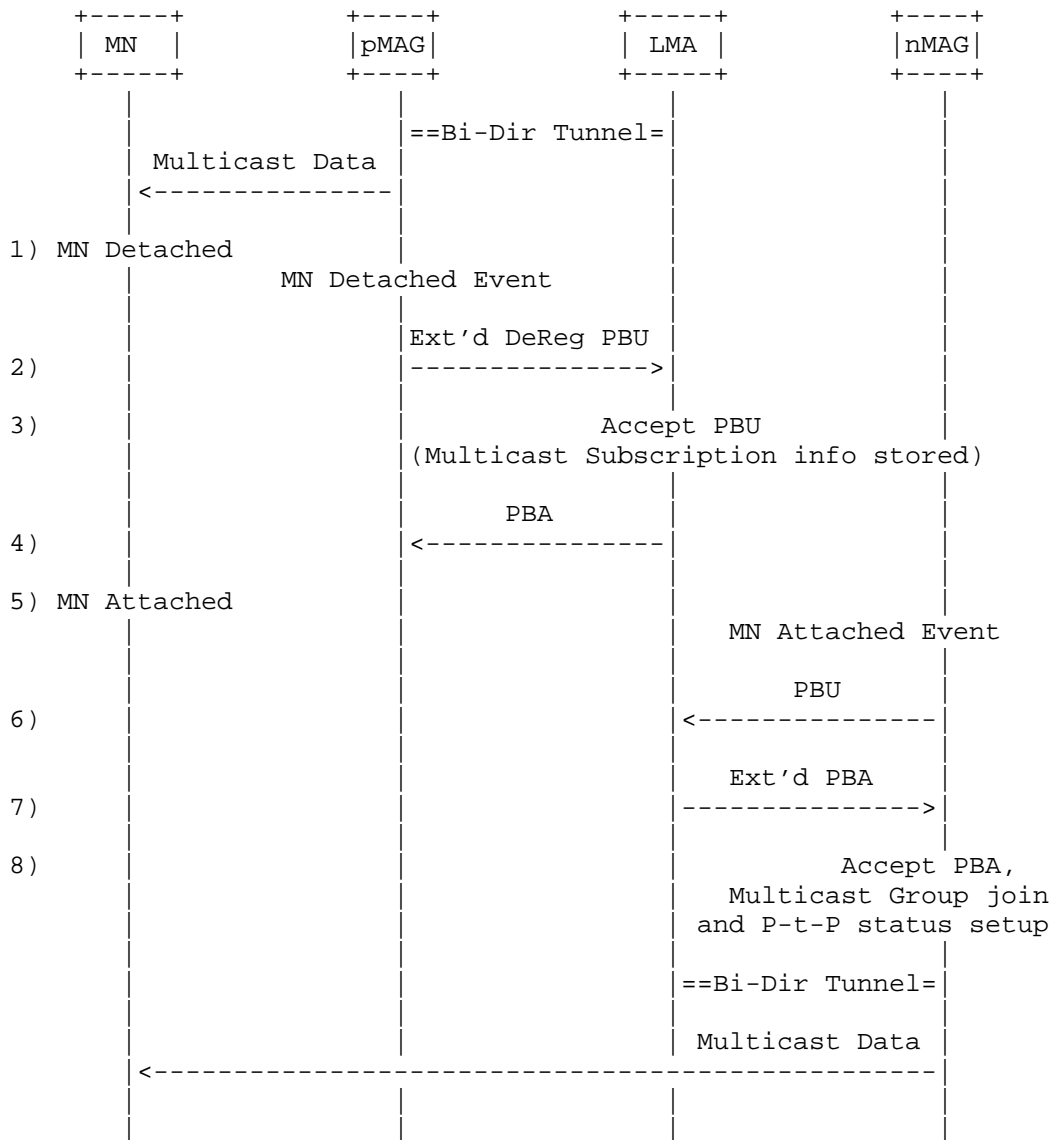


Figure 4: Proactive handover

The message flow is as follows:

1. A registered MN is receiving a multicast content which has been previously subscribed to by sending a standard MLD report from the MN to the currently serving MAG, pMAG. The pMAG keeps the multicast status state of the point-to-point link with the MN.

2. The MN perceives a better radio link and decides to initiate a handover process over a radio access controlled by a new MAG, nMAG. As a consequence, pMAG determines a detach event corresponding to this MN, and updates the attachment status of this MN to the LMA by sending an extended Proxy Binding Update message, including a new TLV-encoded option, named "Active Multicast Subscription", which contains the multicast context of the active multicast subscriptions in the moment of handover.
3. The LMA processes the PBU message. Additionally, the LMA stores in the Binding Cache the information regarding the on-going multicast subscription(s) when the detachment is initiated. This information will be kept until a new registration of the MN is completed by another MAG, or till the Binding Cache expiration, according to [RFC5213].
4. The LMA acknowledges to the pMAG the previous PBU message.
5. As a result of the handover process, the MN attaches to another MAG, called nMAG.
6. The nMAG triggers a registration process by sending a PBU message (with flag S set to 1) to the LMA.
7. After the analysis of the PBU message, the LMA sends an extended PBA including the new "Active Multicast Subscription" option, which contains the multicast context of the active subscriptions in the moment of handover.
8. The nMAG processes the PBA message following all the standard procedures described in [RFC5213]. Additionally, with the new information relative to multicast subscription, the nMAG will set up the multicast status of the point-to-point link between the nMAG and the MN, and will join the content identified by (S,G) on behalf of the MN in case the nMAG is not receiving already such content due to a previous subscription ordered by another MN attached to it. From that instant, the multicast content is served to the MN.

#### 5.2.2. Handover of reactive type

##### 5.2.2.1. Rationale

In the reactive case, the LMA receives the MN registration from the nMAG without having previously received the MN de-registration from the pMAG.

As the nMAG is not aware of any active multicast subscription of the

MN, the nMAG will start a conventional registration process, by sending a normal PBU message (with flag S set to 1) towards the LMA.

After receiving the PBU message from the nMAG, the LMA will take the decision of interrogating or not the pMAG regarding any existing multicast subscription for that MN. This decision is taken following a procedure that is described later in section Section 5.2.3.

Once the multicast subscription information is retrieved from the pMAG, the LMA encapsulates it in the PBA message by using the TLV option "Active Multicast Subscription", and forwards the PBA message to the nMAG. Then, the nMAG can subscribe the multicast flow on behalf of the MN, if there is no other MN receiving it already at the nMAG. The multicast status can be also set in advance for the point-to-point link towards the MN.

#### 5.2.2.2. Message flow description

Figure 5 and Figure 6 summarize this process.

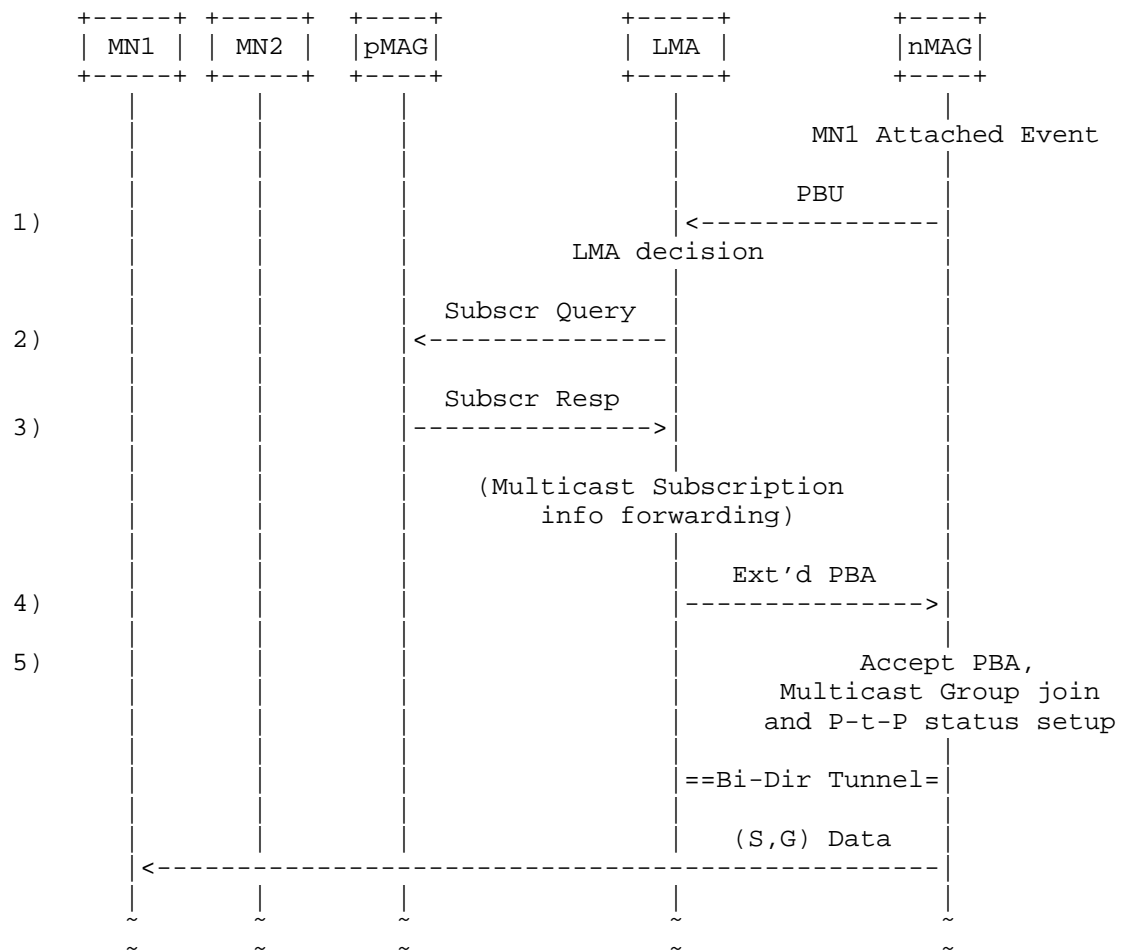


Figure 5: Reactive handover (steps 1 to 5)

Consider as starting point the situation where a couple of MNs, named MN1 and MN2, are attached to the pMAG, both MNs being multicast-enabled nodes, but only MN1 maintains an active multicast subscription at this moment. As consequence, the value of the A flag in the LMA is set to 1 for MN1, and set to 0 for MN2.

The sequence of messages for the handover of MN1 and MN2 is the following (as depicted in Figure 5):

1. At certain time, the MN1 perceives a better radio link and decides to attach at a new MAG, nMAG, in a handover process (as it is a reactive case, the pMAG is not aware of the detachment process). Then, the nMAG triggers a registration process by sending a PBU message (with flag S set to 1) to the LMA.
2. Prior to acknowledge the received PBU message, the LMA checks the status of the A flag for this MN. Due that the flag A=1, the LMA queries the pMAG about if there is any active multicast subscription for the MN1, by sending a Subscription Query message.
3. The pMAG answers the LMA with a Subscription Response message including the multicast context of the existing subscriptions.
4. After processing the pMAG answer, the LMA acknowledges (with flag S set to 1) the PBU message, including the multicast subscription information within the new TLV-encoded option "Active Multicast Subscription". The nMAG then processes the extended PBA message.
5. The nMAG processes the PBA message, and it proceeds to set up the multicast status of the point-to-point link between the nMAG and the MN1, and to join the content identified by (S,G) on behalf of the MN1 in case the nMAG is not receiving already such content. (The bidirectional tunnel is also set up between the nMAG and the LMA if it has not been established before by another MN connection). At this moment, the multicast content can be served to the MN1. The unicast traffic for the MN1 can be forwarded as well.

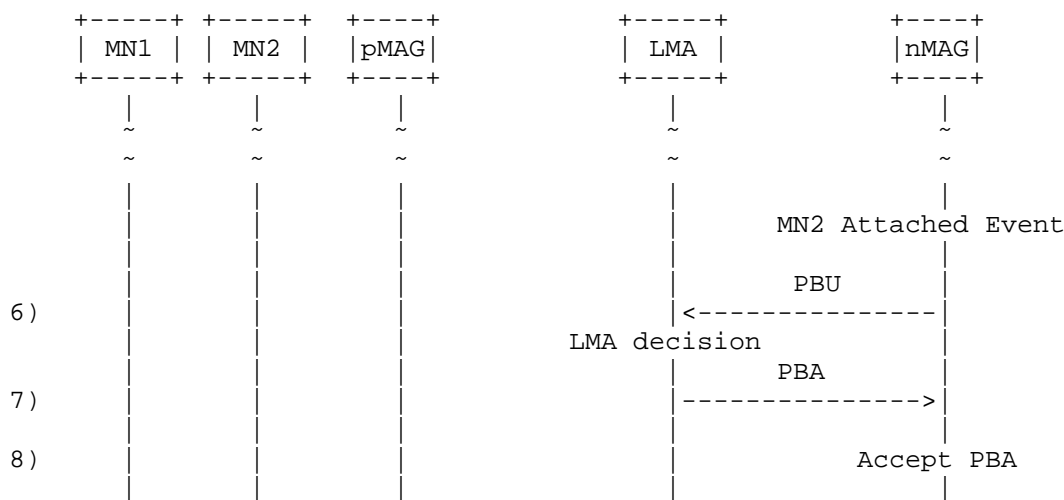


Figure 6: Reactive handover (steps 6 to 8)

6. In parallel, the MN2 perceives a better radio link and decides to attach also to the nMAG in a reactive handover process as well (the pMAG is not aware of this detachment process either). Then, the nMAG triggers a registration process by sending a PBU message (with flag S set to 1) to the LMA.

7. Prior to acknowledge the received PBU message, the LMA checks the status of the A flag for this MN. Due that the flag A=0, the LMA does not query the pMAG, and acknowledges the PBU message (with flag S set to 0). The nMAG then processes PBA message.

8. The nMAG is now ready to forward the unicast traffic to the MN2.

#### 5.2.2.3. Further considerations for the reactive handover signaling

A handover event is managed independently by the pMAG and nMAG. It is not a synchronized process. In a reactive handover, the LMA will receive a registration PBU from nMAG before a de-registration PBU from pMAG, if any.

In the message flows detailed above, it could be the case that the LMA receives a de-registration PBU from pMAG just after sending the Subscription Query message, but before receiving the Subscription Response message. That de-registration PBU message from pMAG will carry the multicast subscription information required to assist the MN in the handover, so such valuable information SHOULD be kept by the LMA. Furthermore, it is possible that once the Subscription Query message arrives to pMAG, the pMAG could have already removed



the multicast related information for the MN.

In order to avoid losing the multicast subscription information sent in the de-registration PBU message, the LMA SHOULD store it, and include it in the PBA message towards the nMAG in case the Subscription Response message from the pMAG does not contain multicast subscription information for the MN.

#### 5.2.3. LMA decision process

A key point of the solution proposed in this document resides on the LMA decision of interrogating the pMAG about a potential active subscription of the MN entering the nMAG. Several variables take place, and it is required to define a mechanism for assisting the LMA in its decision process.

Basically two flags will be used. One flag, the named "multicast Signaling" or S flag, is used to signal the multicast capabilities of the MAGs and the transport of the multicast subscription information within the PBU/PBA messages. The other one, the named "multicast Activity" or A flag, is used to register on the LMA whether the MN is maintaining an active multicast subscription or not.

The following sections summarize the use of these flags on the LMA decision process.

##### 5.2.3.1. LMA processing of S flag on reception of PBU messages

###### 5.2.3.1.1. Proactive handover

In the event of proactive handover, the pMAG has previously informed the LMA about any potential subscription information currently active in the MN. The actions to be carried out by the LMA once it receives the PBU message from the nMAG are summarized in the table below.

multicast signaling flag S in PBU	multicast activity flag A in LMA	Meaning	LMA action
S=0	A=0	<ul style="list-style-type: none"> <li>- Multicast not supported by nMAG</li> <li>- No active subscription by MN</li> </ul>	<ul style="list-style-type: none"> <li>- MN registration as in RFC 5213 (S=0 in PBA)</li> </ul>
	A=1	<ul style="list-style-type: none"> <li>- Multicast not supported by nMAG</li> <li>- Active subscription by MN</li> </ul>	<ul style="list-style-type: none"> <li>- LMA stores multicast subscription info</li> <li>- MN registration as in RFC 5213 (S=0 in PBA)</li> </ul>
S=1	A=0	<ul style="list-style-type: none"> <li>- Multicast supported by nMAG</li> <li>- No active subscription by MN</li> </ul>	<ul style="list-style-type: none"> <li>- MN registration as in RFC 5213 (S=0 in PBA)</li> </ul>
	A=1	<ul style="list-style-type: none"> <li>- Multicast supported by nMAG</li> <li>- Active subscription by MN</li> </ul>	<ul style="list-style-type: none"> <li>- LMA stores multicast subscription info</li> <li>- MN registration conveys multicast subscription info (S=1 in PBA)</li> </ul>

Figure 7: Flag processing on LMA for proactive handover

## 5.2.3.1.2. Reactive handover

In the event of reactive handover, the LMA is not aware about any potential subscription information currently active in the MN. The actions to be carried out by the LMA once it receives the PBU message from the nMAG are summarized in the table below.

multicast signaling flag S in PBU	multicast activity flag A in LMA	Meaning	LMA action
S=0	A=0	<ul style="list-style-type: none"> <li>- Multicast not supported by nMAG</li> <li>- No active subscription by MN</li> </ul>	<ul style="list-style-type: none"> <li>- MN registration as in RFC 5213 (S=0 in PBA)</li> </ul>
	A=1	<ul style="list-style-type: none"> <li>- Multicast not supported by nMAG</li> <li>- Active subscription by MN</li> </ul>	<ul style="list-style-type: none"> <li>- LMA does not query pMAG</li> <li>- MN registration as in RFC 5213 (S=0 in PBA)</li> </ul>
S=1	A=0	<ul style="list-style-type: none"> <li>- Multicast supported by nMAG</li> <li>- No active subscription by MN</li> </ul>	<ul style="list-style-type: none"> <li>- LMA does not query pMAG</li> <li>- MN registration as in RFC 5213 (S=0 in PBA)</li> </ul>
	A=1	<ul style="list-style-type: none"> <li>- Multicast supported by nMAG</li> <li>- Active subscription by MN</li> </ul>	<ul style="list-style-type: none"> <li>- LMA queries pMAG to obtain multicast subscription</li> <li>- MN registration conveys multicast subscription info (S=1 in PBA)</li> </ul>

Figure 8: Flag processing on LMA for reactive handover

## 5.2.3.2. LMA set-up of S flag in PBA messages

Once the LMA decision process is finished, the LMA builds the PBA message to complete the registration process triggered by the nMAG. The value of the S flag in the PBA message will be set according to the data specified in the table below.

S flag received in PBU message	S flag sent in PBA message	Meaning
S=0  (multicast not supported by nMAG)	S=0	No further meaning
	S=1	N/A
S=1 (multicast is supported by nMAG)	S=0	No active subscription on MN
	S=1	<ul style="list-style-type: none"> <li>- Mcast context available: Multicast subscription info is conveyed in the PBA message</li> <li>- Mcast context not available: It has to be requested by using the Subscription Query message.</li> </ul>

Figure 9: S flag configuration in PBA messages

#### 5.2.4. Prevention of large delays of the binding acknowledgement for unicast traffic

According to the message sequences described for the reactive handover case, in case the LMA has to request the multicast subscription information from the pMAG, the binding request sent by the nMAG is maintained on-hold till the LMA receives, processes and includes the multicast subscription information into the extended PBA message. As consequence, the unicast traffic may then suffer an extra delay motivated by the multicast-related signaling. During that time, the unicast traffic with destination the MN being registered by the nMAG MUST be buffered or discarded by the LMA.

In order to avoid any potential large delay in the forwarding of unicast traffic arriving at the LMA towards the MN, a mechanism SHOULD be implemented to decouple multicast from unicast traffic reception by the MN.

Figure 10 shows this mechanism:

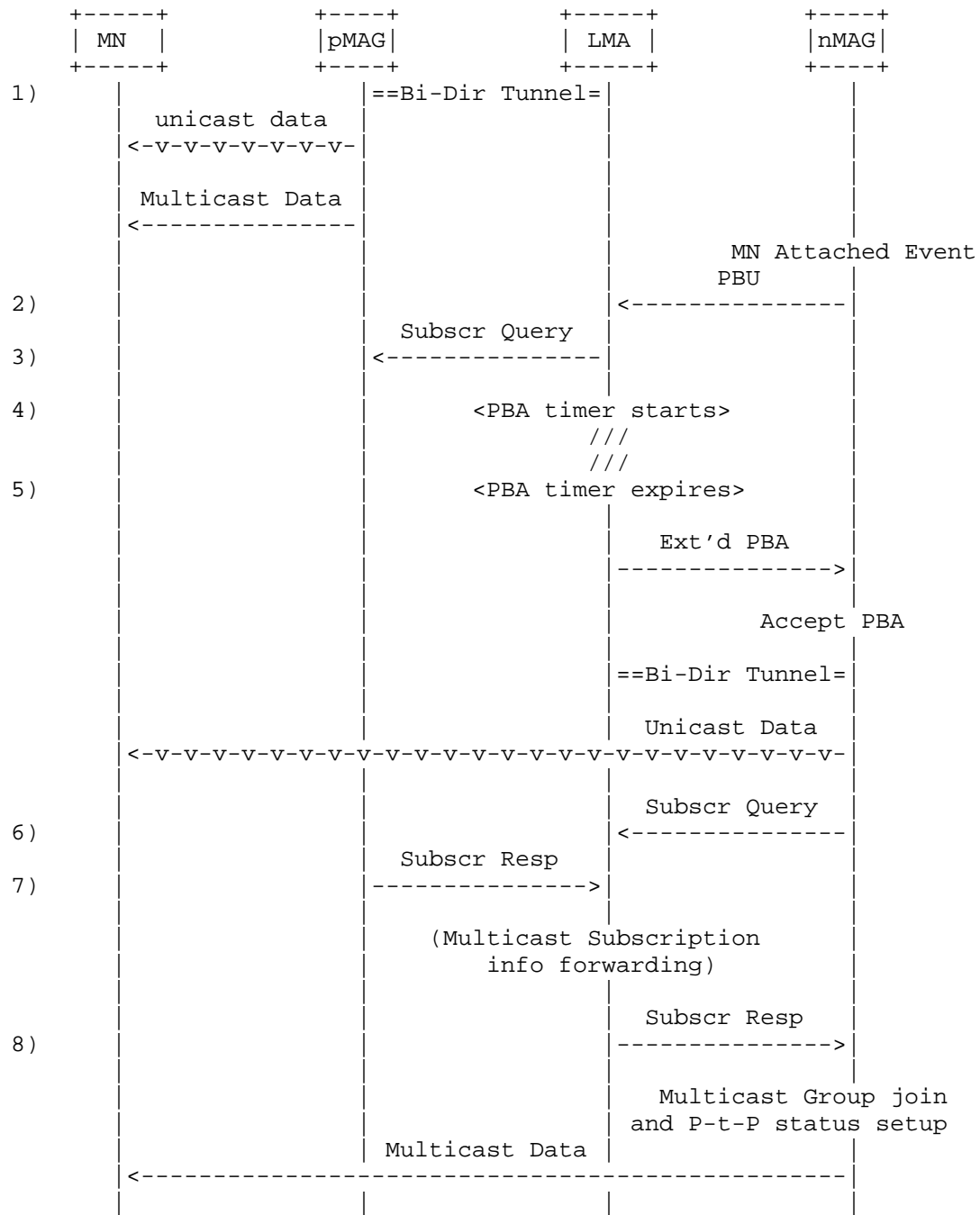


Figure 10: Decoupling of unicast and multicast signaling

The sequence of messages is the following:

1. An MN is attached to the pMAG. The MN is a multicast-enabled node, and it is receiving both unicast and multicast traffic simultaneously.
2. Some time later, the MN perceives a better radio link and decides to attach at a new MAG, nMAG, in a handover process (as a reactive case, the pMAG is not aware of the detachment process). Then, the nMAG triggers a registration process by sending a PBU message (with flag S set to 1) to the LMA.
3. Prior to acknowledge the received PBU message, the LMA decides to query the pMAG about if there is any active multicast subscription for the MN, by sending a Subscription Query message. The LMA decision is based on the checking of flag A when the reactive handover manages the multicast activity indication.
4. Immediately after sending the Subscription Query message, the LMA starts the timer "PBA timer", which determines the maximum waiting time before the PBA is sent to avoid any potential large delay in the forwarding of unicast traffic towards the MN.
5. In case the "PBA timer" expires, the LMA acknowledges the PBU message, by sending the PBA message with flag S=1, without the multicast context information. The nMAG then processes the extended PBA message. Such acknowledgement will allow the MN to receive the unicast traffic from that time on. The bidirectional tunnel is also set up between the nMAG and the LMA if it has not been established before.
6. In parallel, the nMAG sends a Subscription Query message to the LMA requesting the multicast-subscription details yet unknown for the MN.
7. The pMAG answers the Subscription Query message originally sent by the LMA, including the multicast context.
8. After processing the pMAG answer, the LMA sends a Subscription Response message to the nMAG, including the multicast subscription information within the new TLV-encoded option "Active Multicast Subscription". The nMAG processes the PBA message, and it proceeds to set up the multicast status of the point-to-point link between the nMAG and the MN, and to join the content identified by (S,G) on behalf of the MN in case the nMAG is not receiving already such content. The bidirectional tunnel is also set up between the nMAG and the LMA if it has not been established before. At this moment, the multicast content can

also be served to the MN.

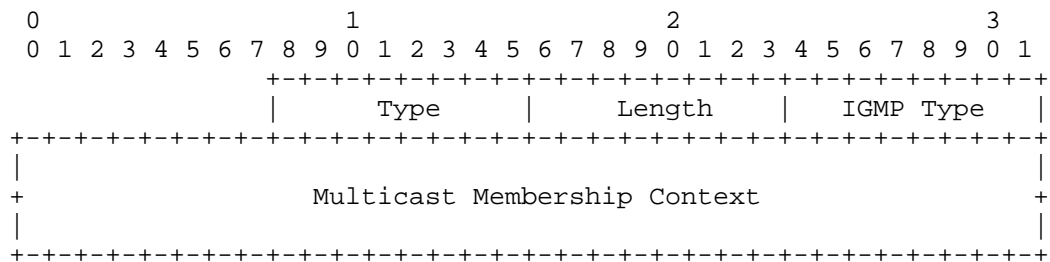
## 6. IPv4 support

IPv4-based mobile nodes (being either IPv4/IPv6 dual-stack, or IPv4-only enabled) can be supported in a PMIPv6 domain according to [RFC5844]. When referring to multicast membership protocols and procedures, this means that IGMP functionality has to be also supported between the PMIPv6 entities, as documented in [RFC6224], to allow the MAG to request multicast contents to the mobility anchor on behalf of the mobiles nodes attached to it.

In order for this specification to support that, the following additions are needed.

### 6.1. Active Multicast Subscription for IPv4

The Active Multicast Subscription option defined in Section 4.1.1, which transports the multicast membership context of the MN during handover, should be compatible with IGMP-based formats. Specifically, the option format is defined for IPv4-based MNs as follows:



IGMPv3 is the primary objective for the definition of the option format. IGMPv1 and IGMPv2 are also considered for backward compatibility. The alignment requirement of this option is  $4n+1$ .

Type:

To be defined by IANA, for indication of an IPv4 Active Multicast Subscription option.

Length:

8-bit unsigned integer indicating the length of the option in octets, excluding the type and length fields.

IGMP type:

Field used to identify the IPv4 multicast membership protocol in use, and the corresponding format of the next Multicast Membership Context information field. This field maps the type codification used in the original IGMP specifications for the Report message.

0x12: Use of IGMPv1 multicast membership protocol.

0x16: Use of IGMPv2 multicast membership protocol.

0x22: Use of IGMPv3 multicast membership protocol.

Multicast Membership Context:

Multicast subscription information corresponding to a single subscribed multicast address. Depending on the IGMP version being used by the MN, the format of the Multicast Context could follow the following formats:

- * For IGMPv1, the Group Address format as defined in [RFC1112].
- * For IGMPv2, the Group Address format as defined in [RFC2236].
- * For IGMPv3, the Group Record format as defined in [RFC3376].

6.2. Signaling procedures for IPv4 support

Generic signaling procedures for the support of IPv4 in PMIPv6 domains have been already specified in [RFC5844]. In order to prevent errors while signaling the on-going multicast subscription for a MN during the handover process, the following extensions have to be considered.

- o If the registration / de-registration process in a handover is for an IPv6-only MN, and the type of the received Active Multicast Subscription option indicates IPv4, then the multicast membership context received is silently discarded.
- o If the registration / de-registration process in a handover is for an IPv4-only MN, and the type of the received Active Multicast Subscription option indicates IPv6, then the multicast membership context received is silently discarded.
- o If the registration / de-registration process in a handover is for a dual stack MN, the received Active Multicast Subscription option



(or options) is (are) accepted independently of the type indication.

### 6.3. Binding Cache extensions for IPv4 support

Additionally, since the membership information is temporally stored in the mobility anchor under some circumstances (e.g., proactive handover), the Binding Cache entry for an IPv4-based multicast-enabled MN should be extended for storing the IGMP-based context formats mentioned above, including the IGMP version indicator.

## 7. Co-existence with PMIPv6 multicast architectural evolutions

Along this document, it has been considered that the LMA entity is in charge of delivering both unicast and multicast traffic to a certain MN through the bi-directional tunnels connecting to the MAG where the MN is attached, as specified in the base solution defined in [RFC6224]. However, the solution described in this memo is not only applicable to the base solution, but it can also be applied to the solutions described in [I-D.ietf-multimob-pmipv6-ropt] to solve the tunnel convergence problem.

The Multicast Tree Mobility Anchor (MTMA) solution in [I-D.ietf-multimob-pmipv6-ropt] makes use of a separate entity to serve multicast traffic through distinct tunnels connected to the MAGs. The tunnels for multicast traffic could not be set up in advance if they are dynamical in nature.

When the "multicast activity" flag is also present in the MN's policy store, the nMAG knows in advance the multicast activity of the incoming MN. Consequently, the nMAG can trigger the multicast tunnel set up in parallel to the registration process, including the acquisition of the active multicast subscription details (the multicast context), saving time on serving the multicast flow to the incoming MN. The concrete procedure for multicast tunnel establishment is out of the scope of this document.

## 8. Security Considerations

This proposal does not pose any additional security threats to those already identified in [RFC5213]. All the security considerations in [RFC5213] are directly applicable to this protocol. The signaling messages, Proxy Binding Update, and Proxy Binding Acknowledgement (extended with the new options defined in this document), the Subscription Query Message, the Subscription Response Message, the Multicast Activity Indication and the Multicast Activity Indication

Acknowledge, exchanged between the mobile access gateway and the local mobility anchor, MUST be protected using end-to-end security association(s) offering integrity and data origin authentication.

The mobile access gateway and the local mobility anchor MUST implement the IPsec security mechanism mandated by Proxy Mobile IPv6 [RFC5213] to secure the signaling described in this document. In the following, we describe the Security Policy Database (SPD) and Security Association Database (SAD) entries necessary to protect the new signaling introduced by this specification (Subscription Query Message, Subscription Response Message, Multicast Activity Indication and Multicast Activity Indication Acknowledge). We use the same format used by [RFC4877]. The SPD and SAD entries are only example configurations. A particular mobile access gateway implementation and a local mobility anchor home agent implementation could configure different SPD and SAD entries as long as they provide the required security of the signaling messages.

For the examples described in this document, a mobile access gateway with address "mag_address_1", and a local mobility anchor with address "lma_address_1" are assumed.

mobile access gateway SPD-S:

- IF local_address = mag_address_1 &  
     remote_address = lma_address_1 &  
     proto = MH & (remote_mh_type = Subscription Query |  
     local_mh_type = Subscription Response |  
     remote_mh_type = Multicast Activity Indication Ack. |  
     local_mh_type = Multicast Activity Indication)  
     Then use SA1 (OUT) and SA2 (IN)

mobile access gateway SAD:

- SA1(OUT, spi_a, lma_address_1, ESP, TRANSPORT):  
     local_address = mag_address_1 &  
     remote_address = lma_address_1 &  
     proto = MH
- SA2(IN, spi_b, mag_address_1, ESP, TRANSPORT):  
     local_address = lma_address_1 &  
     remote_address = mag_address_1 &  
     proto = MH

local mobility anchor SPD-S:

- IF local_address = lma_address_1 &  
     remote_address = mag_address_1 &  
     proto = MH & (remote_mh_type = Subscription Response |  
     local_mh_type = Subscription Query |  
     remote_mh_type = Multicast Activity Indication |  
     local_mh_type = Multicast Activity Indication Ack.)

Then use SA2 (OUT) and SA1 (IN)

```
local mobility anchor SAD:
- SA2(OUT, spi_b, mag_address_1, ESP, TRANSPORT):
    local_address = lma_address_1 &
    remote_address = mag_address_1 &
    proto = MH
- SA1(IN, spi_a, lma_address_1, ESP, TRANSPORT):
    local_address = mag_address_1 &
    remote_address = lma_address_1 &
    proto = MH
```

## 9. IANA Considerations

This document defines the new following elements which values to be allocated by IANA:

- o Mobility Header types: the Subscription Query and Subscription Response, and the Multicast Activity Indication and Multicast Activity Indication Acknowledge mobility header types.
- o Mobility options: the Active Multicast Subscription mobility option for both IPv4 and IPv6 modes of operation.
- o Flags: the multicast Signaling (S), the multicast Information (I), and the multicast Active (A) flags.

## 10. Contributors

Dirk Von Hugo (Telekom Innovation Laboratories,  
Dirk.von-Hugo@telekom.de) extensively contributed to this document.

## 11. Acknowledgments

The authors would like to thank (in alphabetical order) Hitoshi Asaeda, Georgios Karagiannis, Marco Liebsch, Behcet Sarikaya, Thomas C. Schmidt and Stig Venaas for their valuable comments and discussions on the Multimob mailing list. The authors are also grateful with Hitoshi Asaeda, Akbar Rahman, Behcet Sarikaya and Stig Venaas for their review of this document.

The research of Carlos J. Bernardos leading to these results has received funding from the European Community's Seventh Framework Programme (FP7-ICT-2009-5) under grant agreement n. 258053 (MEDIEVAL project), being also partially supported by the Ministry of Science

and Innovation (MICINN) of Spain under the QUARTET project (TIN2009-13992-C02-01).

The research of Ignacio Soto has also received funding from the Spanish MICINN through the I-MOVING project (TEC2010-18907).

## 12. References

### 12.1. Normative References

- [RFC1112] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, August 1989.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC2236] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.
- [RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.
- [RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.
- [RFC4877] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

### 12.2. Informative References

- [I-D.ietf-multimob-pmipv6-ropt]  
Zuniga, J., Contreras, L., Bernardos, C., Jeon, S., and Y. Kim, "Multicast Mobility Routing Optimizations for Proxy Mobile IPv6", draft-ietf-multimob-pmipv6-ropt-03 (work in progress), February 2013.

- [I-D.von-hugo-multimob-future-work]  
Hugo, D., Asaeda, H., Sarikaya, B., and P. Seite,  
"Evaluation of further issues on Multicast Mobility:  
Potential future work for WG MultiMob",  
draft-von-hugo-multimob-future-work-02 (work in progress),  
June 2010.
- [Papagiannaki, et al.]  
Papagiannaki, K., Moon, S., Fralieggh, C., Thiran, P., and  
C. Diot, "Measurement and Analysis of Single-Hop Delay on  
an IP Backbone Network", IEEE Journal on Selected Areas in  
Communications, vol.21, no.6 , August 2003.
- [RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery  
Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.
- [RFC5949] Yokota, H., Chowdhury, K., Koodli, R., Patil, B., and F.  
Xia, "Fast Handovers for Proxy Mobile IPv6", RFC 5949,  
September 2010.
- [RFC6224] Schmidt, T., Waehlisich, M., and S. Krishnan, "Base  
Deployment for Multicast Listener Support in Proxy Mobile  
IPv6 (PMIPv6) Domains", RFC 6224, April 2011.
- [RFC6636] Asaeda, H., Liu, H., and Q. Wu, "Tuning the Behavior of  
the Internet Group Management Protocol (IGMP) and  
Multicast Listener Discovery (MLD) for Routers in Mobile  
and Wireless Networks", RFC 6636, May 2012.
- [Verizon] "LTE: The Future of Mobile Broadband Technology", Verizon  
White Paper ([http://opennetwork.verizonwireless.com/pdfs/  
VZW_LTE_White_Paper_12-10.pdf](http://opennetwork.verizonwireless.com/pdfs/VZW_LTE_White_Paper_12-10.pdf)) , 2010.
- [Y.1541] "Network performance objectives for IP-based services",  
ITU-T Recommendation Y.1541 , December 2011.

#### Appendix A. Performance comparison with base solution

This appendix briefly analyzes and compares the performance improvement provided by the fast handover extensions specified in this document with the base multicast solution defined in [RFC6224]. The main aim is to determine the potential delay reduction in the acquisition of the multicast subscription information by the nMAG during the MN handover. To do that, the analysis will focus on the delay additional to the unicast handover due to the multicast operation in both cases.

Different delay components have to be taken into account for this comparison. Since the interaction between the actors during the handover process (MN, pMAG, nMAG, LMA) is different for each of the solutions, then different sources of delay can be expected for each of them.

#### A.1. Delay characterization of the base solution

The base solution relies on the standard MLD procedures to obtain the multicast subscription information directly from the MN. Once the nMAG completes the configuration of point-to-point link to the attaching MN (the configuration of this link as downstream interface of an MLD proxy instance can run in parallel), it immediately sends an MLD General Query towards the MN for getting knowledge of any active multicast subscription by the MN. When the MN receives the MLD Query, the MN provides information about the active memberships it maintains in the form of an MLD Report message. After successful transmission of this information via the wireless point of attachment to nMAG the corresponding MLD proxy instance at the nMAG will set up the multicast status of the downstream interface. According to this process, the delay is originated on the MAG-MN communication.

The delay components to be considered for the base solution are the following:

- o D_bh, which is the unidirectional (one way) delay encountered in the transmission path between the nMAG and the wireless point of attachment
- o D_radio, which is the unidirectional delay due to the transfer of MLD control messages over the radio channel (user plane) between the wireless point of attachment and the MN, for the MLD Query and Report messages.
- o D_mld, which is the delay incurred by the MN to answer the MLD Query.

The total observed delay can be then formulated as:

$$D_{base} = 2 \times (D_{bh} + D_{radio}) + D_{mld}$$

#### A.2. Delay characterization of the SIAL solution

As described in this document, it is possible to distinguish two scenarios depending on the order in which the LMA receives the notifications of the MN registration and de-registration in the nMAG and the pMAG respectively.

In the proactive case, the MN is firstly de-registered by the pMAG, and later on it is registered by the nMAG. As specified in this document, the LMA will store the multicast subscription information, which will be provided to the nMAG during the MN registration process. Since the registration process necessarily happens before the MLD Query and Report process described in the base solution, the proactive case is inherently faster than the base solution. In fact, since the multicast subscription information is acquired properly during the registration process, the delay incurred is null.

In the reactive case, the LMA receives the MN registration from the nMAG without having previously received the MN de-registration from the pMAG. In case the MN maintains an active subscription, the LMA will query the pMAG to retrieve the multicast subscription information, which is forwarded to the nMAG. According to this process, the delay is originated on the MAG-LMA communication.

The delay components to be considered for the base solution are the following:

- o D_{net}, which is the unidirectional delay found in the network path between the LMA and the MAG.

The total observed delay can be then formulated as:

$$D_{\text{sial}} = 2 \times D_{\text{net}}$$

### A.3. Performance comparison

The performance of the base solution is highly dependent on the radio technology used by the MN to attach to the PMIPv6-Domain. Different radio technologies have distinct properties in terms of radio framing, radio access contention or collision avoidance, channel reliability, etc.

New radio access technologies, such as the one specified in new Long Term Evolution (LTE) standards intend to reduce the latency in order to provide high speed communications. Even though, typical one-way latencies in the LTE radio access will stay around 15 ms [Verizon].

The backhaul delay characterization becomes problematic. In a real network there are several solutions for the backhaul connection in terms of network topology (ring, star, point-to-point, etc) and technology (optical fiber, microwave transmission, xDSL-based accesses, etc), all of them having distinct properties in terms of performance, reliability and delay. These solutions commonly coexist in a real mobile network, in such a way that an MN changing the point of attachment can pass smoothly from one solution to another. A

value of  $D_{bh}=5$  ms can be established as typical value for the backhaul latency in modern networks.

Finally, the MLD induced delay is intrinsic to the MLD protocol specification. A host receiving an MLD Query message will wait a random time in the range (0, Maximum Response Delay) to send the MLD Report message. The default value of the Maximum Response Delay (configurable through the Query Response Interval in MLD) is 10 s in [RFC2710], or 5 s in the best case described in [RFC6636]. Then, in average, it can be expected a potential delay of 5 or 2,5 s, respectively.

As we have seen,  $D_{base}$  is, on average, greater than 2,5 sec with the best case of the values of Query Response Interval in MLD that are recommended in [RFC6636]. That means that the handover delay of the base solution is on the order of seconds while in the solution presented in this specification it is on the order of milliseconds (as it is shown below). To improve the performance of the base solution we could further reduce the value of Query Response Interval but the implications of doing so would need to be carefully analyzed. Even if we assume that Query Response Interval is 0 sec,  $D_{base}$  would be of around  $2 \times (5 \text{ ms} + 15 \text{ ms}) = 40 \text{ ms}$  for last generation systems. Note that this calculation does not take into account the necessary time to re-establish the data plane after the handover to make possible the MLD Query reception. The expected delay will get much worse for older generation systems (e.g., 3G-based radio systems can suffer radio delays in the order of hundreds of ms).

For the SIAL case, the delay in the MAG-LMA communication will be derived from the network diameter (i.e., the number of hops found between the MAG and the LMA in the PMIPv6-Domain). This is largely influenced by the internal network planning. An administrative domain can typically have in the order of 5 hops from access to the interconnection gateway providing connectivity to other networks. Even if the LMA plays a central role topologically in the PMIPv6 domain, such number of hops seems reasonable in a common nation-wide network. Each hop in the path between MAG and LMA will add a certain delay, which can be estimated to be around 1 ms in the best case [Papagiannaki, et al.] and 3 ms in the worst case [Y.1541]. With this in mind, a total delay  $D_{sial}$  of around  $2 \times 5 \times 3 \text{ ms} = 30 \text{ ms}$  can be expected in the worst case.

Then, as conclusion, in a typical deployment, it can be stated that SIAL proposal, even for the worst-case consideration, will perform better than the best case situation for the base solution, which consists of the last generation radio technology, LTE. For any other radio technology the base solution will show even larger deviation from the delay achievable with the SIAL proposal.



## Appendix B. Change Log

The following changes has been made from -00 version.

1. Multicast Address Record format defined in [RFC3810] has been adopted for transferring multicast subscription information in the Active Multicast Subscription mobility option.

The following changes has been made from -01 version.

1. A new appendix has been created to include a performance comparison between this proposal and the base solution.
2. Comments from Akbar Rahman review has been addressed.

The following changes has been made from -02 version.

1. Minor editorial corrections.

The following changes has been made from  
draft-ietf-multimob-fast-handover-03 version.

1. The name of the draft file has been changed to draft-ietf-multimob-handover-optimization as requested by the chairs.

The following changes has been made from  
draft-ietf-multimob-handover-optimization-00 version.

1. New Section 1.1 has been introduced to list a number of basic requirements to be covered for an optimization solution to the handover process in [RFC6224].
2. New Section 6 has been introduced to define the support of IPv4-based MNs in this specification.
3. Section 4.1.1 has been reworked for facilitating the alignment with the IPv4 format defined in new Section 6.
4. Minor editorial corrections.

The following changes has been made from  
draft-ietf-multimob-handover-optimization-01 version.

1. Clarification statements added in several sections according to the comments from B. Sarikaya and S. Venaas.

2. Minor editorial corrections.

Authors' Addresses

Luis M. Contreras  
Telefonica I+D  
Ronda de la Comunicacion, s/n  
Sur-3 building, 3rd floor  
Madrid 28050  
Spain

Email: [lmcm@tid.es](mailto:lmcm@tid.es)

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

Phone: +34 91624 6236  
Email: [cjbc@it.uc3m.es](mailto:cjbc@it.uc3m.es)  
URI: <http://www.it.uc3m.es/cjbc/>

Ignacio Soto  
Universidad Carlos III de Madrid  
Av. Universidad, 30  
Leganes, Madrid 28911  
Spain

Email: [isoto@it.uc3m.es](mailto:isoto@it.uc3m.es)



MULTIMOB Working Group  
Internet-Draft  
Intended status: Experimental  
Expires: August 29, 2013

JC. Zuniga  
InterDigital  
LM. Contreras  
Telefonica I+D  
CJ. Bernardos  
UC3M  
S. Jeon  
Instituto de Telecomunicacoes  
Y. Kim  
Soongsil University  
February 25, 2013

Multicast Mobility Routing Optimizations for Proxy Mobile IPv6  
draft-ietf-multimob-pmipv6-ropt-03

Abstract

The MULTIMOB group has specified a base solution to support IP multicasting in a PMIPv6 domain [RFC6224]. In this document, some enhancements to the base solution are described. These enhancements include the use of a multicast tree mobility anchor as the topological anchor point for multicast traffic, as well as a direct routing option where the MAG can provide access to multicast content in the local network. These enhancements provide benefits such as reducing multicast traffic replication and supporting different PMIPv6 deployment scenarios.

Status of this Memo

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

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

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

This Internet-Draft will expire on August 29, 2013.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the

document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Terminology . . . . .	3
3. Overview . . . . .	5
3.1. Multicast Tree Mobility Anchor (subscription via MTMA) . . . . .	5
3.2. Direct Routing (subscription via direct routing) . . . . .	6
4. Mobile Access Gateway Operation . . . . .	8
4.1. Extensions to Binding Update List Data Structure . . . . .	8
4.2. MAG as MLD proxy . . . . .	8
4.2.1. MTMA mode (subscription via MTMA) . . . . .	8
4.2.2. Direct Routing mode (subscription via direct routing) . . . . .	10
5. Local Mobility Anchor Operation . . . . .	13
5.1. Dynamic IP Multicast Selector Option . . . . .	13
5.1.1. Option application rules . . . . .	13
5.1.2. Option format . . . . .	13
6. Multicast Tree Mobility Anchor Operation . . . . .	14
6.1. Conceptual Data Structures . . . . .	15
7. Mobile Node Operation . . . . .	15
8. IPv4 support . . . . .	15
9. IANA Considerations . . . . .	15
10. Security Considerations . . . . .	16
11. Authors . . . . .	16
12. References . . . . .	16
12.1. Normative References . . . . .	16
12.2. Informative References . . . . .	17
Appendix A. MTMA Deployment Use Cases . . . . .	18
A.1. PMIPv6 domain with ratio 1:1 . . . . .	18
A.2. PMIPv6 domain with ratio N:1 . . . . .	18
A.3. PMIPv6 domain with ratio 1:N . . . . .	20
A.4. PMIPv6 domain with H-LMA . . . . .	22
Authors' Addresses . . . . .	24

## 1. Introduction

Proxy Mobile IPv6 [RFC5213] is a network-based approach to solving the IP mobility problem. In a Proxy Mobile IPv6 (PMIPv6) domain, the Mobile Access Gateway (MAG) behaves as a proxy mobility agent in the network and performs the mobility management on behalf of the Mobile Node (MN). The Local Mobility Anchor (LMA) is the home agent for the MN and the topological anchor point. PMIPv6 was originally designed for unicast traffic. However, a PMIPv6 domain may handle data from both unicast and multicast sources.

The Internet Group Management Protocol (IGMPv3) [RFC3376] is used by IPv4 hosts to report their IP multicast group memberships to neighboring multicast routers. Multicast Listener Discovery (MLDv2) [RFC3810] is used in a similar way by IPv6 routers to discover the presence of IPv6 multicast hosts. Also, the IGMP/MLD proxy [RFC4065] specification allows an intermediate (i.e., edge) node to appear as a multicast router to downstream hosts, and as a host to upstream multicast routers. IGMP and MLD related protocols however were not originally designed to address IP mobility of multicast listeners (i.e., IGMP and MLD protocols were originally designed for fixed networks).

The MULTIMOB group has specified a base solution to support IP multicast listener mobility in a PMIPv6 domain [RFC6224], which describes deployment options without modifying mobility and multicast protocol standards. The PMIPv6 allows a MAG to establish multiple PMIPv6 tunnels with different LMAs, e.g., up to one per MN. In the presence of multicast traffic, multiple instances of the same traffic can converge to the same MAG. Hence, when IP multicasting is applied into PMIPv6, it leads to redundant traffic at a MAG. This is the so-called tunnel convergence problem.

In order to address this issue, a comprehensive solution is proposed in this document, consisting of two complementary enhancements: multicast anchor and direct routing. The former enhancement makes use of a multicast tree mobility anchor (MTMA) as the topological anchor point for remotely delivering multicast traffic, while the latter enhancement uses direct routing taking advantage of local multicast source availability, allowing a MAG to connect directly to a multicast router for simple access to local content. Neither of the two schemes has any impact on the MN to support multicast listener mobility.

## 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",

"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [RFC2119].

This document uses the terminology defined in [RFC5213], [RFC6275], and [RFC3810]. Specifically, the definition of PMIPv6 domain is reused from [RFC5213] and reproduced here for completeness.

Proxy Mobile IPv6 Domain (PMIPv6-Domain): Proxy Mobile IPv6 domain refers to the network where the mobility management of a mobile node is handled using the Proxy Mobile IPv6 protocol as defined in [RFC5213]. The Proxy Mobile IPv6 domain includes local mobility anchors and mobile access gateways between which security associations can be set up and authorization for sending Proxy Binding Updates on behalf of the mobile nodes can be ensured.

In this draft we refine such definition from the point of view of the kind of traffic served to the MN in the following way:

PMIPv6 unicast domain: PMIPv6 unicast domain refers to the network covered by one LMA for unicast service. This service supports mobility as the MN moves from one MAG to another one, both associated to the same LMA regarding the MN unicast traffic.

PMIPv6 multicast domain: PMIPv6 multicast domain refers to the network covered by one network element named MTMA (defined below) for multicast service in such a way that an MN using that service is not aware of mobility as it moves from one MAG to another.

From the definitions above, it can be stated that a PMIPv6 domain can have several PMIPv6 unicast domains and PMIPv6 multicast domains. Additionally, some other definitions are introduced, as follows.

MTMA or multicast tree mobility anchor: An entity working as topological anchor point for multicast traffic.

H-LMA or Hybrid-LMA: An entity dedicated to both unicast and multicast services, that is able to work as both LMA and MTMA simultaneously.

Direct routing: This scheme uses the native multicast infrastructure for retrieving multicast data. For an operator having its own local content, this technique also includes the case where the content source is directly connected to the MAG.

Subscription via MTMA: Multicast subscription mode in which the content is retrieved from the remote (e.g., home) MTMA.

Subscription via direct routing: Multicast subscription mode in which the content is retrieved using direct routing from the local domain.

### 3. Overview

This document specifies a solution to the tunnel convergence problem composed of two operational modes that can be used as complementary enhancements: multicast tree mobility anchor (MTMA) and direct routing. Next, each one of these two operational modes is introduced.

#### 3.1. Multicast Tree Mobility Anchor (subscription via MTMA)

An MTMA is used to serve as the mobility anchor for multicast traffic. Typically, the MTMA will be used to get access to remote multicast content.

The MTMA connects to the MAG as described in [RFC6224] and it can reuse native PMIPv6 features such as tunnel establishment and security [RFC5213], heartbeat [RFC5847], etc. Unicast traffic will go normally to the LMAs in the PMIPv6 domain as described in [RFC5213]. A MAG connecting to the MTMA acts as a MLD proxy.

This section describes how the MTMA works in scenarios of MN attachment and multicast mobility. It concentrates on the case of both LMA and MTMA defining a unique PMIPv6 domain. Some other different deployment scenarios are presented in Appendix A.

Figure 1 shows an example of a PMIPv6 domain supporting multicast mobility. The LMA is dedicated to unicast traffic, and the MTMA is dedicated to multicast traffic. The MTMA can be considered to be a form of upstream multicast router with tunnel interfaces allowing subscription via MTMA for the MNs. Note that there can be multiple LMAs for unicast traffic in a given PMIPv6 domain (not shown in Figure 1 for simplicity). Similarly, more than one MTMA could be deployed by the operator, for example to serve different multicast groups (not shown in Figure 1). This would require support for MLD proxy with multiple interfaces [I-D.ietf-multimob-pmipv6-source], [I-D.contreras-multimob-multiple-upstreams], [I-D.asaeda-pim-mlproxy-multif].

As shown in Figure 1, MAG1 may connect to both unicast (LMAs) and multicast (MTMAs) entities. Thus, a given MN may simultaneously receive both unicast and multicast traffic. In Figure 1, MN1 and MN2 receive unicast traffic, multicast traffic, or both, whereas MN3 receives multicast traffic only.



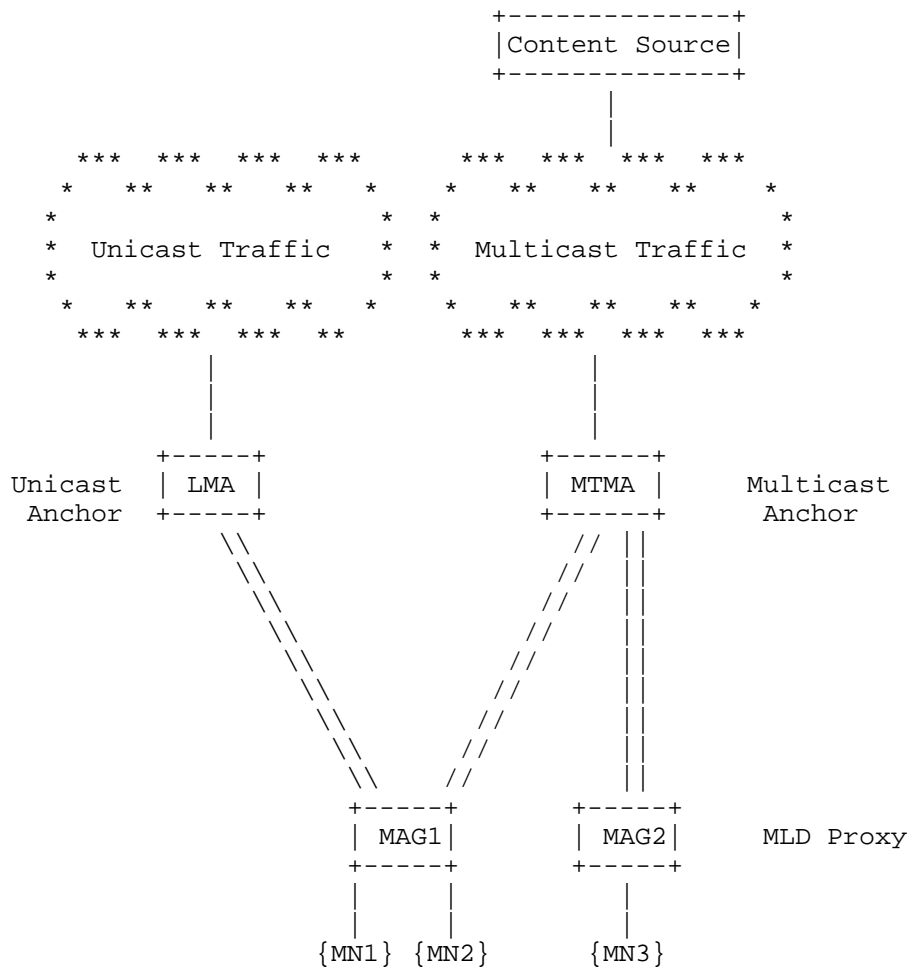


Figure 1: Architecture of Multicast Tree Mobility Anchor (MTMA)

### 3.2. Direct Routing (subscription via direct routing)

Direct routing uses a native multicast infrastructure, allowing a MAG to directly connect to a multicast router (as next hop) in the PMIPv6 domain. A MAG acts as a MLD proxy.

The main purpose of direct routing is to provide optimal connectivity for local content. As a consequence, it alleviates the MTMA of the channel management and data delivery of locally available content. Unicast traffic will go as normally to the LMAs in the PMIPv6 domain.

This section describes how the direct routing works in scenarios of

MN attachment and multicast mobility.

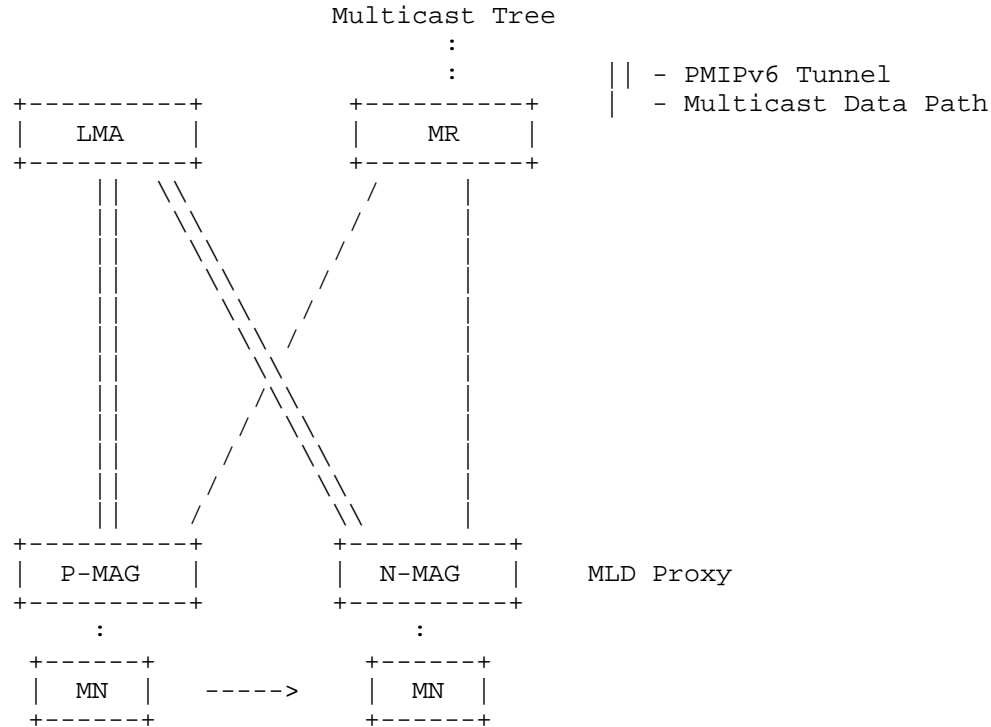


Figure 2: Architecture for direct routing based PMIPv6 multicasting

Figure 2 shows the architecture for the local routing case using native multicasting infrastructure [I-D.deng-multimob-pmip6-requirement].

The LMA is dedicated to unicast traffic, and the multicast traffic is obtained from an upstream multicast router present in the PMIPv6 domain. Note that there can be multiple LMAs for unicast traffic (not shown in Figure 1 for simplicity) in a given PMIPv6 domain.

As shown in Figure 2, a MAG may connect to both unicast (LMA) and multicast (MR) routers. Thus, a given MN may simultaneously receive both unicast and multicast traffic.

As seen in Figure 2, each MAG has a direct connection (i.e., not using the tunnel interface) with a multicast router. To facilitate IGMP/MLD signaling and multicast traffic forwarding, an MLD proxy function defined in [RFC4605] SHOULD be implemented in the MAG. There SHOULD be direct connectivity between the MAG and the local

multicast router (or additional MLD proxy).

#### 4. Mobile Access Gateway Operation

This section describes the operation of the mobile access gateway, considering that the MAG incorporates MLD proxy functions as per [RFC4605].

##### 4.1. Extensions to Binding Update List Data Structure

The binding update list (BUL) in the MAG must be updated to be able to handle the fact that more than one entity (i.e., LMA and MTMA) may be serving the mobile node for different kind of traffic.

##### 4.2. MAG as MLD proxy

###### 4.2.1. MTMA mode (subscription via MTMA)

In case of subscription via MTMA, all MAGs that are connected to the MTMA must support the MLD proxy function [RFC4605]. Specifically in Figure 1, each of the MAG1-MTMA and MAG2-MTMA tunnel interfaces define an MLD proxy domain. The MNs are considered to be on the downstream interface of the MLD proxy (of the MAG), and the MTMA is considered to be on the upstream interface (of the MAG) as per [RFC4605]. Note that the MAG could also be an IGMP proxy. For brevity this document will refer primarily to MLD proxy, but all references to "MLD proxy" should be understood to also include "IGMP/MLD proxy" functionality.

Figure 3 shows the procedure when MN1 attaches to a MAG, and establishes associations with the LMA (unicast) and the MTMA (multicast).

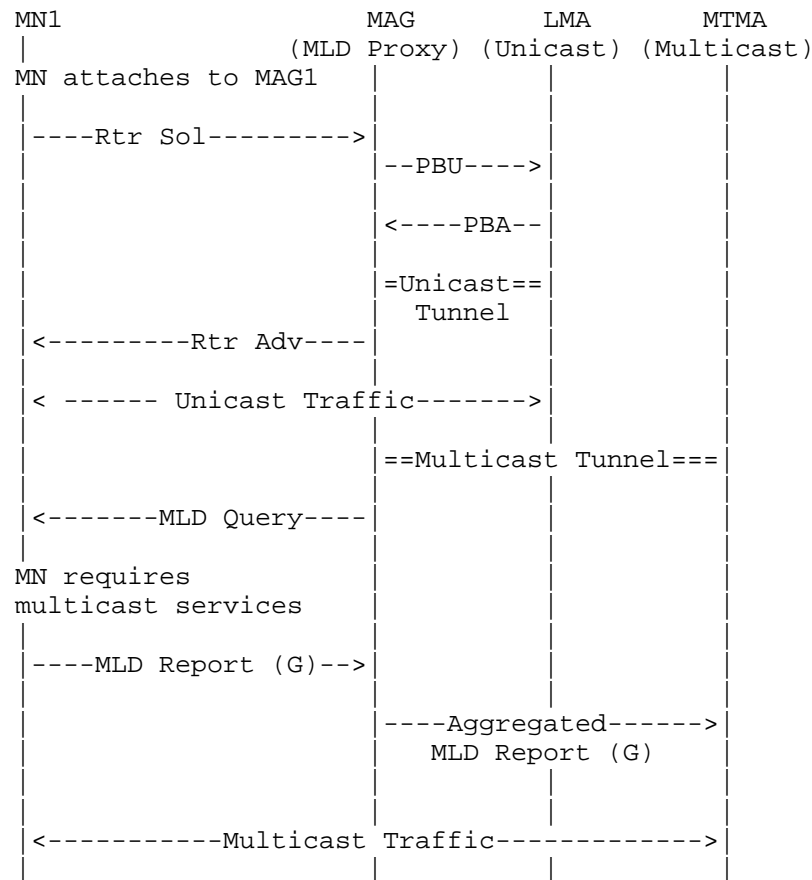


Figure 3: MN Attachment and Multicast Service Establishment for MTMA

In Figure 3, the MAG first establishes the PMIPv6 tunnel with LMA for unicast traffic as defined in [RFC5213] after being triggered by the Router Solicitation message from MN1. Unicast traffic will then flow between MN1 and LMA.

For multicast traffic, a multicast tunnel may have been pre-configured between MAG and MTMA, or may be dynamically established when the first MN appears at the MAG.

MN1 sends the MLD report message (when required by its upper layer applications) as defined in [RFC3810] in response to an MLD Query from MAG. The MAG, acting as a MLD Proxy defined in [RFC4605], will then send an Aggregated MLD Report to the multicast anchor, MTMA (assuming that this is a new multicast group which the MAG had not previously subscribed to). Multicast traffic will then flow from the

MTMA towards MN1.

We next consider a mobility scenario in which MN1 with an ongoing multicast subscription moves from one MAG to another to MAG. According to the baseline solution signaling method described in [RFC6224], after MN1 mobility, the new MAG acting in its role of MLD proxy will send an MLD Query to the newly observed MN on its downlink. Assuming that the subsequent MLD Report from MN1 requests membership for a new multicast group (from the new MAG's point of view), this will then result in an Aggregated MLD Report being sent to the MTMA from the new MAG. This message will be sent through a multicast tunnel between the new MAG and MTMA (pre-established or dynamically established).

When MN1 detaches, the old MAG may keep the multicast tunnel with the multicast MTMA if there are still other MNs using the multicast tunnel. Even if there are no MNs currently on the multicast tunnel, the old MAG may decide to keep the multicast tunnel temporarily for potential future use.

As discussed above, existing MLD (and MLD proxy) signaling will handle a large part of the multicast mobility management for the MN.

#### 4.2.2. Direct Routing mode (subscription via direct routing)

In this case, the MLD proxy instance is configured to obtain the multicast traffic locally. Figure 4 shows an example of multicast service establishment. The MAG first establishes the PMIPv6 tunnel with the LMA for unicast traffic as defined in [RFC5213] after being triggered by the Router Solicitation message from the MN. Unicast traffic will then flow between the MN and LMA.

For multicast traffic, it is assumed that the upstream interface of the MLD proxy instance has been configured pointing to a multicast router internal to the PMIPv6 domain (or towards an additional MLD proxy node in the domain), for all the multicast channels (which, in consequence, have to be local). There should be direct connectivity between the MAG and the local multicast router (or additional MLD proxy).

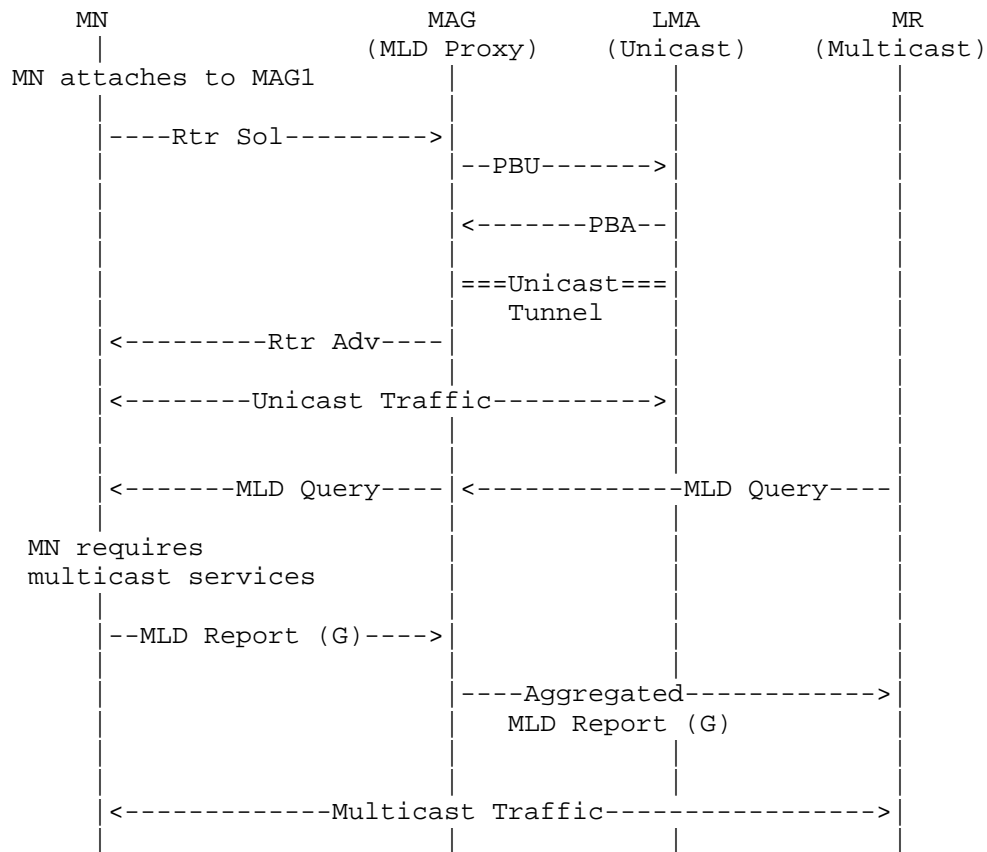


Figure 4: Multicast service establishment for direct routing

Upon detecting node attachment from an incoming interface, the MAG adds each downstream interface to the MLD Proxy instance with upstream link to an MR according to the standard MLD proxy operations [RFC3810] and sends an MLD Query message towards the MN. The MN sends the MLD report message (when required by its upper layer applications) in response to an MLD Query from MAG. Upon receiving the MLD Report message from each incoming interface, the MAG checks the MLD Proxy instance associated with the downstream interface and then the MLD Report messages will be aggregated and forwarded to the upstream link associated with the MR (assuming that this is a new multicast group which the MAG had not previously subscribed to). Multicast traffic will then flow from the local multicast router towards the MN.

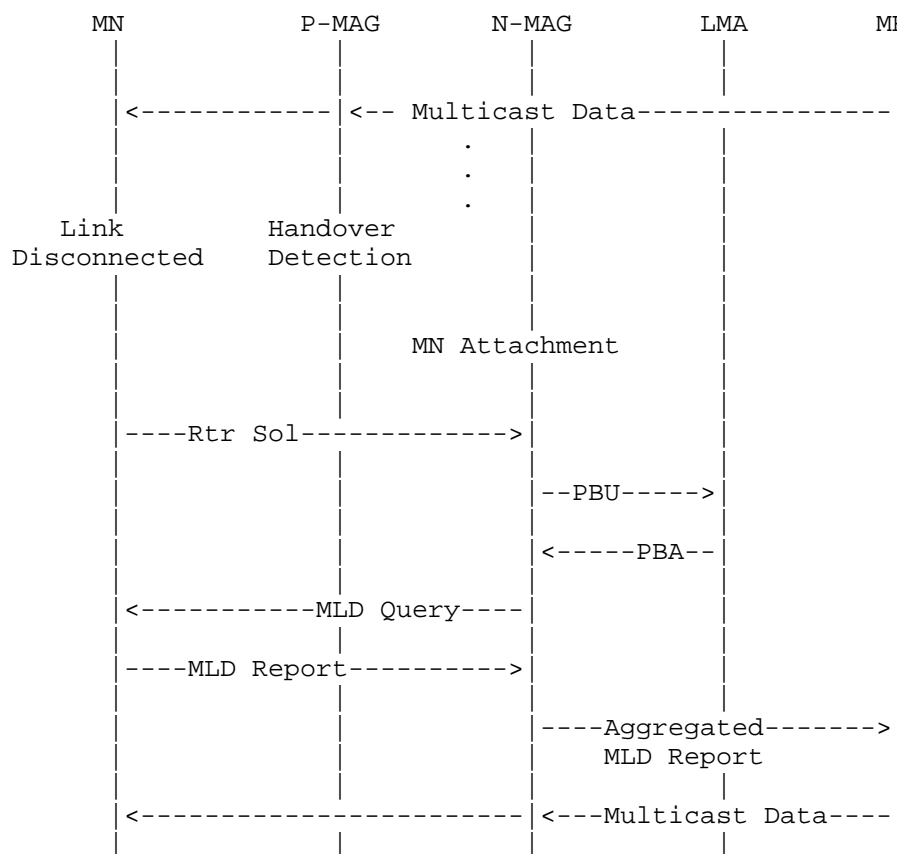


Figure 5: Multicast mobility signaling for direct routing

Figure 5 shows the handover operation procedure for the direct routing operation mode. When an MN hands off to the next MAG (N-MAG) from the previous MAG (P-MAG), the N-MAG detects the newly arrived attached MN and performs binding update procedure by exchanging PBU/PBA signaling messages with LMA. At the same time, a MLD Proxy instance detecting the new MN transmits an MLD query message to the MN. After receiving the MLD query message, the MN sends an MLD report message that includes the multicast group information. The N-MAG then sends an aggregated MLD report message to the upstream link associated with the MR. In the direct routing case, an upstream interface of MLD Proxy instance is decided towards certain multicast router based on the operator's configuration or multicast routing, as compared to the base solution defined in [RFC6224] where it is determined for each MN based on the Proxy Binding Update List. When the N-MAG receives the multicast packets from the MR, it then simply forwards them without tunnel encapsulation. The N-MAG updates the

MN's location information to the LMA by exchanging PBU/PBA signaling messages.

## 5. Local Mobility Anchor Operation

This section includes a new mobility option to support dynamic policies on subscription via MTMA/direct routing based on the local mobility anchor conveying the required info to the mobile access gateway in the proxy binding acknowledge message.

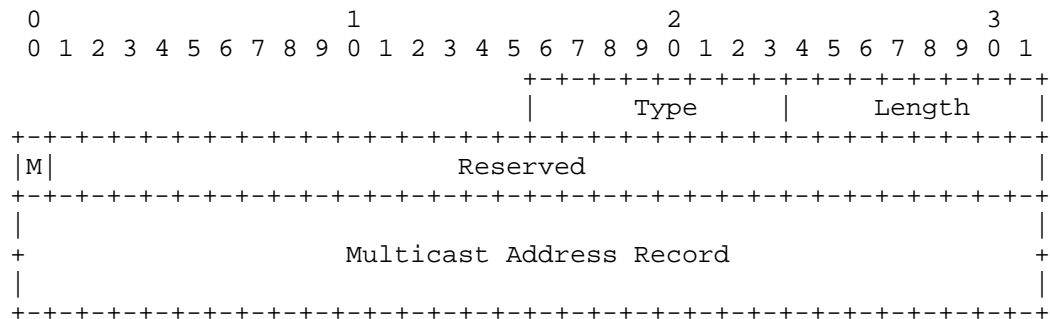
### 5.1. Dynamic IP Multicast Selector Option

#### 5.1.1. Option application rules

A new TLV-encoded mobility option, "Dynamic IP Multicast Selector" option is defined for use with the PBA (Proxy Binding Acknowledge) message exchanged between an LMA and a MAG to convey dynamic policies on subscription via MTMA/direct routing. This option is used for exchanging the IP addresses of both the group subscribed to by the MN, and the source(s) delivering it, as well as the applicable filter mode. This information is carried by using directly the Multicast Address Record format defined in [RFC3810]. There can be multiple "Dynamic IP Multicast Selector" options present in the message, one for each active subscription maintained by the MN (i.e., one per Multicast Address Record).

#### 5.1.2. Option format

The format of this new option is as follows:



Type:

To be defined by IANA.



Length:

8-bit unsigned integer indicating the length of the option in octets, excluding the type and length fields.

Reserved:

This field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

Dynamic IP Multicast Selector Mode Flag:

This field indicates the subscription via MTMA/direct routing mode. If the (M) flag value is set to a value of (1), it is an indication that the IP multicast traffic associated to the multicast group identified by the Multicast Address Record in this mobility option SHOULD be routed locally (subscription via direct routing mode). If the (M) flag value is set to a value of (0), it is an indication that IP multicast traffic associated to the multicast group identified by the Multicast Address Record in this mobility option SHOULD be routed to the home network, via the MTMA (subscription via MTMA mode). All other IP traffic associated with the mobile node SHOULD be managed according to a default policy configured at the PMIPv6 multicast domain.

Multicast Address Record:

Multicast subscription information corresponding to a single subscribed multicast address as defined in [RFC3810].

## 6. Multicast Tree Mobility Anchor Operation

The MTMA provides connectivity to the multicast infrastructure out of the PMIPv6 domain. The MTMA itself could either act as an additional MLD proxy (only in the case where all the connected MAGs act also as MLD proxies), reporting to a further node an aggregated view of the subscriptions in a PMIPv6 multicast domain; or it can act as a designated multicast router for all the MAGs in a PMIPv6 multicast domain. The MTMA will then request the multicast content on behalf of the MAGs (and MNs behind them). In addition, the MTMA will create and maintain the corresponding multicast forwarding states per each tunnel interface towards the MAGs. Whatever the role played, when the MAGs act as MLD proxy, the MTMA becomes the MLD querier of the MLD proxy instance located in each MAG.

## 6.1. Conceptual Data Structures

The MTMA does not directly interact with the MNs attached to any of the MAGs. The MTMA only manages the multicast groups subscribed per MAG on behalf of the MNs attached to it. Having this in mind, the relevant information to be stored in the MTMA should be the tunnel interface identifier (tunnel-if-id) of the bi-directional tunnel for multicast between the MTMA and every MAG (e.g., similar to what it is stated in [RFC5213] for the unicast case), the IP addresses of the multicast group delivered per tunnel to each of the MAGs, and the IP addresses of the sources injecting the multicast traffic per tunnel to the multicast domain defined by the MTMA.

## 7. Mobile Node Operation

The MN operation is not impacted by the existence of an MTMA as anchor for the multicast traffic being subscribed or the use of direct routing. The MN will act according to the stated operations in [RFC5213] and [RFC6224].

This draft considers that every MN requesting multicast-only services is previously registered in a PMIPv6 unicast domain to get a unicast IP address. The registration can also be required also for several purposes such as remote management, billing, multicast configuration, etc.

A given mobile node's policy profile information must be updated to be able to store the IPv6 addresses of both the LMA and MTMA, the later for the subscription via MTMA case.

## 8. IPv4 support

This document does not introduce any IPv4-specific issue. IPv4 and dual-stack IPv4/IPv6 considerations covered in section 4.4 of [RFC6224] also apply to the extensions defined in this document. Although references to "MLD proxy" have been used in the document, it should be understood to also include "IGMP/MLD proxy" functionality.

## 9. IANA Considerations

TBD.

## 10. Security Considerations

This draft discusses the operations of existing protocols without modifications. It does not introduce new security threats beyond the current security considerations of PMIPv6 [RFC5213], MLD [RFC3810], IGMP [RFC3376] and IGMP/MLD Proxying [RFC4605].

## 11. Authors

Additional co-authors of this document are:

Akbar Rahman

InterDigital Communications, LLC

E-mail: akbar.rahman@interdigital.com

Ignacio Soto

Universidad Carlos III de Madrid

E-mail: isoto@it.uc3m.es

## 12. References

### 12.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.
- [RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.
- [RFC4065] Kempf, J., "Instructions for Seamoby and Experimental Mobility Protocol IANA Allocations", RFC 4065, July 2005.
- [RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.
- [RFC4605] Fenner, B., He, H., Haberman, B., and H. Sandick, "Internet Group Management Protocol (IGMP) / Multicast

Listener Discovery (MLD)-Based Multicast Forwarding  
("IGMP/MLD Proxying"), RFC 4605, August 2006.

- [RFC4607] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5847] Devarapalli, V., Koodli, R., Lim, H., Kant, N., Krishnan, S., and J. Laganier, "Heartbeat Mechanism for Proxy Mobile IPv6", RFC 5847, June 2010.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

## 12.2. Informative References

- [I-D.asaeda-pim-mldproxy-multif]  
Asaeda, H. and S. Jeon, "Multiple Upstream Interface Support for IGMP/MLD Proxy",  
draft-asaeda-pim-mldproxy-multif-01 (work in progress),  
February 2013.
- [I-D.contreras-multimob-multiple-upstreams]  
Contreras, L. and C. Bernardos, "Extension of the MLD proxy functionality to support multiple upstream interfaces",  
draft-contreras-multimob-multiple-upstreams-00 (work in progress), October 2012.
- [I-D.deng-multimob-pmip6-requirement]  
Deng, H., Chen, G., Schmidt, T., Seite, P., and P. Yang, "Multicast Support Requirements for Proxy Mobile IPv6",  
draft-deng-multimob-pmip6-requirement-02 (work in progress), July 2009.
- [I-D.ietf-multimob-pmipv6-source]  
Schmidt, T., Gao, S., Zhang, H., and M. Waehlich, "Mobile Multicast Sender Support in Proxy Mobile IPv6 (PMIPv6) Domains", draft-ietf-multimob-pmipv6-source-02 (work in progress), October 2012.
- [RFC6224] Schmidt, T., Waehlich, M., and S. Krishnan, "Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains", RFC 6224, April 2011.

## Appendix A. MTMA Deployment Use Cases

From the network architecture point of view, there are several options when considering the multicast tree mobility anchor (MTMA) approach. These options can be distinguished in terms of the number of LMAs and MTMAs present in a PMIPv6 domain and the service relationship that a set of MNs gets from them, in the form of a "LMA : MTMA" ratio. According to that, it is possible to differentiate the following approaches:

- o A set of MNs is served in a PMIPv6 domain by two entities, one MTMA for multicast service, and one LMA for unicast, in such a way that the ratio is 1:1 (one common PMIPv6 unicast and multicast domain).
- o A set of MNs is served in a PMIPv6 domain by several entities, one MTMA for multicast service, while the others (LMAs) for unicast, in such a way that the ratio is N:1 (N PMIPv6 unicast domains coexist with a unique multicast domain).
- o A set of MNs is served in a PMIPv6 domain by several entities, one LMA for unicast, while the others (MTMAs) are devoted to multicast service, in such a way that the ratio is 1:N (one single PMIPv6 unicast domain coexists with multiple multicast domains).

Scenarios with an N:M ratio are considered to be a combination of the previous ones.

### A.1. PMIPv6 domain with ratio 1:1

This approach basically refers to the architecture presented in Figure 1. Within this approach, a common set of MNs is served by a couple of entities, one LMA for unicast and one MTMA for multicast. All the MNs of the set are served by these two elements as they move in the PMIPv6 domain.

### A.2. PMIPv6 domain with ratio N:1

This approach basically refers to the situation where a common set of MNs is served by a unique MTMA for multicast service, but simultaneously there are subsets from that group of MNs which are served by distinct LMAs for unicast service as they move in the PMIPv6 domain. Each particular MN association with the LMAs (unicast) and MTMA (multicast) remains always the same as it moves in the PMIPv6 domain.

Figure 6 shows the scenario here described.

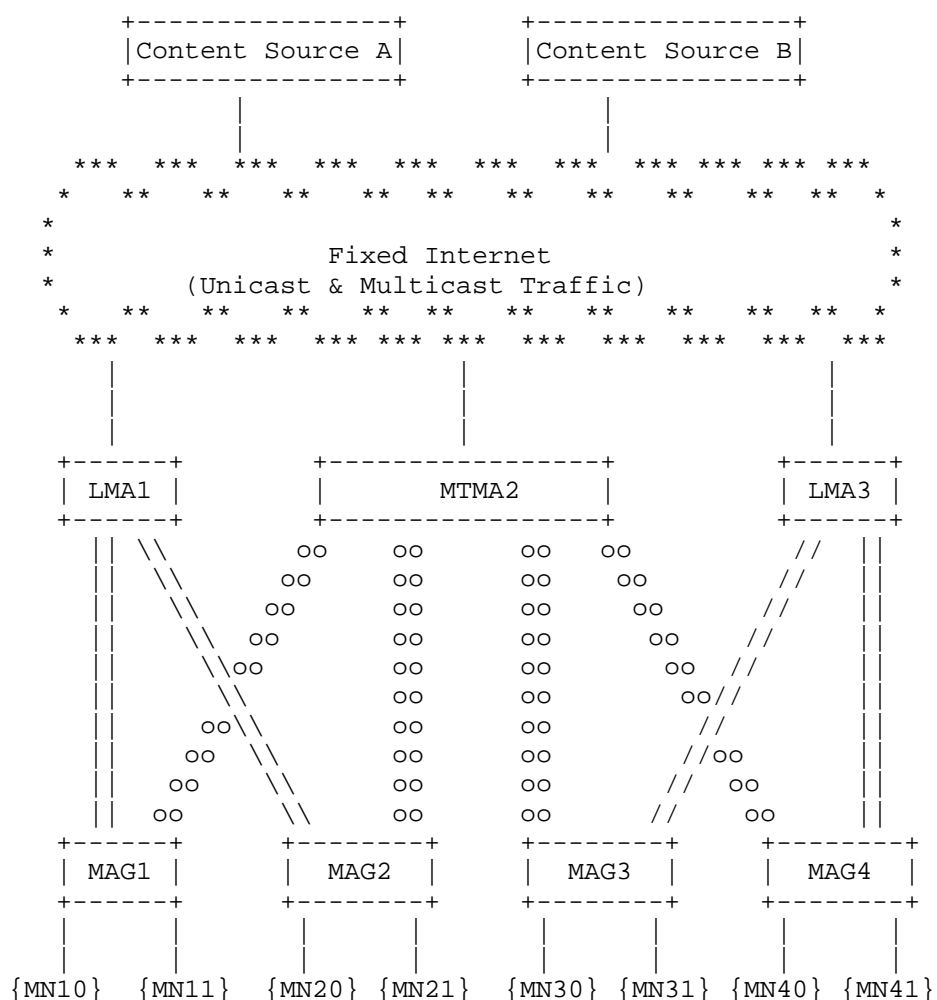


Figure 6: PMIPv6 domain with ratio N:1

The Figure 6 proposes an architecture where there are two entities acting as LMAs, LMA1 and LMA3, while there is another one, named MTMA2, working as multicast tree mobility anchor. LMA1 and LMA3 constitute two distinct unicast domains, whereas MTMA2 forms a single multicast domain. The tunnels among MAGs and LMAs represented by lines ("||") indicate a tunnel transporting unicast traffic, while the tunnels among MAGs and MTMA2 depicted with circles ("o") show a tunnel transporting multicast traffic.

In the figure it can be observed that all the MNs are served by MTMA2 for the incoming multicast traffic from sources A or B. However,

there are different subsets regarding unicast traffic which maintain distinct associations within the PMIPv6 domain. For instance, the subset formed by MN10, MN11, MN20 and MN21 is served by LMA1 for unicast, and the rest of MNs are being served by LMA3. For the scenario described above, the association between each MN and the corresponding LMA and MTMA is permanently maintained.

#### A.3. PMIPv6 domain with ratio 1:N

This approach is related to a scenario where a common group of MNs is served by a unique LMA for unicast service, but simultaneously there are subsets from that group of MNs which are served by distinct MTMAs for multicast service as they move in the PMIPv6 domain. Different MTMAs might be associated to serving different multicast groups. These associations remain the same even if the MNs move within the PMIPv6 domain.

Figure 7 shows the scenario here described.

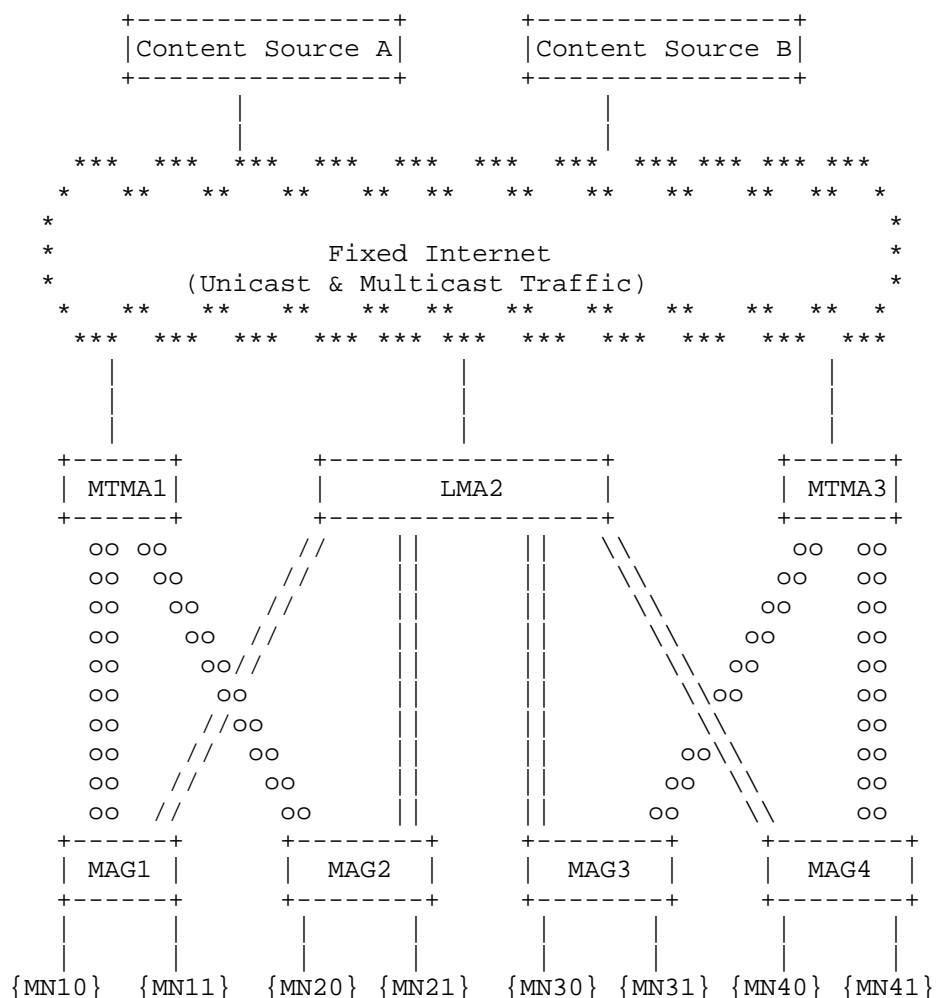


Figure 7: PMIPv6 domain with ratio 1:N

The Figure 7 proposes an architecture where the LMA2 is the unique LMA for a certain group of MNs, while there are two others entities, MTMA1 and MTMA3, acting as MTMAs for different subsets of MNs of the same group. MTMA1 and MTMA3 constitute two distinct multicast domains, whereas LMA2 forms a single unicast domain. Each MTMA could be devoted to carry on a different content (for instance, MTMA1 for source A and MTMA3 for source B). Looking at the picture, the subset formed by MN10, MN11, MN20 and MN21 is served by MTMA1 for multicast. The rest of MNs are being served by MTMA3 also for multicast. Finally, all of them are served by LMA2 for unicast. For the scenario described above, the association between multicast content



and MTMA is permanently maintained.

#### A.4. PMIPv6 domain with H-LMA

The H-LMA is defined as an entity which simultaneously transports unicast and multicast service, that is, it simultaneously works as LMA and MTMA. In the context of the MTMA solution, an H-LMA can play the role of MTMA for an entire group of MNs in a PMIPv6 domain, while acting simultaneously as LMA for a subset of them. The figure 9 adapts the PMIPv6 domain with ratio N:1 scenario of figure 7 to the case where MTMA2 is an H-LMA, which serves multicast traffic to all the MNs in the picture, and simultaneously, it is able to serve unicast traffic to the subset formed by MN30, MN40 and MN41.

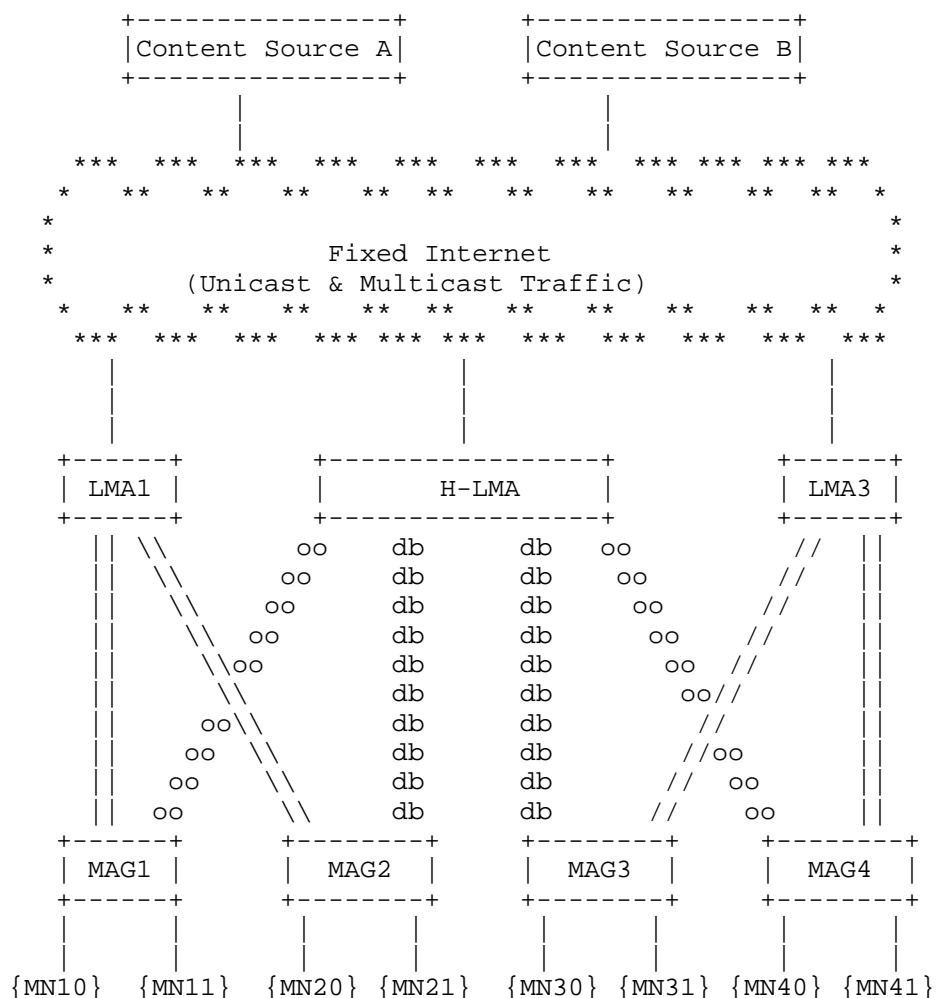


Figure 8: PMIPv6 domain with H-LMA

Figure 7 presents a PMIPv6 network where there are two pure unicast LMAs, LMA1 and LMA3, and a hybrid LMA, labeled as H-LMA in the figure. The H-LMA is an MTMA from the perspective of MAG1 and MAG4. The tunnels among MAGs and LMAs represented by lines ("|") indicate a tunnel transporting exclusively unicast traffic, the tunnels depicted with circles ("o") show a tunnel transporting exclusively multicast traffic, and the tunnels with mixed lines and circles ("db") describe a tunnel transporting both types of traffic simultaneously.

All of the MNs in the figure receive the multicast traffic from H-LMA (one single multicast domain), but it is possible to distinguish three subsets from the unicast service perspective (that is, three unicast domains). The first subset is the one formed by MN10, MN11 and MN 20, which receives unicast traffic from LMA1. A second subset is the one formed by MN21 and MN30, which receives unicast traffic from H-LMA. And finally, a third subset is built on MN31, MN40 and MN41, which receives unicast traffic from LMA3. For the scenario described above, the association between each MN and the corresponding LMA and H-LMA is permanently maintained.

#### Authors' Addresses

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

Email: [JuanCarlos.Zuniga@InterDigital.com](mailto:JuanCarlos.Zuniga@InterDigital.com)  
URI: <http://www.InterDigital.com/>

Luis M. Contreras  
Telefonica I+D  
Don Ramon de la Cruz, 82-84  
Madrid 28006  
Spain

Email: [lmcm@tid.es](mailto:lmcm@tid.es)

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

Phone: +34 91624 6236  
Email: [cjbc@it.uc3m.es](mailto:cjbc@it.uc3m.es)  
URI: <http://www.it.uc3m.es/cjbc/>

Seil Jeon  
Instituto de Telecomunicacoes  
Campus Universitario de Santiago  
Aveiro 3810-193  
Portugal

Email: [seiljeon@av.it.pt](mailto:seiljeon@av.it.pt)  
URI: <https://atnog.av.it.pt/~sjeon/>

Younghan Kim  
Soongsil University  
Sangdo-dong, Dongjak-gu  
Seoul 511  
Republic of Korea

Email: [yhkim@dcn.ssu.ac.kr](mailto:yhkim@dcn.ssu.ac.kr)  
URI: <http://dcnlab.ssu.ac.kr/>



MULTIMOB Group  
Internet-Draft  
Intended status: Standards Track  
Expires: August 29, 2013

T C. Schmidt, Ed.  
HAW Hamburg  
S. Gao  
H. Zhang  
Beijing Jiaotong University  
M. Waehlich  
link-lab & FU Berlin  
February 25, 2013

Mobile Multicast Sender Support in Proxy Mobile IPv6 (PMIPv6) Domains  
draft-ietf-multimob-pmipv6-source-03

Abstract

Multicast communication can be enabled in Proxy Mobile IPv6 domains via the Local Mobility Anchors by deploying MLD Proxy functions at Mobile Access Gateways, via a direct traffic distribution within an ISP's access network, or by selective route optimization schemes. This document describes the support of mobile multicast senders in Proxy Mobile IPv6 domains for all three scenarios. Protocol optimizations for synchronizing PMIPv6 with PIM, as well as extended MLD Proxy functions are presented. Mobile sources always remain agnostic of multicast mobility operations.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of this Memo

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

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

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

This Internet-Draft will expire on August 29, 2013.

## Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	4
2. Terminology . . . . .	5
3. Base Solution for Source Mobility and PMIPv6 Routing . . . . .	5
3.1. Overview . . . . .	5
3.2. Base Solution for Source Mobility: Details . . . . .	9
3.2.1. Operations of the Mobile Node . . . . .	9
3.2.2. Operations of the Mobile Access Gateway . . . . .	9
3.2.3. Operations of the Local Mobility Anchor . . . . .	9
3.2.4. IPv4 Support . . . . .	10
3.2.5. Efficiency of the Distribution System . . . . .	11
4. Direct Multicast Routing . . . . .	11
4.1. Overview . . . . .	12
4.2. MLD Proxies at MAGs . . . . .	13
4.2.1. Considerations for PIM-SM on the Upstream . . . . .	14
4.2.2. SSM Considerations . . . . .	14
4.3. PIM-SM . . . . .	14
4.3.1. Routing Information Base for PIM-SM . . . . .	14
4.3.2. Operations of PIM in Phase One . . . . .	15
4.3.3. Operations of PIM in Phase Two . . . . .	16
4.3.4. Operations of PIM in Phase Three . . . . .	16
4.3.5. PIM-SSM Considerations . . . . .	17
4.3.6. Handover Optimizations for PIM . . . . .	17
4.4. BIDIR-PIM . . . . .	18
4.4.1. Routing Information Base for BIDIR-PIM . . . . .	18
4.4.2. Operations of BIDIR-PIM . . . . .	18
5. Extended MLD Proxy Function for Optimized Source Mobility in PMIPv6 . . . . .	19
5.1. Peering Function for MLD Proxies . . . . .	19
5.1.1. Operations at the Multicast Sender . . . . .	19
5.1.2. Operations at the Multicast Listener . . . . .	20
6. IANA Considerations . . . . .	21
7. Security Considerations . . . . .	21
8. Acknowledgements . . . . .	22
9. References . . . . .	22
9.1. Normative References . . . . .	22
9.2. Informative References . . . . .	23
Appendix A. Multiple Upstream Interface Proxy . . . . .	23
A.1. Operations for Local Multicast Sources . . . . .	24
A.2. Operations for Local Multicast Subscribers . . . . .	24
Appendix B. Evaluation of Traffic Flows . . . . .	24
Appendix C. Change Log . . . . .	25
Authors' Addresses . . . . .	26



## 1. Introduction

Proxy Mobile IPv6 (PMIPv6) [RFC5213] extends Mobile IPv6 (MIPv6) [RFC6275] by network-based management functions that enable IP mobility for a host without requiring its participation in any mobility-related signaling. Additional network entities called the Local Mobility Anchor (LMA), and Mobile Access Gateways (MAGs), are responsible for managing IP mobility on behalf of the mobile node (MN). An MN connected to a PMIPv6 domain, which only operates according to the base specifications of [RFC5213], cannot participate in multicast communication, as MAGs will discard group packets.

Multicast support for mobile listeners can be enabled within a PMIPv6 domain by deploying MLD Proxy functions at Mobile Access Gateways, and multicast routing functions at Local Mobility Anchors [RFC6224]. This base deployment option is the simplest way to PMIPv6 multicast extensions in the sense that it follows the common PMIPv6 traffic model and neither requires new protocol operations nor additional infrastructure entities. Standard software functions need to be activated on PMIPv6 entities, only, at the price of possibly non-optimal multicast routing.

Alternate solutions leverage performance optimization by providing multicast routing at the access gateways directly, or by selective route optimization schemes. Such approaches (partially) follow the business model of providing multicast data services in parallel to PMIPv6 unicast routing.

Multicast listener support satisfies the needs of receptive use cases such as IPTV or server-centric gaming on mobiles. However, current trends in the Internet enfold towards user-centric, highly interactive group applications like user generated streaming, conferencing, collective mobile sensing, etc. Many of these popular applications create group content at end systems and can largely profit from a direct data transmission to a multicast-enabled network.

This document describes the support of mobile multicast senders in Proxy Mobile IPv6 domains subsequently for the base deployment scenario [RFC6224], for direct traffic distribution within an ISP's access network, as well as for selective route optimization schemes. The contribution of this work reflects the source mobility problem as discussed in [RFC5757]. Mobile Nodes in this setting remain agnostic of multicast mobility operations.

## 2. Terminology

This document uses the terminology as defined for the mobility protocols [RFC6275], [RFC5213] and [RFC5844], as well as the multicast edge related protocols [RFC3376], [RFC3810] and [RFC4605].

## 3. Base Solution for Source Mobility and PMIPv6 Routing

### 3.1. Overview

The reference scenario for multicast deployment in Proxy Mobile IPv6 domains is illustrated in Figure 1. MAGs play the role of first-hop access routers that serve multiple MNs on the downstream while running an MLD/IGMP proxy instance for every LMA upstream tunnel.

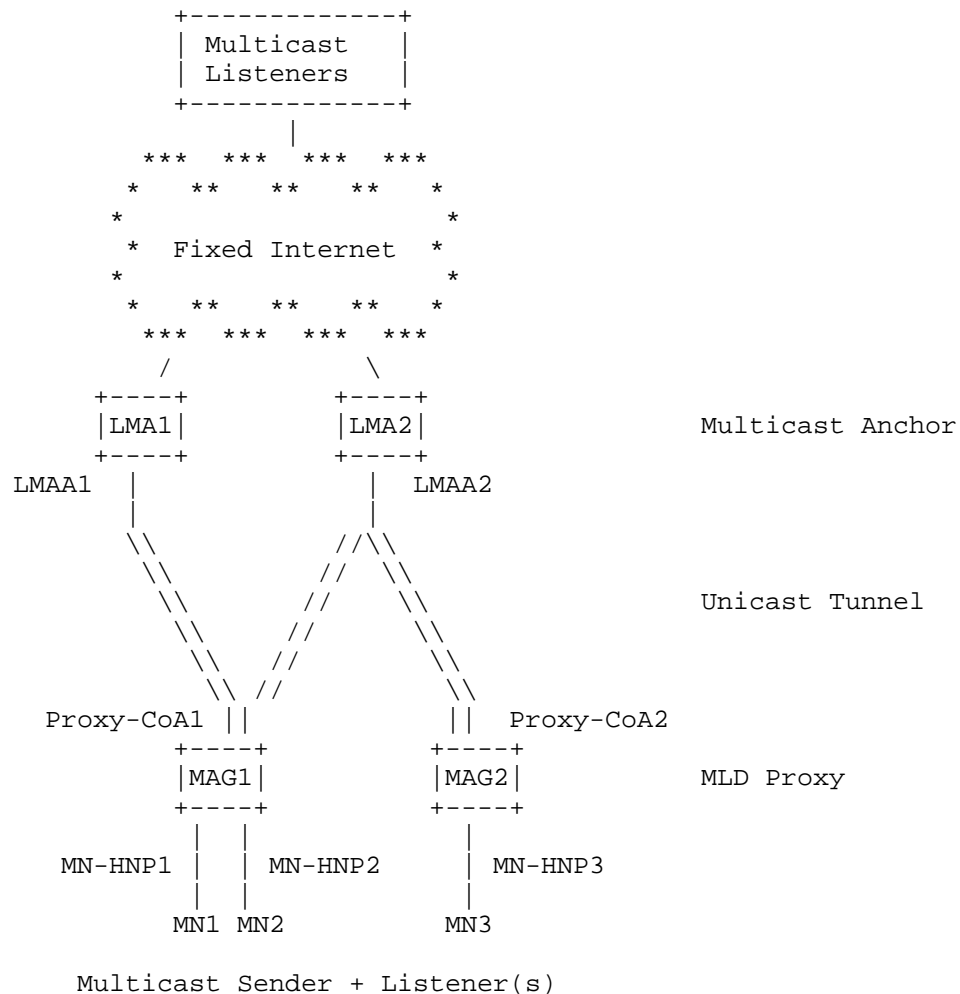


Figure 1: Reference Network for Multicast Deployment in PMIPv6 with Source Mobility

An MN in a PMIPv6 domain will decide on multicast data transmission completely independent of its current mobility conditions. It will send packets as initiated by applications, using its source address with Home Network Prefix (HNP) and a multicast destination address chosen by application needs. Multicast packets will arrive at the currently active MAG via one of its downstream local (wireless) links. A multicast unaware MAG would simply discard these packets in the absence of a multicast routing information base (MRIB).

An MN can successfully distribute multicast data in PMIPv6, if MLD

proxy functions are deployed at the MAG as described in [RFC6224]. In this set-up, the MLD proxy instance serving a mobile multicast source has configured its upstream interface at the tunnel towards MN's corresponding LMA. For each LMA, there will be a separate instance of an MLD proxy.

According to the specifications given in [RFC4605], multicast data arriving from a downstream interface of an MLD proxy will be forwarded to the upstream interface and to all but the incoming downstream interfaces that have appropriate forwarding states for this group. Thus multicast streams originating from an MN will arrive at the corresponding LMA and directly at all mobile receivers co-located at the same MAG and MLD Proxy instance. Serving as the designated multicast router or an additional MLD proxy, the LMA forwards data to the fixed Internet, whenever forwarding states are maintained by multicast routing. If the LMA is acting as another MLD proxy, it will forward the multicast data to its upstream interface, and to downstream interfaces with matching subscriptions, accordingly.

In case of a handover, the MN (unaware of IP mobility) can continue to send multicast packets as soon as network connectivity is reconfigured. At this time, the MAG has determined the corresponding LMA, and IPv6 unicast address configuration (including PMIPv6 bindings) has been performed. Still multicast packets arriving at the MAG are discarded (if not buffered) until the MAG has completed the following steps.

1. The MAG has determined that the MN is admissible to multicast services.
2. The MAG has added the new downstream link to the MLD proxy instance with up-link to the corresponding LMA.

As soon as the MN's uplink is associated with the corresponding MLD proxy instance, multicast packets are forwarded again to the LMA and eventually to receivers within the PMIP domain (see the call flow in Figure 2). In this way, multicast source mobility is transparently enabled in PMIPv6 domains that deploy the base scenario for multicast.

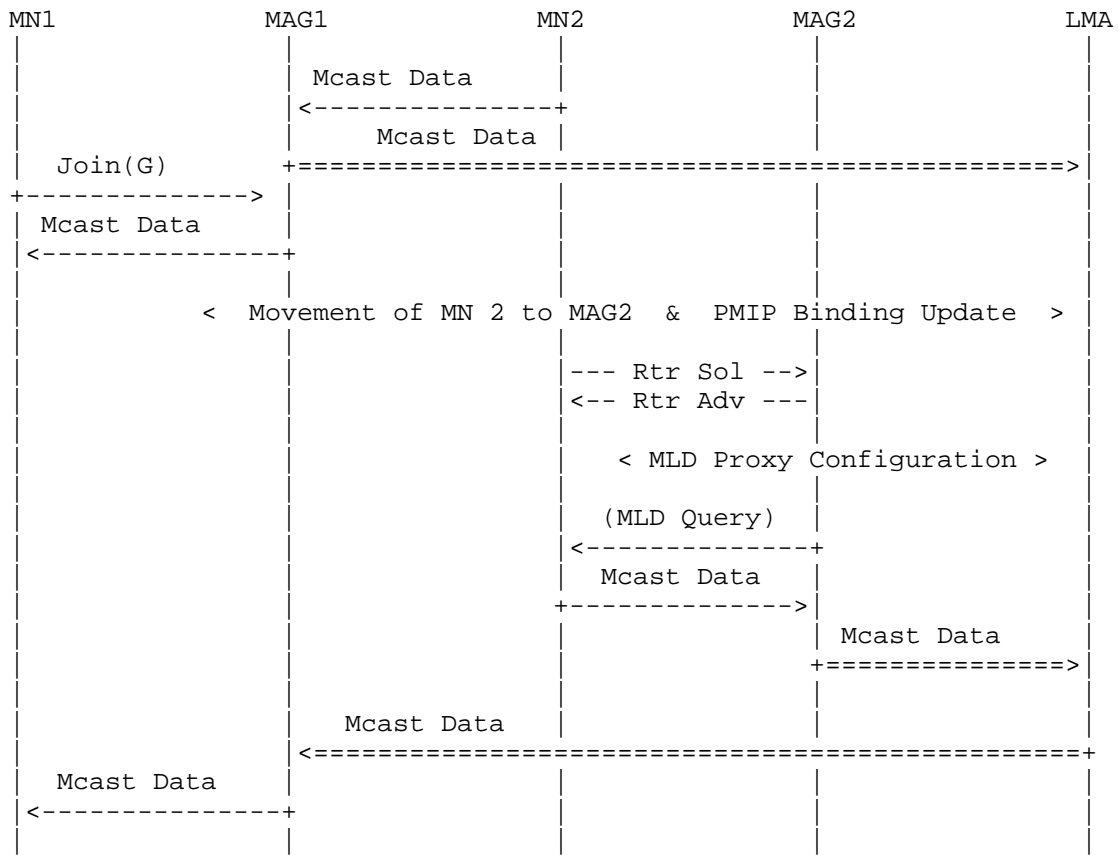


Figure 2: Call Flow for Group Communication in Multicast-enabled PMIP

These multicast deployment considerations likewise apply for mobile nodes that operate with their IPv4 stack enabled in a PMIPv6 domain. PMIPv6 can provide IPv4 home address mobility support [RFC5844]. IPv4 multicast is handled by an IGMP proxy function at the MAG in an analogous way.

Following these deployment steps, multicast traffic distribution transparently inter-operates with PMIPv6. It is worth noting that an MN - while being attached to the same MAG as the mobile source, but associated with a different LMA - cannot receive multicast traffic on a shortest path. Instead, multicast streams flow up to the LMA of the mobile source, are transferred to the LMA of the mobile listener and tunneled downwards to the MAG again (see Appendix B for further considerations).

### 3.2. Base Solution for Source Mobility: Details

Incorporating multicast source mobility in PMIPv6 requires to deploy general multicast functions at PMIPv6 routers and to define their interaction with the PMIPv6 protocol in the following way.

#### 3.2.1. Operations of the Mobile Node

A Mobile Node willing to send multicast data will proceed as if attached to the fixed Internet. No specific mobility or other multicast related functionalities are required at the MN.

#### 3.2.2. Operations of the Mobile Access Gateway

A Mobile Access Gateway is required to have MLD proxy instances deployed, one for each tunnel to an LMA, which serves as its unique upstream link (cf., [RFC6224]). On the arrival of an MN, the MAG decides on the mapping of downstream links to a proxy instance and the upstream link to the LMA based on the regular Binding Update List as maintained by PMIPv6 standard operations. When multicast data is received from the MN, the MAG MUST identify the corresponding proxy instance from the incoming interface and forwards multicast data upstream according to [RFC4605].

The MAG MAY apply special admission control to enable multicast data transition from an MN. It is advisable to take special care that MLD proxy implementations do not redistribute multicast data to downstream interfaces without appropriate subscriptions in place.

#### 3.2.3. Operations of the Local Mobility Anchor

For any MN, the Local Mobility Anchor acts as the persistent Home Agent and at the same time as the default multicast upstream for the corresponding MAG. It will manage and maintain a multicast forwarding information base for all group traffic arriving from its mobile sources. It SHOULD participate in multicast routing functions that enable traffic redistribution to all adjacent LMAs within the PMIPv6 domain and thereby ensure a continuous receptivity while the source is in motion.

##### 3.2.3.1. Local Mobility Anchors Operating PIM

Local Mobility Anchors that operate the PIM-SM routing protocol [RFC4601] will require sources to be directly connected for sending PIM registers to the RP. This does not hold in a PMIPv6 domain, as MAGs are routers intermediate to MN and the LMA. In this sense, MNs are multicast sources external to the PIM-SM domain.

To mitigate this incompatibility common to all subsidiary MLD proxy domains, the LMA should act as a PIM Border Router and activate the Border-bit. In this case, the `DirectlyConnected(S)` is treated as being TRUE for mobile sources and the PIM-SM forwarding rule "`iif == RPF_interface(S)`" is relaxed to be TRUE, as the incoming tunnel interface from MAG to LMA is considered as not part of the PIM-SM component of the LMA (see A.1 of [RFC4601] ).

In addition, an LMA serving as PIM Designated Router is connected to MLD proxies via individual IP-tunnel interfaces and will experience changing PIM source states on handover. As the incoming interface connects to a point-to-point link, PIM Assert contention is not active, and incoming interface validation is only performed by RPF checks. Consequently, a PIM DR should update incoming source states, as soon as RPF inspection succeeds, i.e., after PMIPv6 forwarding state update. Consequently, PIM routers SHOULD be able to manage these state changes, but some implementations are expected to incorrectly refuse packets until the previous state has timed out.

Notably, running BIDIR PIM [RFC5015] on LMAs remains robust with respect to source location and does not require special configurations or state management for sources.

#### 3.2.4. IPv4 Support

An MN in a PMIPv6 domain may use an IPv4 address transparently for communication as specified in [RFC5844]. For this purpose, an LMA can register an IPv4-Proxy-CoA in its Binding Cache and the MAG can provide IPv4 support in its access network. Correspondingly, multicast membership management will be performed by the MN using IGMP. For multicast support on the network side, an IGMP proxy function needs to be deployed at MAGs in exactly the same way as for IPv6. [RFC4605] defines IGMP proxy behaviour in full agreement with IPv6/MLD. Thus IPv4 support can be transparently provided following the obvious deployment analogy.

For a dual-stack IPv4/IPv6 access network, the MAG proxy instances SHOULD choose multicast signaling according to address configurations on the link, but MAY submit IGMP and MLD queries in parallel, if needed. It should further be noted that the infrastructure cannot identify two data streams as identical when distributed via an IPv4 and IPv6 multicast group. Thus duplicate data may be forwarded on a heterogeneous network layer.

A particular note is worth giving the scenario of [RFC5845] in which overlapping private address spaces of different operators can be hosted in a PMIP domain by using GRE encapsulation with key identification. This scenario implies that unicast communication in

the MAG-LMA tunnel can be individually identified per MN by the GRE keys. This scenario still does not impose any special treatment of multicast communication for the following reasons.

Multicast streams from and to MNs arrive at a MAG on point-to-point links (identical to unicast). Multicast data transmission from the MAG to the corresponding LMA is link-local between the routers and routing/forwarding remains independent of any individual MN. So the MAG-proxy and the LMA SHOULD NOT use GRE key identifiers, but plain GRE encapsulation in multicast communication (including MLD queries and reports). Multicast traffic sent upstream and downstream of MAG-to-LMA tunnels proceeds as router-to-router forwarding according to the multicast routing information base (MRIB) of the MAG or LMA and independent of MN's unicast addresses, while the MAG proxy instance re-distributes multicast data down the point-to-point links (interfaces) according to its own MRIB, independent of MN's IP addresses.

#### 3.2.5. Efficiency of the Distribution System

The distribution system of the base solution directly follows PMIPv6 routing rules, and organizes multicast domains with respect to LMAs. Thus, no coordination between address spaces or services is required between the different instances, provided their associated LMAs belong to disjoint multicast domains. Routing is optimal for communication between MNs of the same domain, or stationary subscribers.

In the following efficiency-related issues remain.

**Multicast reception at LMA** In the current deployment scenario, the LMA will receive all multicast traffic originating from its associated MNs. There is no mechanism to suppress upstream forwarding in the absence of receivers.

**MNs on the same MAG using different LMAs** For a mobile receiver and a source that use different LMAs, the traffic has to go up to one LMA, cross over to the other LMA, and then be tunneled back to the same MAG, causing redundant flows in the access network and at the MAG.

#### 4. Direct Multicast Routing

There are deployment scenarios, where multicast services are available throughout the access network independent of the PMIPv6 routing system [I-D.ietf-multimob-pmipv6-ropt]. In these cases, the visited networks grant a local content distribution service (in



contrast to LMA-based home subscription) with locally optimized traffic flows. It is also possible to deploy a mixed service model of local and LMA-based subscriptions, provided a unique way of service selection is implemented. For example, access routers (MAGs) could decide on service access based on the multicast address G or the SSM channel (S,G) under request (see Section 5 for a further discussion).

#### 4.1. Overview

Direct multicast access can be supported by

- o native multicast routing provided by one multicast router that is neighboring MLD proxies deployed at MAGs within a flat access network, or via tunnel uplinks,
- o a multicast routing protocol such as PIM-SM [RFC4601] or BIDIR-PIM [RFC5015] deployed at the MAGs.

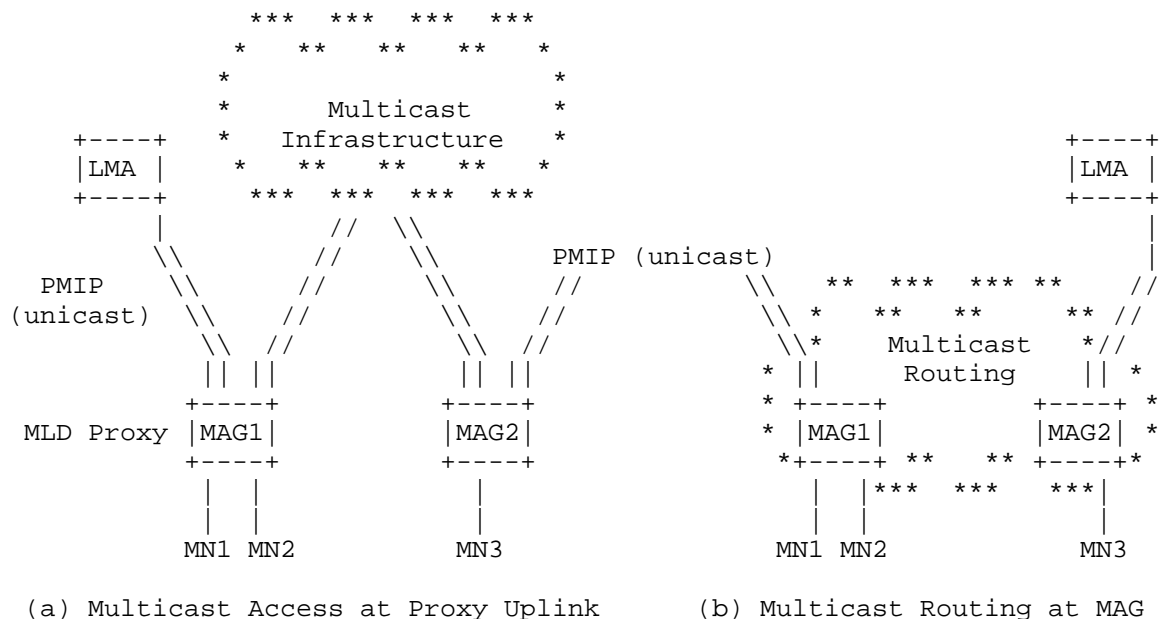


Figure 3: Reference Networks for (a) Proxy-assisted Direct Multicast Access and (b) Dynamic Multicast Routing at MAGs

Figure 3 displays the corresponding deployment scenarios, which separate multicast from PMIPv6 unicast routing. It is assumed throughout these scenarios that all MAGs (MLD proxies) are linked to

a single multicast routing domain. Noteworthy, this scenario requires coordination of multicast address utilization and service bindings.

Multicast traffic distribution can be simplified in these scenarios. A single proxy instance at MAGs with up-link into the multicast domain will serve as a first hop multicast gateway and avoid traffic duplication or detour routing. Multicast routing functions at MAGs will seamlessly embed access gateways within a multicast cloud. However, mobility of the multicast source in this scenario will require some multicast routing protocols to rebuild distribution trees. This can cause significant service disruptions or delays (see [RFC5757] for further aspects). Deployment details are specific to the multicast routing protocol in use, in the following described for common protocols.

#### 4.2. MLD Proxies at MAGs

In a PMIPv6 domain, single MLD proxy instances can be deployed at each MAG that enable multicast service at the access via an uplink to a multicast service infrastructure (see Figure 3 (a) ). To avoid service disruptions on handovers, the uplinks of all proxies SHOULD be adjacent to the same next-hop multicast router. This can either be achieved by arranging proxies within a flat access network, or by upstream tunnels that terminate at a common multicast router.

Multicast data submitted by a mobile source will reach the MLD proxy at the MAG that subsequently forwards flows to the upstream, and all downstream interfaces with appropriate subscriptions. Traversing the upstream will lead traffic into the multicast infrastructure (e.g., to a PIM Designated Router) which will route packets to all local MAGs that have joined the group, as well as further upstream according to protocol procedures and forwarding states.

On handover, a mobile source will reattach at a new MAG and can continue to send multicast packets as soon as PMIPv6 unicast configurations have completed. Like at the previous MAG, the new MLD proxy will forward data upstream and downstream to subscribers. Listeners local to the previous MAG will continue to receive group traffic via the local multicast distribution infrastructure following aggregated listener reports of the previous proxy. In general, traffic from the mobile source continues to be transmitted via the same next-hop router using the same source address and thus remains unchanged when seen from the wider multicast infrastructure.

#### 4.2.1. Considerations for PIM-SM on the Upstream

A mobile source that transmits data via an MLD proxy will not be directly connected to a PIM Designated Router as discussed in Section 3.2.3.1. Countermeasures apply correspondingly.

A PIM Designated Router that is connected to MLD proxies via individual IP-tunnel interfaces will experience invalid PIM source states on handover. In some implementations of PIM-SM this could lead to interim packet loss (see Section Section 3.2.3.1). This problem can be mitigated by aggregating proxies on a lower layer.

#### 4.2.2. SSM Considerations

Source-specific subscriptions invalidate with routes, whenever the source moves from or to the MAG/proxy of a subscriber. Multicast forwarding states will rebuild with unicast route changes. However, this may lead to noticeable service disruptions for locally subscribed nodes.

#### 4.3. PIM-SM

The full-featured multicast routing protocol PIM-SM MAY be deployed in the access network for providing multicast services in parallel to unicast routes. Throughout this section, it is assumed that the PMIPv6 mobility domain is part of a single PIM-SM multicast routing domain with PIM-SM routing functions present at all MAGs and all LMAs. The PIM routing instance at a MAG SHALL then serve as the Designated Router (DR) for all directly attached Mobile Nodes. For expediting handover operations, it is advisable to position PIM Rendezvous Points (RPs) in the core of the PMIPv6 network domain. However, regular IP routing tables need not be present in a PMIPv6 deployment, and additional effort is required to establish reverse path forwarding rules as required by PIM-SM.

##### 4.3.1. Routing Information Base for PIM-SM

In this scenario, PIM-SM will rely on a Multicast Routing Information Base (MRIB) that is generated independently of the policy-based routing rules of PMIPv6. The granularity of mobility-related routing locators required in PIM depends on the complexity (phases) of its deployment.

The following information is needed for all phases of PIM.

- o All routes to networks and nodes (including RPs) that are not mobile members of the PMIPv6 domain MUST be defined consistently among PIM routers and remain unaffected by node mobility. The

setup of these general routes is expected to follow the topology of the operator network and is beyond the scope of this document.

The following route entries are required at a PIM-operating MAG when phases two or three of PIM, or PIM-SSM are in operation.

- o All MNs that are directly attached to the MAG generate local routes to their Home Network Prefixes (HNPs) at the corresponding point-to-point attachments that **MUST** be included into the local MRIB.
- o All routes to MNs that are attached to distant MAGs of the PMIPv6 domain point towards their corresponding LMAs. These routes **MUST** be made available in the MRIB of all PIM routers (except for the local MAG of attachment), but **MAY** be eventually expressed by an appropriate default entry.

#### 4.3.2. Operations of PIM in Phase One

A new mobile source *S* will transmit multicast data of group *G* towards its MAG of attachment. Acting as a PIM DR, the access gateway will unicast-encapsulate the multicast packets and forward the data to the Virtual Interface (VI) with encapsulation target *RP(G)*, a process known as PIM source registering. The RP will decapsulate and natively forward the packets down the RP-based distribution tree towards (mobile and stationary) subscribers.

On handover, the point-to-point link connecting the mobile source to the old MAG will go down and all (*S*,*) flows terminate. In response, the previous DR (MAG) deactivates the data encapsulation channels for the transient source (e.g., all *DownstreamJPState(S,*,VI)* are set to NoInfo state). After reattaching and completing unicast handover negotiations, the mobile source can continue to transmit multicast packets, while being treated as a new source at its new DR (MAG). Source register encapsulation will be immediately initiated, and (*S,G*) data continue to flow natively down the (*,*G*) RP-based tree.

Source handover management in PIM phase one admits low complexity and remains transparent to receivers. In addition, the source register tunnel management of PIM is a fast protocol operation and little overhead is induced thereof. In a PMIPv6 deployment, PIM RPs **MAY** be configured to not initiate (*S,G*) shortest path trees for mobile sources, and thus remain in phase one of the protocol. The price to pay for such simplified deployment lies in possible routing detours by an overall RP-based packet distribution.

#### 4.3.3. Operations of PIM in Phase Two

After receiving source register packets, a PIM RP eventually will initiate a source-specific Join for creating a shortest path tree to the (mobile) source S, and issue a source register stop at the native arrival of data from S. For initiating an (S,G) tree, the RP, as well as all intermediate routers, require route entries for MN's HNP that - unless the RP coincides with the MAG of S - point towards the corresponding LMA of S. Consequently, the (S,G) tree will proceed from the RP via the (stable) LMA, the LMA-MAG tunnel to the mobile source. This tree can be of lesser routing efficiency than the PIM source register tunnel established in phase one, but provides the advantage of immediate data delivery to receivers that share a MAG with S.

On handover, the mobile source reattaches to a new MAG (DR), and PMIPv6 unicast management will transfer the LMA-MAG tunnel to the new point of attachment. However, in the absence of a corresponding multicast forwarding state, the new DR will treat S as a new source and initiate a source registering of PIM phase one with the RP. In response, the PIM RP will recognize the known source at a new (tunnel) interface. A PIM RP implementation compliant with this change can proceed as follows. The RP immediately responds with a register stop, when it receives a register from the new MAG. As the RP had joined the shortest path tree to receive from the source via the LMA, the tree is persistently updated by joins transmitted towards the new MAG on a path via the LMA. In proceeding this way, a quick recovery of PIM transition from phase one to two will be performed per handover.

#### 4.3.4. Operations of PIM in Phase Three

In response to an exceeded threshold of packet transmission, DRs of receivers eventually will initiate a source-specific Join for creating a shortest path tree to the (mobile) source S, thereby transitioning PIM into the final short-cut phase three. For all receivers not sharing a MAG with S, this (S,G) tree will proceed from the receiving DR via the (stable) LMA, the LMA-MAG tunnel to the mobile source. This tree is of higher routing efficiency than established in the previous phase two, but need not outperform the PIM source register tunnel established in phase one. It provides the advantage of immediate data delivery to receivers that share a MAG with S.

On handover, the mobile source reattaches to a new MAG (DR), and PMIPv6 unicast management will transfer the LMA-MAG tunnel to the new point of attachment. However, in the absence of a corresponding multicast forwarding state, the new DR will treat S as a new source

and initiate a source registering of PIM phase one. A PIM implementation compliant with this change can recover phase three states in the following way. First, the RP recovers to phase two as described in the previous section, but - being unaware of the LMA in the role of a static mobility anchor - needs to forward data packets that arrived via the source register tunnel down the RP-base tree towards receivers. Such packets will trigger updates of phase three shortest path trees at the DRs of the receivers. Meanwhile packets arriving at the LMA without source register encapsulation are forwarded natively along the shortest path tree towards receivers.

In consequence, the PIM transition from phase one to two and three will be quickly recovered per handover, but still leads to an enhanced signaling load and repeated delay variations.

#### 4.3.5. PIM-SSM Considerations

Source-specific Joins of receivers will guide PIM to operate in SSM mode and lead to an immediate establishment of source-specific shortest path trees. Such (S,G) trees will equal the distribution system of PIM's final phase three (see Section 4.3.4). However, on handover and in the absence of RP-based data distribution, SSM data delivery cannot be resumed via source registering as in PIM phase one. Consequently, data packets transmitted after a handover will be discarded at the MAG until regular tree maintenance has re-established the (S,G) forwarding state at the new MAG.

#### 4.3.6. Handover Optimizations for PIM

Source-specific shortest path trees are constructed in PIM-SM (phase two and three), and in PIM-SSM that follow LMA-MAG tunnels towards a source. As PIM remains unaware of source mobility management, these trees invalidate under handovers with each tunnel re-establishment at a new MAG. Regular tree maintenance of PIM will recover the states, but remains unsynchronized and too slow to seamlessly preserve PIM data dissemination.

A method to quickly recover PIM (S,G) trees under handover SHOULD synchronize multicast state maintenance with unicast handover operations and MAY proceed as follows. On handover, an LMA reads all (S,G) Join states from its corresponding tunnel interface and identifies those source addresses  $S_i$  that match moving HNPs. After re-establishing the new tunnel, it SHOULD associate the  $(S_i,*)$  Join states with the new tunnel endpoint and immediately trigger a state maintenance (PIM Join) message. In proceeding this way, the source-specific PIM states are transferred to the new tunnel end point and propagated to the new MAG in synchrony with unicast handover procedures.

#### 4.4. BIDIR-PIM

BIDIR-PIM MAY be deployed in the access network for providing multicast services in parallel to unicast routes. Throughout this section, it is assumed that the PMIPv6 mobility domain is part of a single BIDIR-PIM multicast routing domain with BIDIR-PIM routing functions present at all MAGs and all LMAs. The PIM routing instance at a MAG SHALL then serve as the Designated Forwarder (DF) for all directly attached Mobile Nodes. For expediting handover operations, it is advisable to position BIDIR-PIM Rendezvous Point Addresses (RPAs) in the core of the PMIPv6 network domain. As regular IP routing tables need not be present in a PMIPv6 deployment, reverse path forwarding rules as required by BIDIR-PIM need to be established.

##### 4.4.1. Routing Information Base for BIDIR-PIM

In this scenario, BIDIR-PIM will rely on a Multicast Routing Information Base (MRIB) that is generated independently of the policy-based routing rules of PMIPv6. The following information is needed.

- o All routes to networks and nodes (including RPAs) that are not mobile members of the PMIPv6 domain MUST be defined consistently among BIDIR-PIM routers and remain unaffected by node mobility. The setup of these general routes is expected to follow the topology of the operator network and is beyond the scope of this document.

##### 4.4.2. Operations of BIDIR-PIM

BIDIR-PIM will establish spanning trees across its network domain in conformance to its preconfigured RPAs and the routing information provided. Multicast data transmitted by a mobile source will immediately be forwarded by its DF (MAG) onto the spanning group tree without further protocol operations.

On handover, the mobile source re-attaches to a new MAG (DF), which completes unicast network configurations. Thereafter, the source can immediately proceed with multicast packet transmission onto the pre-established distribution tree. BIDIR-PIM does neither require protocol signaling nor additional reconfiguration delays to adapt to source mobility and can be considered the protocol of choice for mobile multicast operations in the access. As multicast streams always flow up to the Rendezvous Point Link, some care should be taken to configure RPAs compliant with network capacities.

## 5. Extended MLD Proxy Function for Optimized Source Mobility in PMIPv6

A deployment of MLD Proxies (see [RFC4605]) at MAGs has proven a useful and appropriate approach to multicast in PMIPv6, see [RFC6224], [I-D.ietf-multimob-pmipv6-ropt]. However, deploying unmodified standard proxies can go along with significant performance degradation for mobile senders as discussed along the lines of this document. To overcome these deficits, an optimized approach to multicast source mobility based on extended peering functions among proxies is introduced in this section. Prior to presenting the solution, we will sketch the relevant requirements.

Solutions that extend MLD Proxies by additional uplinking functions need to comply to the following requirements.

**Prevention of Routing Loops** In the absence of a full-featured routing logic at an MLD Proxy, simple and locally decidable rules need to prevent source traffic from traversing the network in loops as potentially enabled by multiple uplinks.

**Unique coverage of receivers** Listener functions at Proxies require simple, locally decidable rules to initiate a unique delivery of multicast packets to all receivers.

Following different techniques, these requirements are met in the following solutions.

### 5.1. Peering Function for MLD Proxies

In this section, we define a peering interface for MLD proxies that allows for a direct data exchange of locally attached multicast sources. Such peering interfaces can be configured - as a direct link or a bidirectional tunnel - between any two proxy instances (locally deployed as in [RFC6224] or remotely) and remain as silent virtual links in regular proxy operations. Data on such link is exchanged only in cases, where one peering proxy directly connects on the downstream to a source of multicast traffic, which the other peering proxy actively subscribes to. Operations are defined for ASM and SSM, but provide superior performance in the presence of source-specific signaling (IGMPv3/MLDv2).

#### 5.1.1. Operations at the Multicast Sender

An MLD Proxy in the perspective of a sender will see peering interfaces as restricted downstream interfaces. It will install and maintain source filters at its peering links that will restrict data transmission to those packets that originate from a locally attached source at the downstream. In detail, a proxy will extract from its



configuration the network prefixes attached to its downstream interfaces and MUST implement a source filter base at its peering interfaces that restricts data transmission to IP source addresses from its local prefixes. This filter base Must be updated, if and only if the downstream configuration changes. In this way, a multihop forwarding on peering links is prevented. Multicast packets that arrive from the upstream interface of the proxy are thus only forwarded to regular downstream interfaces with appropriate subscription states.

Multicast traffic arriving from a locally attached source will be forwarded to the regular upstream interface and all downstreams with appropriate subscription states (i.e., regular Proxy operations). In addition, local multicast packets are transferred to those peering interfaces with appropriate subscription states.

#### 5.1.2. Operations at the Multicast Listener

From the listener side, peering interfaces appear as preferred upstream links. Thus an MLD proxy with peering interconnects will offer several interfaces for pulling remote traffic: the regular upstream and the peerings. Traffic arriving from any of the peering links will be mutually disjoint, but normally also available from the upstream. To prevent duplicate traffic from arriving at the listener side, the proxy

- o MAY delay aggregated reports to the upstream, and
- o MUST apply appropriate filters to exclude duplicate streams.

In detail, it first issues listener reports (in parallel) to its peering links, which only span one (virtual) hop. Whenever the expected traffic (e.g., SSM channels) does not completely arrive from the peerings after a waiting time (default: 10 ms), additional (complementary, in the case of SSM) reports are sent to the standard upstream interface.

After the arrival of traffic from peering links, an MLD proxy MUST install source filters at the upstream in the following way.

ASM with IGMPv2/MLDv1 In the presence of Any Source Multicast using IGMPv2/MLDv1, only, the proxy cannot signal source filtering to its upstream. Correspondingly, it applies (S,*) ingress filters at its upstream interface for all sources S seen in traffic of the peering links. It is noteworthy that unwanted traffic is still replicated to the proxy via the access network.

ASM with IGMPv3/MLDv2 In the presence of source-specific signaling (IGMPv3/MLDv2), the upstream interface is set to (S,*) exclude mode for all sources S seen in traffic of the peering links. The corresponding source-specific signaling will prevent duplicate traffic forwarding throughout the access network.

SSM In the presence of Source Specific Multicast, the proxy will subscribe on its uplink interface to those (S,G) channels, only, that do not arrive via the peering links.

In proceeding this way, multicast group data arrive from peering interfaces first, while only peer-wise unavailable traffic is retrieved from the regular upstream interface.

## 6. IANA Considerations

TODO.

Note to RFC Editor: this section may be removed on publication as an RFC.

## 7. Security Considerations

TODO

Consequently, no new threats are introduced by this document in addition to those identified as security concerns of [RFC3810], [RFC4605], [RFC5213], and [RFC5844].

However, particular attention should be paid to implications of combining multicast and mobility management at network entities. As this specification allows mobile nodes to initiate the creation of multicast forwarding states at MAGs and LMAs while changing attachments, threats of resource exhaustion at PMIP routers and access networks arrive from rapid state changes, as well as from high volume data streams routed into access networks of limited capacities. In addition to proper authorization checks of MNs, rate controls at replicators MAY be required to protect the agents and the downstream networks. In particular, MLD proxy implementations at MAGs SHOULD carefully procure for automatic multicast state extinction on the departure of MNs, as mobile multicast listeners in the PMIPv6 domain will not actively terminate group membership prior to departure.

## 8. Acknowledgements

The authors would like to thank (in alphabetical order) Luis M. Contreras, Muhamma Omer Farooq, Bohao Feng, Dirk von Hugo, Ning Kong, Jouni Korhonen, He-Wu Li, Akbar Rahman, Stig Venaas, Li-Li Wang, Qian Wu, Zhi-Wei Yan for advice, help and reviews of the document. Funding by the German Federal Ministry of Education and Research within the G-LAB Initiative (project HAMcast) is gratefully acknowledged.

## 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.
- [RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.
- [RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.
- [RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.
- [RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.
- [RFC4605] Fenner, B., He, H., Haberman, B., and H. Sandick, "Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")", RFC 4605, August 2006.
- [RFC5015] Handley, M., Kouvelas, I., Speakman, T., and L. Vicisano, "Bidirectional Protocol Independent Multicast (BIDIR-PIM)", RFC 5015, October 2007.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.

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

## 9.2. Informative References

- [I-D.ietf-multimob-pmipv6-ropt]  
Zuniga, J., Contreras, L., Bernardos, C., Jeon, S., and Y. Kim, "Multicast Mobility Routing Optimizations for Proxy Mobile IPv6", draft-ietf-multimob-pmipv6-ropt-03 (work in progress), February 2013.
- [RFC2236] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.
- [RFC5757] Schmidt, T., Waehlich, M., and G. Fairhurst, "Multicast Mobility in Mobile IP Version 6 (MIPv6): Problem Statement and Brief Survey", RFC 5757, February 2010.
- [RFC5845] Muhanna, A., Khalil, M., Gundavelli, S., and K. Leung, "Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6", RFC 5845, June 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.

## Appendix A. Multiple Upstream Interface Proxy

In this section, we document upstream extensions for an MLD proxy that were originally developed during the work on this document. Multiple proxy instances deployed at a single MAG (see Section 3) can be avoided by adding multiple upstream interfaces to a single MLD Proxy. In a typical PMIPv6 deployment, each upstream of a single proxy instance can interconnect to one of the LMAs. With such ambiguous upstream options, appropriate forwarding rules MUST be supplied to

- o unambiguously guide traffic forwarding from directly attached mobile sources, and
- o lead listener reports to initiating unique traffic subscriptions.

This can be achieved by a complete set of source- and group-specific filter rules (e.g., (S,*), (*,G)) installed at proxy interfaces. These filters MAY be derived in parts from PMIPv6 routing policies, and can include a default behavior (e.g., (*,*)).

### A.1. Operations for Local Multicast Sources

Packets from a locally attached multicast source will be forwarded to all downstream interfaces with appropriate subscriptions, as well as up the interface with the matching source-specific filter.

Typically, the upstream interface for a mobile multicast source is chosen based on the policy routing (e.g., the MAG-LMA tunnel interface for LMA-based routing or the interface towards the multicast router for direct routing), but alternate configurations MAY be applied. Packets from a locally attached multicast source will be forwarded to the corresponding upstream interface with the matching source-specific filter, as well as all the downstream interfaces with appropriate subscriptions.

### A.2. Operations for Local Multicast Subscribers

Multicast listener reports are group-wise aggregated by the MLD proxy. The aggregated report is issued to the upstream interface with matching group/channel-specific filter. The choice of the corresponding upstream interface for aggregated group membership reports MAY be additionally based on some administrative scoping rules for scoped multicast group addresses.

In detail, a Multiple Upstream Interface Proxy will provide and maintain a Multicast Subscription Filter Table that maps source- and group-specific filters to upstream interfaces. The forwarding decision for an aggregated MLD listener report is based on the first matching entry from this table, with the understanding that for IGMPv3/MLDv2 the MLD Proxy performs a state decomposition, if needed (i.e., a (*,G) subscription is split into (S,G) and (* \ S,G) in the presence of (*,G) after (S,G) interface entries), and that (S,*)-filters are always false in the absence of source-specific signaling, i.e. in IGMPv2/MLDv1 only domains.

In typical deployment scenarios, specific group services (channels) could be either associated with selected uplinks to remote LMAs, while a (*,*) default subscription entry (in the last table line) is bound to a local routing interface, or selected groups are configured as local services first, while a (*,*) default entry (in the last table line) points to a remote uplink that provides the general multicast support.

## Appendix B. Evaluation of Traffic Flows

TODO

## Appendix C. Change Log

The following changes have been made from version draft-ietf-multimob-pmipv6-source-02:

1. Added clarifications and details as requested by the working group, resolved nits.
2. Moved Multiple Upstream MLD Proxy to Appendix in response to WG desire.
3. Updated references.

The following changes have been made from version draft-ietf-multimob-pmipv6-source-01:

1. Added clarifications and details as requested by the working group, resolved nits.
2. Detailed out operations of Multiple Upstream MLD Proxies.
3. Clarified operations of MLD proxies with peering links.
4. Many editorial improvements.
5. Updated references.

The following changes have been made from version draft-ietf-multimob-pmipv6-source-00:

1. Direct routing with PIM-SM and PIM-SSM has been added.
2. PMIP synchronization with PIM added for improved handover.
3. Direct routing with BIDIR-PIM has been added.
4. MLD Proxy extensions requirements added.
5. Peering of MLD Proxies added.
6. First sketch of multiple upstream proxy added.
7. Editorial improvements.
8. Updated references.

## Authors' Addresses

Thomas C. Schmidt (editor)  
HAW Hamburg  
Berliner Tor 7  
Hamburg 20099  
Germany

Email: [schmidt@informatik.haw-hamburg.de](mailto:schmidt@informatik.haw-hamburg.de)  
URI: <http://inet.cpt.haw-hamburg.de/members/schmidt>

Shuai Gao  
Beijing Jiaotong University  
Beijing,  
China

Phone:  
Fax:  
Email: [shgao@bjtu.edu.cn](mailto:shgao@bjtu.edu.cn)  
URI:

Hong-Ke Zhang  
Beijing Jiaotong University  
Beijing,  
China

Phone:  
Fax:  
Email: [hkzhang@bjtu.edu.cn](mailto:hkzhang@bjtu.edu.cn)  
URI:

Matthias Waehlich  
link-lab & FU Berlin  
Hoenower Str. 35  
Berlin 10318  
Germany

Email: [mw@link-lab.net](mailto:mw@link-lab.net)





MULTIMOB Group  
Internet-Draft  
Intended status: Standards Track  
Expires: January 14, 2014

T. Schmidt, Ed.  
HAW Hamburg  
S. Gao  
H. Zhang  
Beijing Jiaotong University  
M. Waehlich  
link-lab & FU Berlin  
July 13, 2013

Mobile Multicast Sender Support in Proxy Mobile IPv6 (PMIPv6) Domains  
draft-ietf-multimob-pmipv6-source-04

Abstract

Multicast communication can be enabled in Proxy Mobile IPv6 domains via the Local Mobility Anchors by deploying MLD Proxy functions at Mobile Access Gateways, via a direct traffic distribution within an ISP's access network, or by selective route optimization schemes. This document describes the support of mobile multicast senders in Proxy Mobile IPv6 domains for all three scenarios. Protocol optimizations for synchronizing PMIPv6 with PIM, as well as a peering function for MLD Proxies defined. Mobile sources always remain agnostic of multicast mobility operations.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

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

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

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

This Internet-Draft will expire on January 14, 2014.

## Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Terminology . . . . .	4
3. Base Solution for Source Mobility and PMIPv6 Routing . . . . .	4
3.1. Overview . . . . .	4
3.2. Base Solution for Source Mobility: Details . . . . .	7
3.2.1. Operations of the Mobile Node . . . . .	7
3.2.2. Operations of the Mobile Access Gateway . . . . .	7
3.2.3. Operations of the Local Mobility Anchor . . . . .	7
3.2.4. IPv4 Support . . . . .	8
3.2.5. Efficiency of the Distribution System . . . . .	9
4. Direct Multicast Routing . . . . .	10
4.1. Overview . . . . .	10
4.2. MLD Proxies at MAGs . . . . .	11
4.2.1. Considerations for PIM-SM on the Upstream . . . . .	12
4.2.2. SSM Considerations . . . . .	12
4.3. PIM-SM at MAGs . . . . .	12
4.3.1. Routing Information Base for PIM-SM . . . . .	12
4.3.2. Operations of PIM in Phase One . . . . .	13
4.3.3. Operations of PIM in Phase Two . . . . .	14
4.3.4. Operations of PIM in Phase Three . . . . .	14
4.3.5. PIM-SSM Considerations . . . . .	15
4.3.6. Handover Optimizations for PIM . . . . .	15
4.4. BIDIR-PIM . . . . .	16
4.4.1. Routing Information Base for BIDIR-PIM . . . . .	16
4.4.2. Operations of BIDIR-PIM . . . . .	16
5. Extended MLD Proxy Function for Optimized Source Mobility in PMIPv6 . . . . .	17
5.1. Peering Function for MLD Proxies . . . . .	17
5.1.1. Operations at the Multicast Sender . . . . .	18
5.1.2. Operations at the Multicast Listener . . . . .	18
6. IANA Considerations . . . . .	19

7. Security Considerations . . . . .	19
8. Acknowledgements . . . . .	20
9. References . . . . .	20
9.1. Normative References . . . . .	20
9.2. Informative References . . . . .	21
Appendix A. Multiple Upstream Interface Proxy . . . . .	21
A.1. Operations for Local Multicast Sources . . . . .	22
A.2. Operations for Local Multicast Subscribers . . . . .	22
Appendix B. Change Log . . . . .	23
Authors' Addresses . . . . .	24

## 1. Introduction

Proxy Mobile IPv6 (PMIPv6) [RFC5213] extends Mobile IPv6 (MIPv6) [RFC6275] by network-based management functions that enable IP mobility for a host without requiring its participation in any mobility-related signaling. Additional network entities called the Local Mobility Anchor (LMA), and Mobile Access Gateways (MAGs), are responsible for managing IP mobility on behalf of the mobile node (MN). An MN connected to a PMIPv6 domain, which only operates according to the base specifications of [RFC5213], cannot participate in multicast communication, as MAGs will discard group packets.

Multicast support for mobile listeners can be enabled within a PMIPv6 domain by deploying MLD Proxy functions at Mobile Access Gateways, and multicast routing functions at Local Mobility Anchors [RFC6224]. This base deployment option is the simplest way to PMIPv6 multicast extensions in the sense that it follows the common PMIPv6 traffic model and neither requires new protocol operations nor additional infrastructure entities. Standard software functions need to be activated on PMIPv6 entities, only, at the price of possibly non-optimal multicast routing.

Alternate solutions leverage performance optimization by providing multicast routing at the access gateways directly, or by selective route optimization schemes. Such approaches (partially) follow the business model of providing multicast data services in parallel to PMIPv6 unicast routing.

Multicast listener support satisfies the needs of receptive use cases such as IPTV or server-centric gaming on mobiles. However, current trends in the Internet enfold towards user-centric, highly interactive group applications like user generated streaming, conferencing, collective mobile sensing, etc. Many of these popular applications create group content at end systems and can largely profit from a direct data transmission to a multicast-enabled network.

This document describes the support of mobile multicast senders in Proxy Mobile IPv6 domains subsequently for the base deployment scenario [RFC6224], for direct traffic distribution within an ISP's access network, as well as for selective route optimization schemes. The contribution of this work reflects the source mobility problem as discussed in [RFC5757]. Mobile Nodes in this setting remain agnostic of multicast mobility operations.

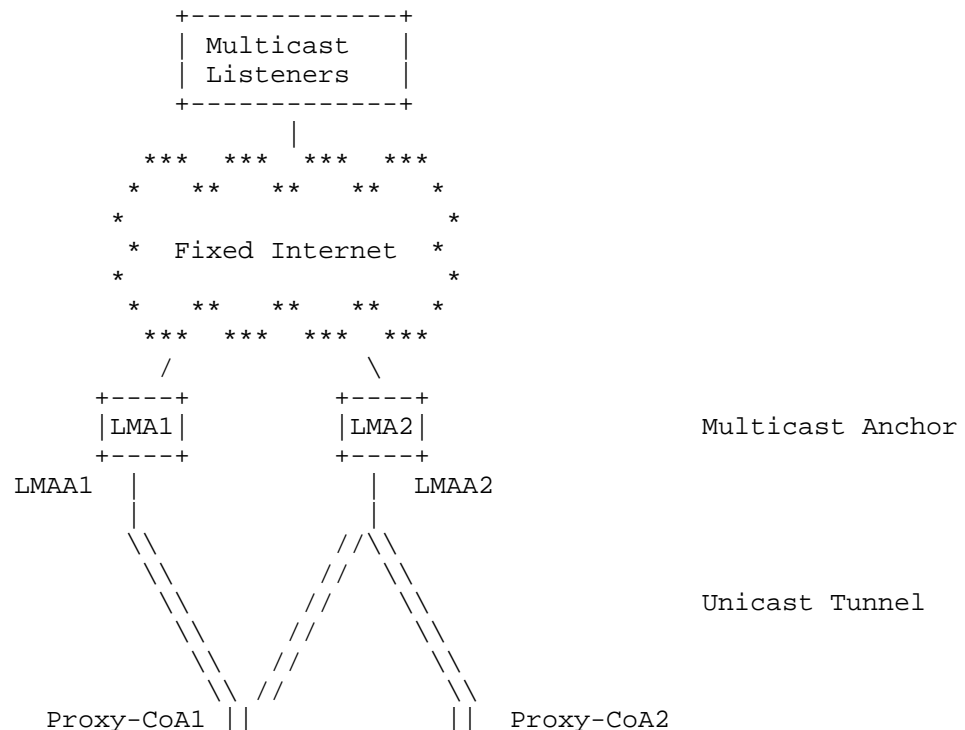
## 2. Terminology

This document uses the terminology as defined for the mobility protocols [RFC6275], [RFC5213] and [RFC5844], as well as the multicast edge related protocols [RFC3376], [RFC3810] and [RFC4605].

## 3. Base Solution for Source Mobility and PMIPv6 Routing

### 3.1. Overview

The reference scenario for multicast deployment in Proxy Mobile IPv6 domains is illustrated in Figure 1. MAGs play the role of first-hop access routers that serve multiple MNs on the downstream while running an MLD/IGMP proxy instance for every LMA upstream tunnel.



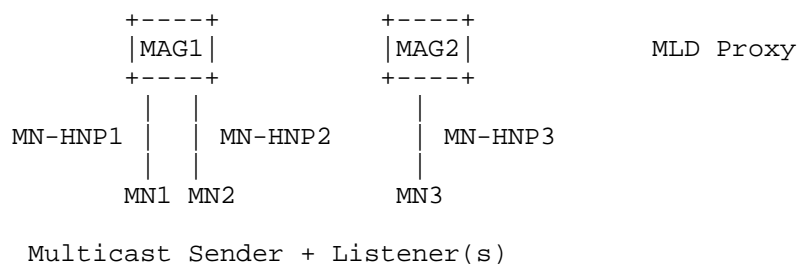


Figure 1: Reference Network for Multicast Deployment in PMIPv6 with Source Mobility

An MN in a PMIPv6 domain will decide on multicast data transmission completely independent of its current mobility conditions. It will send packets as initiated by applications, using its source address with Home Network Prefix (HNP) and a multicast destination address chosen by application needs. Multicast packets will arrive at the currently active MAG via one of its downstream local (wireless) links. A multicast unaware MAG would simply discard these packets in the absence of a multicast routing information base (MRIB).

An MN can successfully distribute multicast data in PMIPv6, if MLD proxy functions are deployed at the MAG as described in [RFC6224]. In this set-up, the MLD proxy instance serving a mobile multicast source has configured its upstream interface at the tunnel towards MN's corresponding LMA. For each LMA, there will be a separate instance of an MLD proxy.

According to the specifications given in [RFC4605], multicast data arriving from a downstream interface of an MLD proxy will be forwarded to the upstream interface and to all but the incoming downstream interfaces that have appropriate forwarding states for this group. Thus multicast streams originating from an MN will arrive at the corresponding LMA and directly at all mobile receivers co-located at the same MAG and MLD Proxy instance. Serving as the designated multicast router or an additional MLD proxy, the LMA forwards data to the fixed Internet, whenever forwarding states are maintained by multicast routing. If the LMA is acting as another MLD proxy, it will forward the multicast data to its upstream interface, and to downstream interfaces with matching subscriptions, accordingly.

In case of a handover, the MN (unaware of IP mobility) can continue to send multicast packets as soon as network connectivity is reconfigured. At this time, the MAG has determined the corresponding LMA, and IPv6 unicast address configuration (including PMIPv6 bindings) has been completed. Still multicast packets arriving at

the MAG are discarded (if not buffered) until the MAG has completed the following steps.

1. The MAG has determined that the MN is admissible to multicast services.
2. The MAG has added the new downstream link to the MLD proxy instance with up-link to the corresponding LMA.

As soon as the MN's uplink is associated with the corresponding MLD proxy instance, multicast packets are forwarded again to the LMA and eventually to receivers within the PMIP domain (see the call flow in Figure 2). In this way, multicast source mobility is transparently enabled in PMIPv6 domains that deploy the base scenario for multicast.

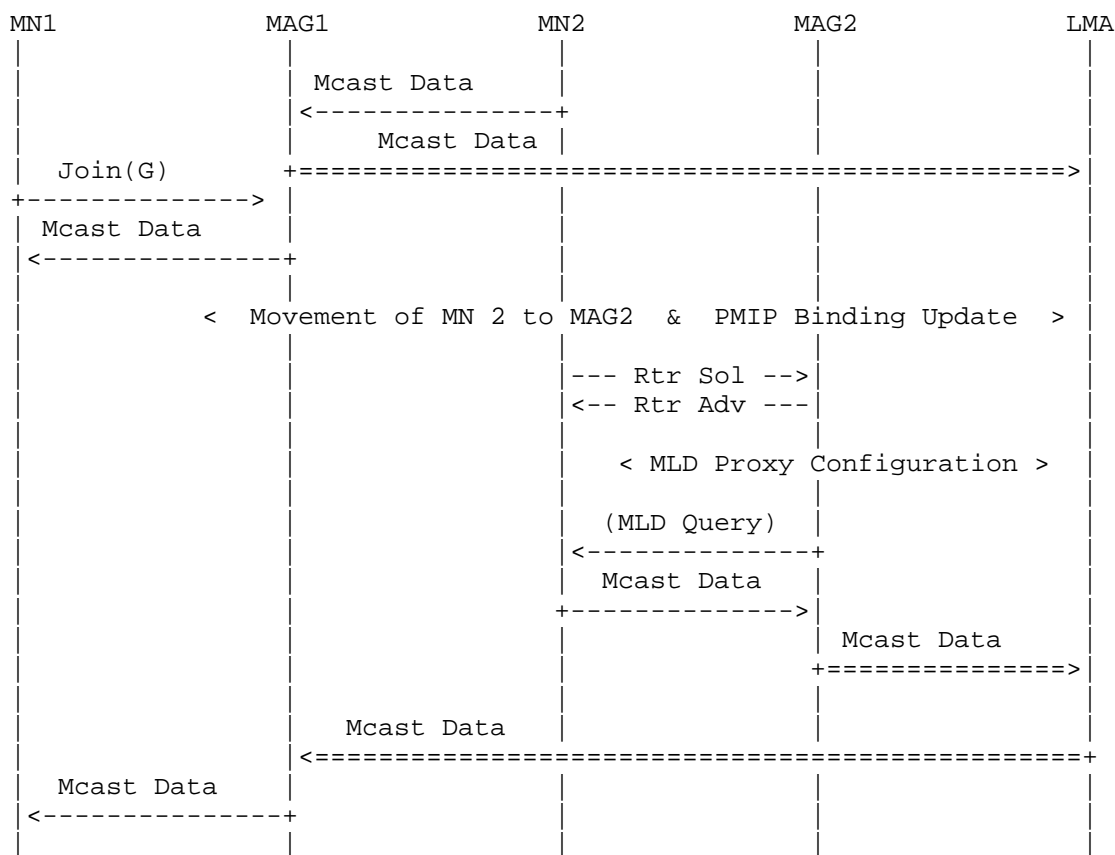


Figure 2: Call Flow for Group Communication in Multicast-enabled PMIP

These multicast deployment considerations likewise apply for mobile nodes that operate with their IPv4 stack enabled in a PMIPv6 domain. PMIPv6 can provide IPv4 home address mobility support [RFC5844]. IPv4 multicast is handled by an IGMP proxy function at the MAG in an analogous way.

Following these deployment steps, multicast traffic distribution transparently inter-operates with PMIPv6. It is worth noting that an MN - while being attached to the same MAG as the mobile source, but associated with a different LMA - cannot receive multicast traffic on a shortest path. Instead, multicast streams flow up to the LMA of the mobile source, are transferred to the LMA of the mobile listener and tunneled downwards to the MAG again (see Section 5 for further optimizations).

### 3.2. Base Solution for Source Mobility: Details

A support of multicast source mobility in PMIPv6 requires to deploy general multicast functions at PMIPv6 routers and to define their interaction with the PMIPv6 protocol in the following way.

#### 3.2.1. Operations of the Mobile Node

A Mobile Node willing to send multicast data will proceed as if attached to the fixed Internet. No specific mobility or other multicast related functionalities are required at the MN.

#### 3.2.2. Operations of the Mobile Access Gateway

A Mobile Access Gateway is required to have MLD proxy instances deployed, one for each tunnel to an LMA, which serves as its unique upstream link (cf., [RFC6224]). On the arrival of an MN, the MAG decides on the mapping of downstream links to a proxy instance and the upstream link to the LMA based on the regular Binding Update List as maintained by PMIPv6 standard operations. When multicast data is received from the MN, the MAG MUST identify the corresponding proxy instance from the incoming interface and forwards multicast data upstream according to [RFC4605].

The MAG MAY apply special admission control to enable multicast data transition from an MN. It is advisable to take special care that MLD proxy implementations do not redistribute multicast data to downstream interfaces without appropriate subscriptions in place.

#### 3.2.3. Operations of the Local Mobility Anchor

For any MN, the Local Mobility Anchor acts as the persistent Home Agent and at the same time as the default multicast upstream for the

corresponding MAG. It will manage and maintain a multicast forwarding information base for all group traffic arriving from its mobile sources. It SHOULD participate in multicast routing functions that enable traffic redistribution to all adjacent LMAs within the PMIPv6 domain and thereby ensure a continuous receptivity while the source is in motion.

#### 3.2.3.1. Local Mobility Anchors Operating PIM

Local Mobility Anchors that operate the PIM-SM routing protocol [RFC4601] will require sources to be directly connected for sending PIM registers to the RP. This does not hold in a PMIPv6 domain, as MAGs are routers intermediate to MN and the LMA. In this sense, MNs are multicast sources external to the PIM-SM domain.

To mitigate this incompatibility common to all subsidiary MLD proxy domains, the LMA MUST act as a PIM Border Router and activate the Border-bit. In this case, the `DirectlyConnected(S)` is treated as being TRUE for mobile sources and the PIM-SM forwarding rule "`iif == RPF_interface(S)`" is relaxed to be TRUE, as the incoming tunnel interface from MAG to LMA is considered as not part of the PIM-SM component of the LMA (see A.1 of [RFC4601]).

In addition, an LMA serving as PIM Designated Router is connected to MLD proxies via individual IP-tunnel interfaces and will experience changing PIM source states on handover. As the incoming interface connects to a point-to-point link, PIM Assert contention is not active, and incoming interface validation is only performed by RPF checks. Consequently, a PIM DR SHOULD update incoming source states, as soon as RPF inspection succeeds, i.e., after PMIPv6 forwarding state update. Consequently, PIM routers SHOULD be able to manage these state changes, but some implementations are expected to incorrectly refuse packets until the previous state has timed out.

Notably, running BIDIR PIM [RFC5015] on LMAs remains robust with respect to source location and does not require special configurations or state management for sources.

#### 3.2.4. IPv4 Support

An MN in a PMIPv6 domain may use an IPv4 address transparently for communication as specified in [RFC5844]. For this purpose, an LMA can register an IPv4-Proxy-CoA in its Binding Cache and the MAG can provide IPv4 support in its access network. Correspondingly, multicast membership management will be performed by the MN using IGMP. For multicast support on the network side, an IGMP proxy function needs to be deployed at MAGs in exactly the same way as for IPv6. [RFC4605] defines IGMP proxy behaviour in full agreement with



IPv6/MLD. Thus IPv4 support can be transparently provided following the obvious deployment analogy.

For a dual-stack IPv4/IPv6 access network, the MAG proxy instances SHOULD choose multicast signaling according to address configurations on the link, but MAY submit IGMP and MLD queries in parallel, if needed. It should further be noted that the infrastructure cannot identify two data streams as identical when distributed via an IPv4 and IPv6 multicast group. Thus duplicate data may be forwarded on a heterogeneous network layer.

A particular note is worth giving the scenario of [RFC5845] in which overlapping private address spaces of different operators can be hosted in a PMIP domain by using GRE encapsulation with key identification. This scenario implies that unicast communication in the MAG-LMA tunnel can be individually identified per MN by the GRE keys. This scenario still does not impose any special treatment of multicast communication for the following reasons.

Multicast streams from and to MNs arrive at a MAG on point-to-point links (identical to unicast). Multicast data transmission from the MAG to the corresponding LMA is link-local between the routers and routing/forwarding remains independent of any individual MN. So the MAG-proxy and the LMA SHOULD NOT use GRE key identifiers, but plain GRE encapsulation in multicast communication (including MLD queries and reports). Multicast traffic is transmitted as router-to-router forwarding via the MAG-to-LMA tunnels and according to the multicast routing information base (MRIB) of the MAG or the LMA. It remains independent of MN's unicast addresses, while the MAG proxy instance re-distributes multicast data down the point-to-point links (interfaces) according to its local subscription states, independent of IP addresses of the MN.

### 3.2.5. Efficiency of the Distribution System

The distribution system of the base solution directly follows PMIPv6 routing rules, and organizes multicast domains with respect to LMAs. Thus, no coordination between address spaces or services is required between the different instances, provided their associated LMAs belong to disjoint multicast domains. Routing is optimal for communication between MNs of the same domain, or stationary subscribers.

In the following, efficiency-related issues remain.

Multicast reception at LMA In the current deployment scenario, the LMA will receive all multicast traffic originating from its associated MNs. There is no mechanism to suppress upstream forwarding in the absence of receivers.

MNs on the same MAG using different LMAs For a mobile receiver and a source that use different LMAs, the traffic has to go up to one LMA, cross over to the other LMA, and then be tunneled back to the same MAG, causing redundant flows in the access network and at the MAG.

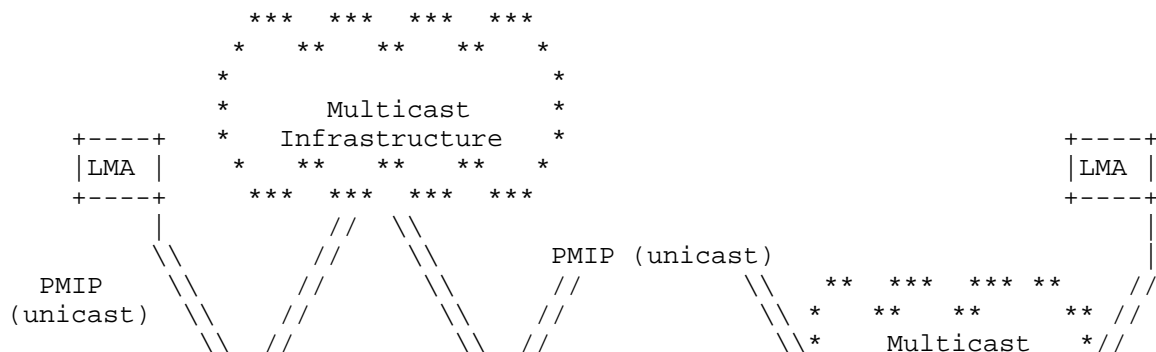
#### 4. Direct Multicast Routing

There are deployment scenarios, where multicast services are available throughout the access network independent of the PMIPv6 routing system [I-D.ietf-multimob-pmipv6-ropt]. In these cases, the visited networks grant a local content distribution service (in contrast to LMA-based home subscription) with locally optimized traffic flows. It is also possible to deploy a mixed service model of local and LMA-based subscriptions, provided a unique way of service selection is implemented. For example, access routers (MAGs) could decide on service access based on the multicast address G or the SSM channel (S,G) under request (see Appendix A for further discussions).

##### 4.1. Overview

Direct multicast access can be supported by

- o native multicast routing provided by one multicast router that is neighboring MLD proxies deployed at MAGs within a flat access network, or via tunnel uplinks,
- o a multicast routing protocol such as PIM-SM [RFC4601] or BIDIR-PIM [RFC5015] deployed at the MAGs.



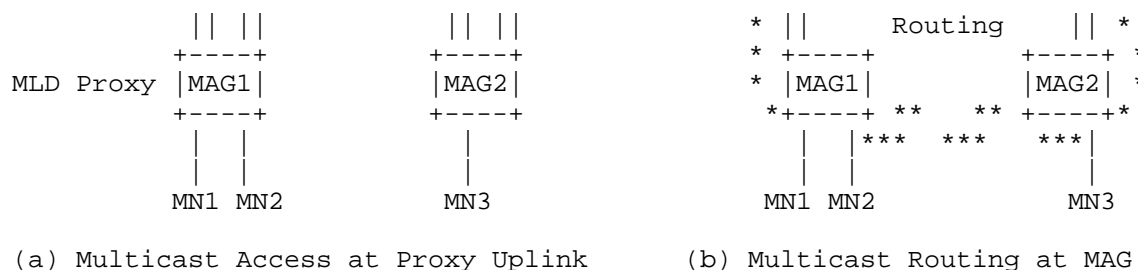


Figure 3: Reference Networks for (a) Proxy-assisted Direct Multicast Access and (b) Dynamic Multicast Routing at MAGs

Figure 3 displays the corresponding deployment scenarios, which separate multicast from PMIPv6 unicast routing. It is assumed throughout these scenarios that all MAGs (MLD proxies) are linked to a single multicast routing domain. Notably, this scenario requires coordination of multicast address utilization and service bindings.

Multicast traffic distribution can be simplified in these scenarios. A single proxy instance at MAGs with up-link into the multicast domain will serve as a first hop multicast gateway and avoid traffic duplication or detour routing. Multicast routing functions at MAGs will seamlessly embed access gateways within a multicast cloud. However, mobility of the multicast source in this scenario will require some multicast routing protocols to rebuild distribution trees. This can cause significant service disruptions or delays (see [RFC5757] for further aspects). Deployment details are specific to the multicast routing protocol in use, in the following described for common protocols.

#### 4.2. MLD Proxies at MAGs

In a PMIPv6 domain, single MLD proxy instances can be deployed at each MAG that enable multicast service at the access via an uplink to a multicast service infrastructure (see Figure 3 (a) ). To avoid service disruptions on handovers, the uplinks of all proxies SHOULD be adjacent to the same next-hop multicast router. This can either be achieved by arranging proxies within a flat access network, or by upstream tunnels that terminate at a common multicast router.

Multicast data submitted by a mobile source will reach the MLD proxy at the MAG that subsequently forwards flows to the upstream, and all downstream interfaces with appropriate subscriptions. Traversing the upstream will lead traffic into the multicast infrastructure (e.g., to a PIM Designated Router) which will route packets to all local MAGs that have joined the group, as well as further upstream according to protocol procedures and forwarding states.

On handover, a mobile source will reattach to a new MAG and can continue to send multicast packets as soon as PMIPv6 unicast configurations have completed. Like at the previous MAG, the new MLD proxy will forward data upstream and downstream to subscribers. Listeners local to the previous MAG will continue to receive group traffic via the local multicast distribution infrastructure following aggregated listener reports of the previous proxy. In general, traffic from the mobile source continues to be transmitted via the same next-hop router using the same source address and thus remains unchanged when seen from the wider multicast infrastructure.

#### 4.2.1. Considerations for PIM-SM on the Upstream

A mobile source that transmits data via an MLD proxy will not be directly connected to a PIM Designated Router as discussed in Section 3.2.3.1. Countermeasures apply correspondingly.

A PIM Designated Router that is connected to MLD proxies via individual IP-tunnel interfaces will experience invalid PIM source states on handover. In some implementations of PIM-SM this could lead to an interim packet loss (see Section Section 3.2.3.1). This problem can be mitigated by aggregating proxies on a lower layer.

#### 4.2.2. SSM Considerations

Source-specific subscriptions invalidate with routes, whenever the source moves from or to the MAG/proxy of a subscriber. Multicast forwarding states will rebuild with unicast route changes. However, this may lead to noticeable service disruptions for locally subscribed nodes.

#### 4.3. PIM-SM at MAGs

The full-featured multicast routing protocol PIM-SM MAY be deployed in the access network for providing multicast services in parallel to unicast routes. Throughout this section, it is assumed that the PMIPv6 mobility domain is part of a single PIM-SM multicast routing domain with PIM-SM routing functions present at all MAGs and all LMAs. The PIM routing instance at a MAG SHALL then serve as the Designated Router (DR) for all directly attached Mobile Nodes. For expediting handover operations, it is advisable to position PIM Rendezvous Points (RPs) in the core of the PMIPv6 network domain. However, regular IP routing tables need not be present in a PMIPv6 deployment, and additional effort is required to establish reverse path forwarding rules as required by PIM-SM.

##### 4.3.1. Routing Information Base for PIM-SM

In this scenario, PIM-SM will rely on a Multicast Routing Information Base (MRIB) that is generated independently of the policy-based routing rules of PMIPv6. The granularity of mobility-related routing locators required in PIM depends on the complexity (phases) of its deployment.

The following information is needed for all phases of PIM.

- o All routes to networks and nodes (including RPs) that are not mobile members of the PMIPv6 domain MUST be defined consistently among PIM routers and MUST remain unaffected by node mobility. The setup of these general routes is expected to follow the topology of the operator network and is beyond the scope of this document.

The following route entries are required at a PIM-operating MAG when phases two or three of PIM, or PIM-SSM are in operation.

- o Local routes to the Home Network Prefixes (HNPs) of all MNs associated with their corresponding point-to-point attachments that MUST be included in the local MRIB.
- o All routes to MNs that are attached to distant MAGs of the PMIPv6 domain point towards their corresponding LMAs. These routes MUST be made available in the MRIB of all PIM routers (except for the local MAG of attachment), but MAY be eventually expressed by an appropriate default entry.

#### 4.3.2. Operations of PIM in Phase One

A new mobile source S will transmit multicast data of group G towards its MAG of attachment. Acting as a PIM DR, the access gateway will unicast-encapsulate the multicast packets and forward the data to the Virtual Interface (VI) with encapsulation target RP(G), a process known as PIM source registering. The RP will decapsulate and natively forward the packets down the RP-based distribution tree towards (mobile and stationary) subscribers.

On handover, the point-to-point link connecting the mobile source to the old MAG will go down and all (S,*) flows terminate. In response, the previous DR (MAG) deactivates the data encapsulation channels for the transient source (i.e., all DownstreamJPState(S,*,VI) are set to NoInfo state). After reattaching and completing unicast handover negotiations, the mobile source can continue to transmit multicast packets, while being treated as a new source at its new DR (MAG). Source register encapsulation will be immediately initiated, and (S,G) data continue to flow natively down the (*,G) RP-based tree.

Source handover management in PIM phase one admits low complexity and remains transparent to receivers. In addition, the source register tunnel management of PIM is a fast protocol operation and little overhead is induced thereof. In a PMIPv6 deployment, PIM RPs MAY be configured to not initiate (S,G) shortest path trees for mobile sources, and thus remain in phase one of the protocol. The price to pay for such simplified deployment lies in possible routing detours by an overall RP-based packet distribution.

#### 4.3.3. Operations of PIM in Phase Two

After receiving source register packets, a PIM RP eventually will initiate a source-specific Join for creating a shortest path tree to the (mobile) source S, and issue a source register stop at the native arrival of data from S. For initiating an (S,G) tree, the RP, as well as all intermediate routers, require route entries for the HNP of the MN that - unless the RP coincides with the MAG of S - point towards the corresponding LMA of S. Consequently, the (S,G) tree will proceed from the RP via the (stable) LMA, down the LMA-MAG tunnel to the mobile source. This tree can be of lesser routing efficiency than the PIM source register tunnel established in phase one, but provides the advantage of immediate data delivery to receivers that share a MAG with S.

On handover, the mobile source reattaches to a new MAG (DR), and PMIPv6 unicast management will transfer the LMA-MAG tunnel to the new point of attachment. However, in the absence of a corresponding multicast forwarding state, the new DR will treat S as a new source and initiate a source registering of PIM phase one with the RP. In response, the PIM RP will recognize the known source at a new (tunnel) interface immediately responds with a register stop. As the RP had joined the shortest path tree to receive from the source via the LMA, it will see an RPF change when data arrives at a new interface. Implementation-dependent, this can trigger an update of the PIM MRIB and trigger a new PIM Join message. Otherwise, the tree is periodically updated by Joins transmitted towards the new MAG on a path via the LMA. In proceeding this way, a quick recovery of PIM transition from phase one to two will be performed per handover.

#### 4.3.4. Operations of PIM in Phase Three

In response to an exceeded threshold of packet transmission, DRs of receivers eventually will initiate a source-specific Join for creating a shortest path tree to the (mobile) source S, thereby transitioning PIM into the final short-cut phase three. For all receivers not sharing a MAG with S, this (S,G) tree will range from the receiving DR via the (stable) LMA, the LMA-MAG tunnel to the mobile source. This tree is of higher routing efficiency than

established in the previous phase two, but need not outperform the PIM source register tunnel established in phase one. It provides the advantage of immediate data delivery to receivers that share a MAG with S.

On handover, the mobile source reattaches to a new MAG (DR), and PMIPv6 unicast management will transfer the LMA-MAG tunnel to the new point of attachment. However, in the absence of a corresponding multicast forwarding state, the new DR will treat S as a new source and initiate a source registering of PIM phase one. A PIM implementation compliant with this change can recover phase three states in the following way. First, the RP recovers to phase two as described in the previous section, and will not forward data arriving via the source register tunnel. Tree maintenance eventually triggered by the RPF change (see Section 4.3.3) will generate proper states for a native forwarding from the new MAG via the LMA. Thereafter, packets arriving at the LMA without source register encapsulation are forwarded natively along the shortest path tree towards receivers.

In consequence, the PIM transition from phase one to two and three will be quickly recovered per handover, but still leads to an enhanced signaling load and intermediate packet loss.

#### 4.3.5. PIM-SSM Considerations

Source-specific Joins of receivers will guide PIM to operate in SSM mode and lead to an immediate establishment of source-specific shortest path trees. Such (S,G) trees will equal the distribution system of PIM's final phase three (see Section 4.3.4). However, on handover and in the absence of RP-based data distribution, SSM data delivery cannot be resumed via source registering as in PIM phase one. Consequently, data packets transmitted after a handover will be discarded at the MAG until regular tree maintenance has re-established the (S,G) forwarding state at the new MAG.

#### 4.3.6. Handover Optimizations for PIM

Source-specific shortest path trees are constructed in PIM-SM (phase two and three), and in PIM-SSM that follow LMA-MAG tunnels towards a source. As PIM remains unaware of source mobility management, these trees invalidate under handovers with each tunnel re-establishment at a new MAG. Regular tree maintenance of PIM will recover the states, but remains unsynchronized and too slow to seamlessly preserve PIM data dissemination.

A method to quickly recover PIM (S,G) trees under handover SHOULD synchronize multicast state maintenance with unicast handover operations and MAY proceed as follows. On handover, an LMA reads all

(S,G) Join states from its corresponding tunnel interface and identifies those source addresses  $S_i$  that match moving HNPs. After re-establishing the new tunnel, it SHOULD associate the  $(S_i,*)$  Join states with the new tunnel endpoint and immediately trigger a state maintenance (PIM Join) message. In proceeding this way, the source-specific PIM states are transferred to the new tunnel end point and propagated to the new MAG in synchrony with unicast handover procedures.

#### 4.4. BIDIR-PIM

BIDIR-PIM MAY be deployed in the access network for providing multicast services in parallel to unicast routes. Throughout this section, it is assumed that the PMIPv6 mobility domain is part of a single BIDIR-PIM multicast routing domain with BIDIR-PIM routing functions present at all MAGs and all LMAs. The PIM routing instance at a MAG SHALL then serve as the Designated Forwarder (DF) for all directly attached Mobile Nodes. For expediting handover operations, it is advisable to position BIDIR-PIM Rendezvous Point Addresses (RPAs) in the core of the PMIPv6 network domain. As regular IP routing tables need not be present in a PMIPv6 deployment, reverse path forwarding rules as required by BIDIR-PIM need to be established.

##### 4.4.1. Routing Information Base for BIDIR-PIM

In this scenario, BIDIR-PIM will rely on a Multicast Routing Information Base (MRIB) that is generated independently of the policy-based routing rules of PMIPv6. The following information is needed.

- o All routes to networks and nodes (including RPAs) that are not mobile members of the PMIPv6 domain MUST be defined consistently among BIDIR-PIM routers and remain unaffected by node mobility. The setup of these general routes is expected to follow the topology of the operator network and is beyond the scope of this document.

##### 4.4.2. Operations of BIDIR-PIM

BIDIR-PIM will establish spanning trees across its network domain in conformance to its preconfigured RPAs and the routing information provided. Multicast data transmitted by a mobile source will immediately be forwarded by its DF (MAG) onto the spanning group tree without further protocol operations.

On handover, the mobile source re-attaches to a new MAG (DF), which completes unicast network configurations. Thereafter, the source can



immediately proceed with multicast packet transmission onto the pre-established distribution tree. BIDIR-PIM does neither require protocol signaling nor additional reconfiguration delays to adapt to source mobility and can be considered the protocol of choice for mobile multicast operations in the access. As multicast streams always flow up to the Rendezvous Point Link, some care should be taken to configure RPAs compliant with network capacities.

## 5. Extended MLD Proxy Function for Optimized Source Mobility in PMIPv6

A deployment of MLD Proxies (see [RFC4605]) at MAGs has proven a useful and appropriate approach to multicast in PMIPv6, see [RFC6224], [I-D.ietf-multimob-pmipv6-ropt]. However, deploying unmodified standard proxies can go along with significant performance degradation for mobile senders as discussed along the lines of this document. To overcome these deficits, an optimized approach to multicast source mobility based on extended peering functions among proxies is introduced in this section. Prior to presenting the solution, we will sketch the relevant requirements.

Solutions that extend MLD Proxies by additional uplinking functions need to comply to the following requirements.

**Prevention of Routing Loops** In the absence of a full-featured routing logic at an MLD Proxy, simple and locally decidable rules need to prevent source traffic from traversing the network in loops as potentially enabled by multiple uplinks.

**Unique coverage of receivers** Listener functions at Proxies require simple, locally decidable rules to initiate a unique delivery of multicast packets to all receivers.

Following different techniques, these requirements are met in the following solutions.

### 5.1. Peering Function for MLD Proxies

In this section, we define a peering interface for MLD proxies that allows for a direct data exchange of locally attached multicast sources. Such peering interfaces can be configured - as a direct link or a bidirectional tunnel - between any two proxy instances (locally deployed as in [RFC6224] or remotely) and remain as silent virtual links in regular proxy operations. Data on such link is exchanged only in cases, where one peering proxy directly connects on the downstream to a source of multicast traffic, which the other peering proxy actively subscribes to. Operations are defined for ASM and SSM, but provide superior performance in the presence of source-specific signaling (IGMPv3/MLDv2).

#### 5.1.1. Operations at the Multicast Sender

An MLD Proxy in the perspective of a sender will see peering interfaces as restricted downstream interfaces. It will install and maintain source filters at its peering links that will restrict data transmission to those packets that originate from a locally attached source at the downstream. In detail, a proxy will extract from its configuration the network prefixes attached to its downstream interfaces and MUST implement a source filter base at its peering interfaces that restricts data transmission to IP source addresses from its local prefixes. This filter base Must be updated, if and only if the downstream configuration changes. In this way, a multihop forwarding on peering links is prevented. Multicast packets that arrive from the upstream interface of the proxy are thus only forwarded to regular downstream interfaces with appropriate subscription states.

Multicast traffic arriving from a locally attached source will be forwarded to the regular upstream interface and all downstreams with appropriate subscription states (i.e., regular Proxy operations). In addition, local multicast packets are transferred to those peering interfaces with appropriate subscription states.

#### 5.1.2. Operations at the Multicast Listener

From the listener side, peering interfaces appear as preferred upstream links. Thus an MLD proxy with peering interconnects will offer several interfaces for pulling remote traffic: the regular upstream and the peerings. Traffic arriving from any of the peering links will be mutually disjoint, but normally also available from the upstream. To prevent duplicate traffic from arriving at the listener side, the proxy

- o MAY delay aggregated reports to the upstream, and
- o MUST apply appropriate filters to exclude duplicate streams.

In detail, it first issues listener reports (in parallel) to its peering links, which only span one (virtual) hop. Whenever the expected traffic (e.g., SSM channels) does not completely arrive from the peerings after a waiting time (default: 10 ms), additional (complementary, in the case of SSM) reports are sent to the standard upstream interface.

After the arrival of traffic from peering links, an MLD proxy MUST install source filters at the upstream in the following way.

ASM with IGMPv2/MLDv1 In the presence of Any Source Multicast using IGMPv2/MLDv1, only, the proxy cannot signal source filtering to its upstream. Correspondingly, it applies (S,*) ingress filters at its upstream interface for all sources S seen in traffic of the peering links. It is noteworthy that unwanted traffic is still replicated to the proxy via the access network.

ASM with IGMPv3/MLDv2 In the presence of source-specific signaling (IGMPv3/MLDv2), the upstream interface is set to (S,*) exclude mode for all sources S seen in traffic of the peering links. The corresponding source-specific signaling will prevent duplicate traffic forwarding throughout the access network.

SSM In the presence of Source Specific Multicast, the proxy will subscribe on its uplink interface to those (S,G) channels, only, that do not arrive via the peering links.

In proceeding this way, multicast group data arrive from peering interfaces first, while only peer-wise unavailable traffic is retrieved from the regular upstream interface.

## 6. IANA Considerations

TODO.

Note to RFC Editor: this section may be removed on publication as an RFC.

## 7. Security Considerations

TODO

Consequently, no new threats are introduced by this document in addition to those identified as security concerns of [RFC3810], [RFC4605], [RFC5213], and [RFC5844].

However, particular attention should be paid to implications of combining multicast and mobility management at network entities. As this specification allows mobile nodes to initiate the creation of multicast forwarding states at MAGs and LMAs while changing attachments, threats of resource exhaustion at PMIP routers and access networks arrive from rapid state changes, as well as from high volume data streams routed into access networks of limited capacities. In addition to proper authorization checks of MNs, rate controls at replicators MAY be required to protect the agents and the downstream networks. In particular, MLD proxy implementations at MAGs SHOULD carefully procure for automatic multicast state extinction on the departure of MNs, as mobile multicast listeners in

the PMIPv6 domain will not actively terminate group membership prior to departure.

## 8. Acknowledgements

The authors would like to thank (in alphabetical order) Luis M. Contreras, Muhamma Omer Farooq, Bohao Feng, Dirk von Hugo, Ning Kong, Jouni Korhonen, He-Wu Li, Akbar Rahman, Stig Venaas, Li-Li Wang, Qian Wu, Zhi-Wei Yan for advice, help and reviews of the document. Funding by the German Federal Ministry of Education and Research within the G-LAB Initiative (projects HAMcast, Mindstone and SAFEST) is gratefully acknowledged.

## 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.
- [RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.
- [RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.
- [RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.
- [RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.
- [RFC4605] Fenner, B., He, H., Haberman, B., and H. Sandick, "Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP /MLD Proxying")", RFC 4605, August 2006.
- [RFC5015] Handley, M., Kouvelas, I., Speakman, T., and L. Vicisano, "Bidirectional Protocol Independent Multicast (BIDIR-PIM)", RFC 5015, October 2007.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

## 9.2. Informative References

- [I-D.ietf-multimob-pmipv6-ropt]  
Zuniga, J., Contreras, L., Bernardos, C., Jeon, S., and Y. Kim, "Multicast Mobility Routing Optimizations for Proxy Mobile IPv6", draft-ietf-multimob-pmipv6-ropt-07 (work in progress), July 2013.
- [RFC2236] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.
- [RFC5757] Schmidt, T., Waehlich, M., and G. Fairhurst, "Multicast Mobility in Mobile IP Version 6 (MIPv6): Problem Statement and Brief Survey", RFC 5757, February 2010.
- [RFC5845] Muhanna, A., Khalil, M., Gundavelli, S., and K. Leung, "Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6", RFC 5845, June 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.

## Appendix A. Multiple Upstream Interface Proxy

In this section, we document upstream extensions for an MLD proxy that were originally developed during the work on this document. Multiple proxy instances deployed at a single MAG (see Section 3) can be avoided by adding multiple upstream interfaces to a single MLD Proxy. In a typical PMIPv6 deployment, each upstream of a single proxy instance can interconnect to one of the LMAs. With such ambiguous upstream options, appropriate forwarding rules MUST be supplied to

- o unambiguously guide traffic forwarding from directly attached mobile sources, and
- o lead listener reports to initiating unique traffic subscriptions.

This can be achieved by a complete set of source- and group-specific filter rules (e.g., (S,*), (*,G)) installed at proxy interfaces. These filters MAY be derived in parts from PMIPv6 routing policies, and can include a default behavior (e.g., (*,*)).

#### A.1. Operations for Local Multicast Sources

Packets from a locally attached multicast source will be forwarded to all downstream interfaces with appropriate subscriptions, as well as up the interface with the matching source-specific filter.

Typically, the upstream interface for a mobile multicast source is chosen based on the policy routing (e.g., the MAG-LMA tunnel interface for LMA-based routing or the interface towards the multicast router for direct routing), but alternate configurations MAY be applied. Packets from a locally attached multicast source will be forwarded to the corresponding upstream interface with the matching source-specific filter, as well as all the downstream interfaces with appropriate subscriptions.

#### A.2. Operations for Local Multicast Subscribers

Multicast listener reports are group-wise aggregated by the MLD proxy. The aggregated report is issued to the upstream interface with matching group/channel-specific filter. The choice of the corresponding upstream interface for aggregated group membership reports MAY be additionally based on some administrative scoping rules for scoped multicast group addresses.

In detail, a Multiple Upstream Interface Proxy will provide and maintain a Multicast Subscription Filter Table that maps source- and group-specific filters to upstream interfaces. The forwarding decision for an aggregated MLD listener report is based on the first matching entry from this table, with the understanding that for IGMPv3/MLDv2 the MLD Proxy performs a state decomposition, if needed (i.e., a (*,G) subscription is split into (S,G) and (* \ S,G) in the presence of (*,G) after (S,G) interface entries), and that (S,*)-filters are always false in the absence of source-specific signaling, i.e. in IGMPv2/MLDv1 only domains.

In typical deployment scenarios, specific group services (channels) could be either associated with selected uplinks to remote LMAs, while a (*,*) default subscription entry (in the last table line) is bound to a local routing interface, or selected groups are configured as local services first, while a (*,*) default entry (in the last table line) points to a remote uplink that provides the general multicast support.

## Appendix B. Change Log

The following changes have been made from version draft-ietf-multimob-pmipv6-source-03:

1. Fixed issues in Section Section 4.3 (PIM phase two and three transistion) according to WG feedback.
2. Editorial improvements, resolved nits.
3. Updated references.

The following changes have been made from version draft-ietf-multimob-pmipv6-source-02:

1. Added clarifications and details as requested by the working group, resolved nits.
2. Moved Multiple Upstream MLD Proxy to Appendix in response to WG desire.
3. Updated references.

The following changes have been made from version draft-ietf-multimob-pmipv6-source-01:

1. Added clarifications and details as requested by the working group, resolved nits.
2. Detailed out operations of Multiple Upstream MLD Proxies.
3. Clarified operations of MLD proxies with peering links.
4. Many editorial improvements.
5. Updated references.

The following changes have been made from version draft-ietf-multimob-pmipv6-source-00:

1. Direct routing with PIM-SM and PIM-SSM has been added.
2. PMIP synchronization with PIM added for improved handover.
3. Direct routing with BIDIR-PIM has been added.
4. MLD Proxy extensions requirements added.

5. Peering of MLD Proxies added.
6. First sketch of multiple upstream proxy added.
7. Editorial improvements.
8. Updated references.

#### Authors' Addresses

Thomas C. Schmidt (editor)  
HAW Hamburg  
Berliner Tor 7  
Hamburg 20099  
Germany

Email: [schmidt@informatik.haw-hamburg.de](mailto:schmidt@informatik.haw-hamburg.de)  
URI: <http://inet.cpt.haw-hamburg.de/members/schmidt>

Shuai Gao  
Beijing Jiaotong University  
Beijing  
China

Email: [shgao@bjtu.edu.cn](mailto:shgao@bjtu.edu.cn)

Hong-Ke Zhang  
Beijing Jiaotong University  
Beijing  
China

Email: [hkzhang@bjtu.edu.cn](mailto:hkzhang@bjtu.edu.cn)

Matthias Waehlich  
link-lab & FU Berlin  
Hoenower Str. 35  
Berlin 10318  
Germany

Email: [mw@link-lab.net](mailto:mw@link-lab.net)



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

H. Liu  
M. McBride  
Huawei Technologies  
July 12, 2012

IGMP/MLD Optimizations in Wireless and Mobile Networks  
draft-liu-multimob-igmp-mld-wireless-mobile-02

Abstract

This document proposes a variety of optimization approaches for IGMP and MLD in wireless and mobile networks. It aims to provide useful guideline to allow efficient multicast communication in these networks using IGMP or MLD protocols.

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 [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 January 13, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Requirements . . . . .	3
2.1. Characteristics of Wireless and Mobile Multicast . . . . .	3
2.2. Wireless Link Model . . . . .	4
2.3. Requirements on IGMP and MLD . . . . .	5
3. IGMP/MLD Optimization for Wireless and Mobile Networks . . . . .	6
3.1. Switching Between Unicast and Multicast Queries . . . . .	6
3.2. General Query Supplemented with Unicast Query . . . . .	6
3.3. Retransmission of Queries . . . . .	7
3.4. General Query Suppression . . . . .	7
3.5. Tuning Response Delay According to Link Type and Status . . . . .	8
3.6. Triggering Reports and Queries Quickly During Handover . . . . .	9
4. Applicability and Interoperability Considerations . . . . .	9
5. IANA Considerations . . . . .	10
6. Security Considerations . . . . .	10
7. Acknowledgements . . . . .	10
8. Normative References . . . . .	10
Authors' Addresses . . . . .	11

## 1. Introduction

With the wide deployment of various wireless access techniques and the tendency to support video applications on wireless networks, wireless and mobile multicast come to attract more and more interests from content and service providers, but still face great challenges when considering dynamic group membership management under constant update of delivery path introduced by node movement, and high probability of loss and congestion due to limited reliability and capacity of wireless links.

Multicast network is generally constructed by IGMP and MLD group management protocol (respectively for IPv4 and IPv6 networks) to track valid receivers and by multicast routing protocol to build multicast delivery paths. This document focuses only on IGMP and MLD, which are used by a host to subscribe a multicast group and are most possibly to be exposed to wireless link to support terminal mobility. As IGMP and MLD were designed for fixed users using wired link, they do not necessarily work well for different wireless link types and mobile scenarios, thus should be considered to be enhanced to be more applicable in these environments.

This memo proposes a variety of optimizations for IGMP and MLD in wireless and mobile networks to improve network performance, with minimum changes on the protocol behavior and without introducing interoperability issues. These solutions can also be applied in wired network when efficiency or reliability is required.

For generality, this memo does not put limitations on the type of wireless techniques running below IGMP or MLD. They could be cellular, WiMAX, WiFi and etc, and are modeled as different abstract link models as described in section 2.2. Even though some of them (such as WiFi) have multicast limitations, it is probable that IGMP/MLD is enabled on the wireless terminal and multicast is supported across the network. The mobile IP protocol adopted on the core side, upstream from the access router, could be PMIP, MIPv4, or MIPv6.

## 2. Requirements

### 2.1. Characteristics of Wireless and Mobile Multicast

Several limitations should be considered when supporting IP multicast in wireless and mobile networks, including:

O Limited link bandwidth: wireless link usually has limited bandwidth, and the situation will be made even worse if high volume video multicast data has to be carried. Also the bandwidth available

in the upstream and downstream directions may be asymmetrical.

O High loss rate: wireless link usually has packet loss ranging from 1% to 30% according to different links types and conditions. Also when packets have to travel between home and access networks (e.g. through tunnel), they are prone to loss if the two networks are distant from each other.

O Frequent membership change: in fixed multicast, membership change only happens when a user leaves or joins a group, while in mobile scenario membership may also change when a user changes its location.

O Prone to performance degradation: the possible increased interaction of protocols across layers for mobility management, and the limitation of link capacity, may lead to network performance degradation and even to complete connection loss.

O Increased Leave Latency: the leave latency in mobile multicast might be increased due to user movement, especially if the traffic has to be transmitted between access and home networks, or if there is a handshake between networks.

## 2.2. Wireless Link Model

Wireless links can be categorized by their different transmission modes into three typical models: point-to-point (PTP), point-to-multipoint (PTMP), and broadcast link models.

In PTP model, one link is dedicated for two communication facilities. For multicast transmission, each PTP link normally has only one receiver and the bandwidth is dedicated for that receiver. Such link model may be implemented by running PPP on the link or having separate VLAN assignment for each receiver. In mobile network, tunnel between entities of home and foreign networks should be recognized as a PTP link.

PTMP is the model for multipoint transmission wherein there is one centralized transmitter and multiple distributed receivers. PTMP provides common downlink channels for all receivers and dedicated uplink channel for each receiver. Bandwidth downstream is shared by all receivers on the same link.

Broadcast link can connect two or more nodes and supports broadcast transmission. It is quite similar to fixed Ethernet link model and its link resource is shared in both uplink and downlink directions.

### 2.3. Requirements on IGMP and MLD

IGMP and MLD are usually run between mobile or wireless terminals and their first-hop access routers (i.e. home or foreign routers) to subscribe an IP multicast channel. Currently the version in-use includes IGMPv2 [RFC2236] and its IPv6 counterpart MLDv1 [RFC2710], IGMPv3 [RFC3376] and its IPv6 counterpart MLDv2 [RFC3810], and LW-IGMPv3/MLDv2 [RFC5790]. All these versions have basic group management capability required by a multicast subscription. The differences lie in that IGMPv2 and MLDv1 can only join and leave a non-source-specific group, while IGMPv3 and MLDv2 can select including and excluding specific sources for their join and leave operation, and LW-IGMPv3/MLDv2 simplifies IGMPv3/MLDv2 procedures by discarding excluding-source function. Among these versions, (LW-)IGMPv3/MLDv2 has the capability of explicitly tracking each host member.

From the illustration given in section 2.1 and 2.2, it is desirable for IGMP and MLD to have the following characteristics when used in wireless and mobile networks:

- o Adaptive to link conditions: wireless network has various link types, each with different bandwidth and performance features. IGMP or MLD should be able to be adaptive to different link model and link conditions to optimize its protocol operation.
- o Minimal group join/leave latency: because mobility and handover may cause a user to join and leave a multicast group frequently, fast join and leave by the user helps to accelerate service activation and to release unnecessary resources quickly to optimize resource utilization.
- o Robust to packet loss: the unreliable packet transmission due to instable wireless link conditions and limited bandwidth, or long distance transmission in mobile network put more strict robustness requirement on delivery of IGMP and MLD protocol messages.
- o Reducing packet exchange: wireless link resources are usually more limited, precious, and congested compared to their wired counterpart. This requires packet exchange be minimized without degrading protocol performance.
- o Packet burst avoidance: large number of packets generated in a short time interval may have the tendency to deteriorate wireless network conditions. IGMP and MLD should be optimized to reduce the probability of packet burst.

### 3. IGMP/MLD Optimization for Wireless and Mobile Networks

This section introduces several optimization methods for IGMP and MLD in wireless or mobile environment. The aim is to meet the requirements described in section 2.3. It should be noted that because an enhancement in one direction might result in weakening effect in another, balances should be taken cautiously to realize overall performance elevation.

#### 3.1. Switching Between Unicast and Multicast Queries

IGMP/MLD protocol uses multicast Queries whose destinations are multicast addresses and also allows use of unicast Query with unicast destination to be sent only to one host. Unicast Query has the advantage of not affecting other hosts on the same link, and is desirable for wireless communication because a mobile terminal often has limited battery power [RFC6636]. But if the number of valid receivers is large, using unicast Query for each receiver is inefficient because large number of Unicast Queries have to be generated, in which situation normal multicast Query will be a good choice because only one General Query is needed. If the number of receivers to be queried is small, unicast Query is advantageous over the multicast one.

More flexibly, the router can choose to switch between unicast and multicast Queries according to the practical network conditions. For example, if the receiver number is small, the router could send unicast Queries respectively to each receiver, without arousing other non-member terminal which is in dormant state. When the receiver number reaches a predefined level, the router could change to use multicast Queries. To have the knowledge of the number of the valid receivers, a router is required to enable explicit tracking, and because Group-Specific Query and Group-and-Source-Specific Query are usually not used under explicit tracking [RFC6636], the switching operation mostly applies to General Queries.

#### 3.2. General Query Supplemented with Unicast Query

Unicast Query also can be used in assistance to General Query to improve the robustness of solicited reports when General Query fails to collect all of its valid members. It requires the explicit tracking to be enabled and can be used when a router after sending a periodical General Query collects successfully most of the valid members' responses while losing some of which are still valid in its database. This may be because these reports are not generated or generated but lost for some unknown reasons. The router could choose to unicast a Query respectively to each non-respondent valid receiver to check whether they are still alive for the multicast reception,

without affecting the majority of receivers that have already responded. Unicast Queries under this condition could be sent at the end of the [Maximum Response Delay] after posting a General Query, and be retransmitted for [Last Member Query Count] times, at an interval of [Last Member Query Interval].

### 3.3. Retransmission of Queries

In IGMP and MLD, apart from the continuously periodical transmission, General Query is also transmitted during a router's startup. It is transmitted for [Startup Query Count] times by [Startup Query Interval]. There are some other cases where retransmission of General Query is beneficial which are not covered by current IGMP and MLD protocols as shown as following.

For example, a router which keeps track of all its active receivers, if after sending a General Query, fails to get any response from the receivers which are still valid in its membership database. This may be because all the responses of the receivers happen to be lost, or the sent Query does not arrive at the other side of the link to the receivers. The router could compensate this situation by retransmitting the General Query to solicit its active members. The retransmission can also be applied to Group-Specific or Group-and-Source-Specific Query on a router without explicit tracking capability, when these Specific Queries cannot collect valid response, to prevent missing valid members caused by lost Queries and Reports.

The above compensating Queries could be sent [Last Member Query Count] times, at the interval of [Last Member Query Interval], if the router cannot get any feedback from the receivers.

### 3.4. General Query Suppression

In IGMP and MLD, General Query is sent periodically and continuously without any limitation. It helps soliciting the state of current valid member but has to be processed by all hosts on the link, whether they are valid multicast receivers or not. When there is no receiver, the transmission of the General Query is a waste of resources for both the host and the router.

An IGMP/MLD router could suppress its transmission of General Query if it knows there is no valid multicast receiver on an interface, e.g. in the following cases:

O When the last member reports its leave for a group. This could be judged by an explicit tracking router checking its membership database, or by a non-explicit-tracking router getting no response

after sending Group-Specific or Group-and-Source-Specific Query.

O When the only member on a PTP link reports its leaving

O When a router after retransmitting General Queries on startup fails to get any response

O When a router previously has valid members but fails to get any response after several rounds of General Queries.

In these cases the router could make the decision that no member is on the interface and totally stop its transmission of periodical General Queries. If afterwards there is any valid member joins a group, the router could resume the original cycle of general Querying. Because General Query has influences on all hosts on a link, suppressing it when it is not needed is beneficial for both the link efficiency and terminal power saving.

### 3.5. Tuning Response Delay According to Link Type and Status

IGMP and MLD use delayed response to spread unsolicited Reports from different hosts to reduce possibility of packet burst. This is implemented by a host responding to a Query in a specific time randomly chosen between 0 and [Maximum Response Delay], the latter of which is determined by the router and is carried in Query messages to inform the hosts for calculation of the response delay. A larger value will lessen the burst better but will increase leave latency (the time taken to cease the traffic flowing after the last member requests the escaping of a channel).

In order to avoid message burst and reduce leave latency, the Response Delay may be dynamically calculated based on the expected number of responders, and link type and status, as shown in the following:

O If the expected number of reporters is large and link condition is bad, longer Maximum Response Delay is recommended; if the expected number of reporters is small and the link condition is good, smaller Maximum response Delay should be set.

o If the link type is PTP, the Maximum Response Delay can be chosen smaller, whereas if the link is PTMP or broadcast medium, the Maximum Response Delay can be configured larger.

The Maximum Response Delay could be configured by the administrator as mentioned above, or be calculated automatically by a software tool implemented according to experiential model for different link modes. The measures to determine the instant value of Maximum Response Delay



are out of this document's scope.

### 3.6. Triggering Reports and Queries Quickly During Handover

When a mobile terminal is moving from one network to another, if it is receiving multicast content, its new access network should try to deliver the content to the receiver without disruption or performance deterioration. In order to implement smooth handover between networks, the terminal's membership should be acquired as quickly as possible by the new access network.

An access router could trigger a Query to a terminal as soon as it detects the terminal's attaching on its link. This could be a General Query if the number of the entering terminals is not small (e.g when they are simultaneously in a moving train). Or this Query could also be a unicast Query for this incoming terminal to prevent unnecessary action of other terminals in the switching area.

For the terminal, it could send a report immediately if it is currently in the multicast reception state, when it begins to connect the new network. This helps establishing more quickly the membership state and enable faster multicast stream injection, because with the active report the router does not need to wait for the query period to acquire the terminal's newest state.

## 4. Applicability and Interoperability Considerations

Among the optimizations listed above, 'Switching between unicast and multicast Queries'(3.1) and 'General Query Supplemented with Unicast Query'(3.2) require a router to know beforehand the valid members connected through an interface, thus require explicit tracking capability. An IGMP/MLD implementation could choose any combination of the methods listed from 3.1 to 3.6 to optimize multicast communication on a specific wireless or mobile network.

For example, an explicit-tracking IGMPv3 router, can switch to unicast General Queries if the number of members on a link is small (3.1), can trigger unicast Query to a previously valid receiver if failing to get expected responses from it (3.2), can retransmit a General Query if after the previous one cannot collect reports from all valid members (3.3), and can stop sending a General Query when the last member leaves the group (3.4), and etc.

For interoperability, it is required if multiple multicast routers are connected to the same network for redundancy, each router are configured with the same optimization policy to synchronize the membership states among the routers.

## 5. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

## 6. Security Considerations

Since the methods only involve the tuning of protocol behavior by e.g. retransmission, changing delay parameter, or other compensating operations, they do not introduce additional security weaknesses. The security considerations described in [RFC2236], [RFC3376], [RFC2710] and [RFC3810] can be reused. And to achieve some security level in insecure wireless network, it is possible to take stronger security procedures during IGMP/MLD message exchange, which are out of the scope of this memo.

## 7. Acknowledgements

The authors would like to thank Qin Wu, Stig Venaas, Gorrry Fairhurst, Thomas C. Schmidt, Marshall Eubanks, Suresh Krishnan, J. William Atwood, WeeSan Lee, Imed Romdhani, Hitoshi Asaeda, Liu Yisong and Wei Yong for their valuable comments and suggestions on this document.

## 8. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC2236] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.
- [RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.
- [RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.
- [RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.
- [RFC5790] Liu, H., Cao, W., and H. Asaeda, "Lightweight Internet

Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Version 2 (MLDv2) Protocols", RFC 5790, February 2010.

[RFC6636] Asaeda, H., Liu, H., and Q. Wu, "Tuning the Behavior of the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) for Routers in Mobile and Wireless Networks", RFC 6636, May 2012.

#### Authors' Addresses

Hui Liu  
Huawei Technologies  
Building Q14, No.156, Beiqing Rd.  
Beijing 100095  
China

Email: [helen.liu@huawei.com](mailto:helen.liu@huawei.com)

Mike McBride  
Huawei Technologies  
2330 Central Expressway  
Santa Clara CA 95050  
USA

Email: [michael.mcbride@huawei.com](mailto:michael.mcbride@huawei.com)



MULTIMOB Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: August 3, 2012

J. Liu  
W. Luo  
W. Yan  
ZTE Corporation  
January 31, 2012

Routes Optimization for PMIPv6 Multicast  
draft-liu-multimob-pmipv6-multicast-ro-00

Abstract

To support IP multicasting in PMIPv6 domain, MULTIMOB WG has issued several proposals including the base solution, dedicated schemes and direct routing which requires all communications to go through the local mobility anchor (LMA), the dedicated server and the native multicasting infrastructure, respectively. As this can be suboptimal, localized routing (LR) allows multicast source attached to the same or different mobile access gateways (MAG) with mobile node to send multicast data by using localized forwarding or a direct tunnel between the gateways without any dedicated devices or dependence of the native multicasting infrastructure. This document describes multicast routes optimization mechanisms for localized routing. The MAG and the LMA are the mobility entities defined in the PMIPv6 protocol and act as PIM-SM routers.

Status of this Memo

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

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

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

This Internet-Draft will expire on August 3, 2012.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

## Table of Contents

1. Introduction . . . . .	3
2. Terminology . . . . .	5
3. Overview . . . . .	5
4. Protocol Operation . . . . .	7
4.1. Add Route to MRIB . . . . .	7
4.2. Optimized Multicast Route Establishment . . . . .	7
4.3. Optimized Multicast Route Deletion . . . . .	9
5. Local Mobility Anchor Operation . . . . .	11
6. Mobile Access Gateway Operation . . . . .	11
7. Mobile Node Operation . . . . .	12
8. Message Format Extension . . . . .	12
8.1. Proxy Binding Update with Source Address Finding Extension . . . . .	12
8.2. Proxy Binding Acknowledgement Message with Source Address Finding Extension . . . . .	13
8.3. Care-of Address Option . . . . .	14
9. Security Considerations . . . . .	15
10. IANA Considerations . . . . .	15
11. Normative References . . . . .	15
Authors' Addresses . . . . .	16

## 1. Introduction

Proxy Mobile IPv6 (PMIPv6) [RFC5213] enables network-based mobility for IPv6 mobile nodes (MNs) that do not implement any mobility protocols. The Local Mobility Anchor (LMA) is the topological anchor point to manages the mobile node's binding state. The Mobile Access Gateway (MAG) is an access router or gateway that manages the mobility- related signaling for an MN. An MN is attached to the Proxy Mobile IPv6 Domain (PMIPv6-Domain) that includes LMA and MAG(s), and is able to receive data coming from outside of the PMIPv6-Domain through LMA and MAG.

Network-based mobility support for unicast is addressed in [RFC5213], while multicast support in PMIPv6 is not discussed in it. Since LMA and MAG set up a bi-directional IPv6-in-IPv6 tunnel for each mobile node and forwards all mobile node's traffic according to [RFC5213], it highly wastes network resources when a large number of mobile nodes join/ subscribe the same multicast sessions/channels, because independent data copies of the same multicast packet are delivered to the subscriber nodes in a unicast manner through MAG.

In order to deploy the multicast service in the PMIPv6 network, many schemes have been proposed:

The base solution described in [RFC6224] provides options for deploying multicast listener functions in PMIPv6-Domains without modifying mobility and multicast protocol standards. However, in this specification, MAG MUST act as an MLD proxy [RFC4605] and hence MUST dedicate a tunnel link between LMA and MAG to an upstream interface for all multicast traffic. It requires all the LMA to forward multicast packets to MAG via PMIPv6 tunnel which can be suboptimal.

[draft-zuniga-multimob-pmipv6-ropt-01]uses a multicast tree mobility anchor(MTMA) as the topological anchor point for multicast traffic, as well as a direct routing option where the MAG can provide access to multicast content in the local network.All the multicast traffic has to go through the MAG-MTMA tunnel which result in suboptimal multicast routing path like the base solution.And the direct routing solution needs native multicasting infrastructure as a requirement

[draft-asaeda-multimob-pmip6-extension-07]describes PMIPv6 extensions to support IP multicast communication for mobile nodes in PMIPv6-Domain.If the LMA is the upstream router for the channel(s) for the MAG, the MAG encapsulates PIM Join/Prune messages using the LMA-MAG bi-directional tunnel. The multicast data has to always go through the LMA-MAG bi-directional tunnel.It does solve the tunnel convergence problem and source mobility,But when multicast source is

a mobile node in the same PMIPv6 domain, using the proposed scheme mentioned above, the routing path through a multicast anchor (LMA) tends to be longer, which results in non-optimal multicast routes and performance degradation. Figure 1 shows the Architecture of Multicast Deployment with listener and source in the same PMIPv6 domain. LMA will receive all multicast traffic originating from its associated MN-S through LMA-MAG2 bi-directional tunnel, and then forward to multicast listener MN through LMA-MAG1 bi-directional tunnel, causing non-optimal multicast routes.

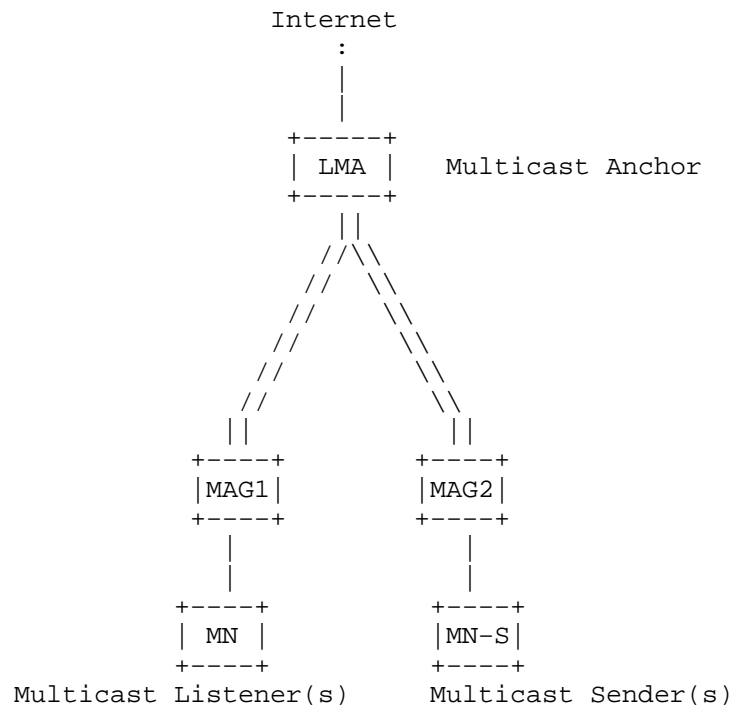


Figure1 Architecture of Multicast Deployment with listener and source in the same PMIPv6 domain

In this document, we discuss how to establish optimized multicast routes for the deployment scenario provided by Figure 1. The proposed protocol assumes that both LMA and MAG enable the Protocol-Independent Multicast - Sparse Mode (PIM-SM) multicast routing protocol [RFC4601], and further MAG MUST operate as an "SSM-aware" router [RFC4604]. The proposed protocol supports seamless handover. It can cooperate with local routing and direct routing to deliver IP multicast packets for mobile nodes and source mobility. In this document, because multicast localized routing is mainly focused on, the detail specification of source mobility and is not described.



## 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

The following terms used in this document are to be interpreted as defined in [RFC5213]; Home Address (HoA), Mobile Access Gateway (MAG), Local Mobility Anchor (LMA), Mobile Node (MN), Proxy Mobile IPv6 Domain (PMIPv6-Domain), LMA Address (LMAA), Proxy Care-of Address (Proxy-CoA), Proxy Binding Update (PBU), and Proxy Binding Acknowledgement (PBA).

Terms DR (Designated Router), MRIB (Multicast Routing Information Base), RPF (Reverse Path Forwarding), RPF Neighbor, SPT (shortest-path tree), PIM Join, Pim Prune, iif (incoming interface), oiflist (outgoing interface list), Source-Specific Multicast (SSM) are to be interpreted as defined in [RFC4601]

## 3. Overview

In the SSM case, the multicast receivers actively send the (HoA,G) subscribe message, for the LMA is just the topological anchor point of the source's Home Address (HoA) in the PMIPv6 network.

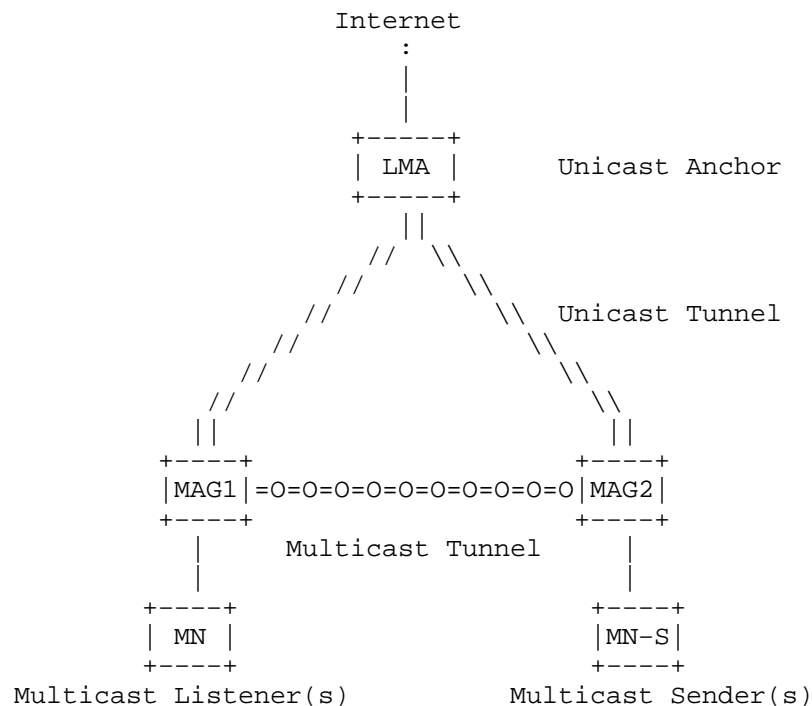


Figure 2 Architecture of Optimized Multicast Routing

As shown in Figure 2, MN (the multicast receivers) and MN-S (the multicast senders) are both mobile nodes in the same PMIPv6 domain; they both have binding cache entries in the LMA. MN sends (HoA, G) subscribe messages (MLD Report messages) specifying sender and multicast addresses to the access link to establish the SPT; the MN has to operate as an "SSM-aware" host [RFC4604]. On receiving the (HoA, G) subscribe message from the MN, the attached MAG1 sends a PBU-F message to LMA to find the CoA (i.e., IP address of MAG2) of MN-S. On the reception of PBU-F, the LMA responds with a PBA-F message including the CoA of MN-S to MAG1, after lookup of its binding cache entry. After acquiring the CoA of MN-S, MAG1 establishes a bi-directional tunnel with MAG2, and sends PIM Join messages to MAG2 through this tunnel; MAG1 and MAG2 establish the related multicast state for MN. So the MAG-based SPT is established successfully and the subsequent multicast data flow will be transmitted through the MAG-based SPT which is represented by "=0" in Figure 2. Unicast data flow will be transmitted through the base PMIPv6 tunnel which is represented by "||" in Figure 2.

The tunnel between MAG1 and MAG2 is used for multicast packets (including signaling and data flow) transmission only.

As described in [RFC4601], on receipt of data from S to G on interface iif (incoming interface of the packet), the DR will firstly check whether the source is directly connected and the iif is identical to the Reverse Path Forwarding (RPF) interface. As shown in Figure 2 ,MAG2 is the DR of MN-S,MAG1 is the DR of MN.After tunnel establishment between MAG1 and MAG2, MAG1 add the tunnel route to the MRIB,the RPF check will be successful.

this draft considers that every MN demanding multicast-only services is previously registered in a PMIPv6 unicast domain to get a unicast IP address.

#### 4. Protocol Operation

##### 4.1. Add Route to MRIB

In PIM-SM, the MRIB is used to decide where to send Join/Prune messages. on receiving the MLD Report message from MN,the MAG of MN has to choose a RPF Neighbor that the MRIB indicates should be used to forward packets to,and then send the Join/Prune message to the RPF Neighbor.

After tunnel establishment between MAG1 and MAG2, MAG1 add the tunnel route to the MRIB,so the RPF Neighbor of MAG1 is MAG2,MAG1 send PIM Join/Prune message through this tunnel.

Once the multicast subscription information is retrieved from the pMAG, the LMA encapsulates it in the PBA message by using the TLV option "Active Multicast Subscription", and forwards the PBA message to the nMAG. Then, the nMAG can subscribe the multicast flow on behalf of the MN, if there is no other MN receiving it already at the nMAG."

When the MAG is connected with other PIM-SM router not over LMA, there's no problem. PIM-SM establishes multicast routing path using RPF algorithm through reflecting MAG's RIB.

But when the MAG is connected with several LMAs including PIM-SM, MRIB SHOULD get information from PMIP routing table but "MAG's RIB doesn't reflect PMIP routing" (Thomas and Hitoshi agreed it).

##### 4.2. Optimized Multicast Route Establishment

This document provides the multicast routes optimization scheme.The procedures are described as follows and illustrated in Figure 3;

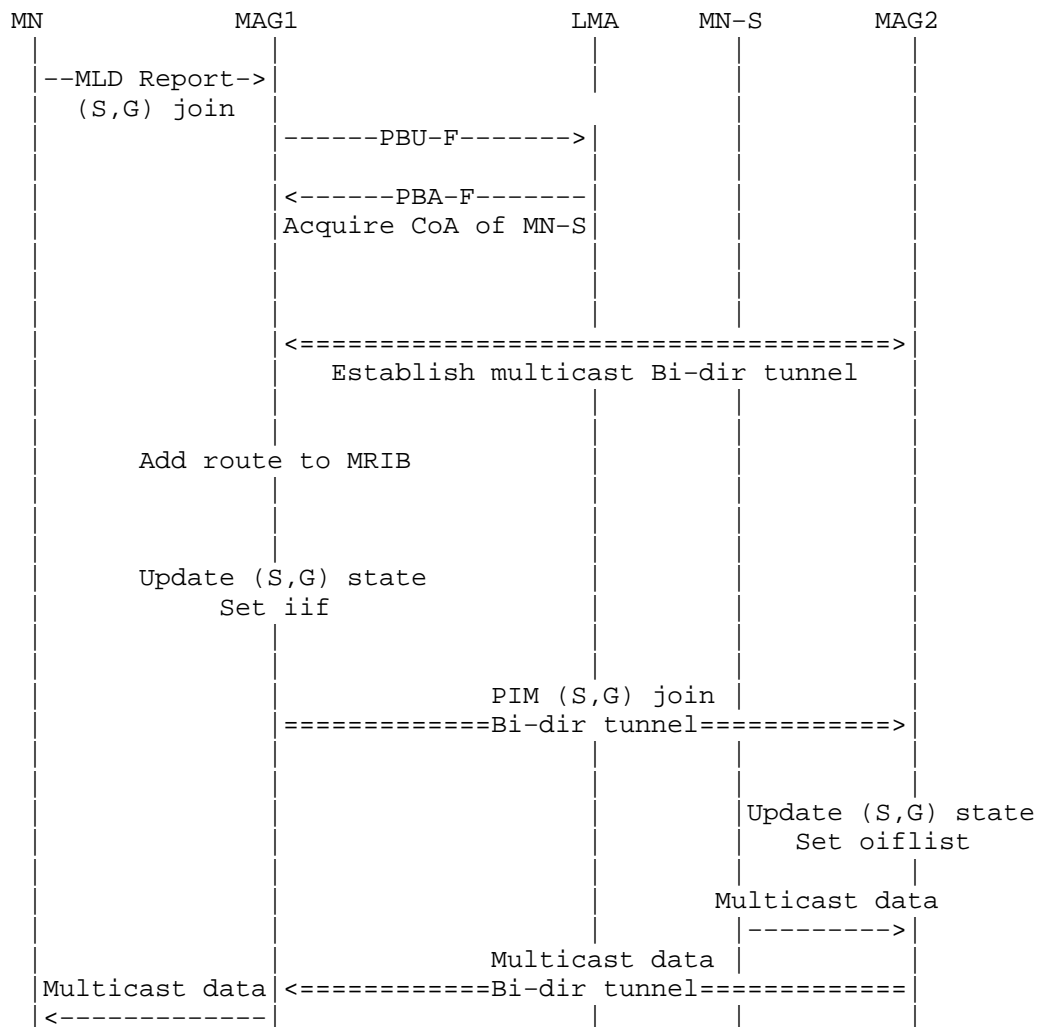


Figure3 Procedure of establishing multicast Route

1.MN sends (HoA,G) subscribe message(MLD Report messages) specifying sender and multicast addresses to the access link.

2.On receiving the (HoA,G) subscribe message from the MN,the attached MAG1 sends a PBU-F message to LMA to find the CoA (i. e., IP address of MAG2) of MN-S.

3.On the reception of PBU-F, the LMA responds with a PBA-F message including the CoA of MN-S to MAG1, after lookup of its binding cache entry.

4. After acquire the CoA of MN-S, MAG1 establish bi-directional tunnel with MAG2. Refer to [RFC5213] for the detailed tunnel negotiation mechanism.

5. After tunnel establishment, MAG1 add the tunnel route to the MRIB, so the RPF Neighbor of MAG1 is MAG2.

6. If there are multicast channels the MN has subscribed but MAG1 has not yet subscribed, MAG1 establishes multicast state for MN, and sets the iif of the multicast state as MAG1-MAG2 tunnel interface. If MAG1 already subscribed the channel, MAG1 updates the iif of the multicast state as MAG1-MAG2 tunnel interface.

7. MAG1 joins the corresponding multicast channels by sending the PIM Join message to the RPF Neighbor MAG2 through the MAG1-MAG2 tunnel.

8. On the reception of PIM Join message from MAG1, If MAG2 has not yet subscribed the multicast channel, MAG2 establishes multicast state for the channel, and adds the MAG2-MAG1 tunnel interface to the oiflist of the multicast state. If MAG2 already subscribed the channel, MAG2 updates the oiflist of the multicast state by adding the MAG2-MAG1 tunnel interface to the oiflist.

9. The subsequent multicast data flow will be transmitted through the optimized multicast route (MAG1-MAG2 bi-directional tunnel).

#### 4.3. Optimized Multicast Route Deletion

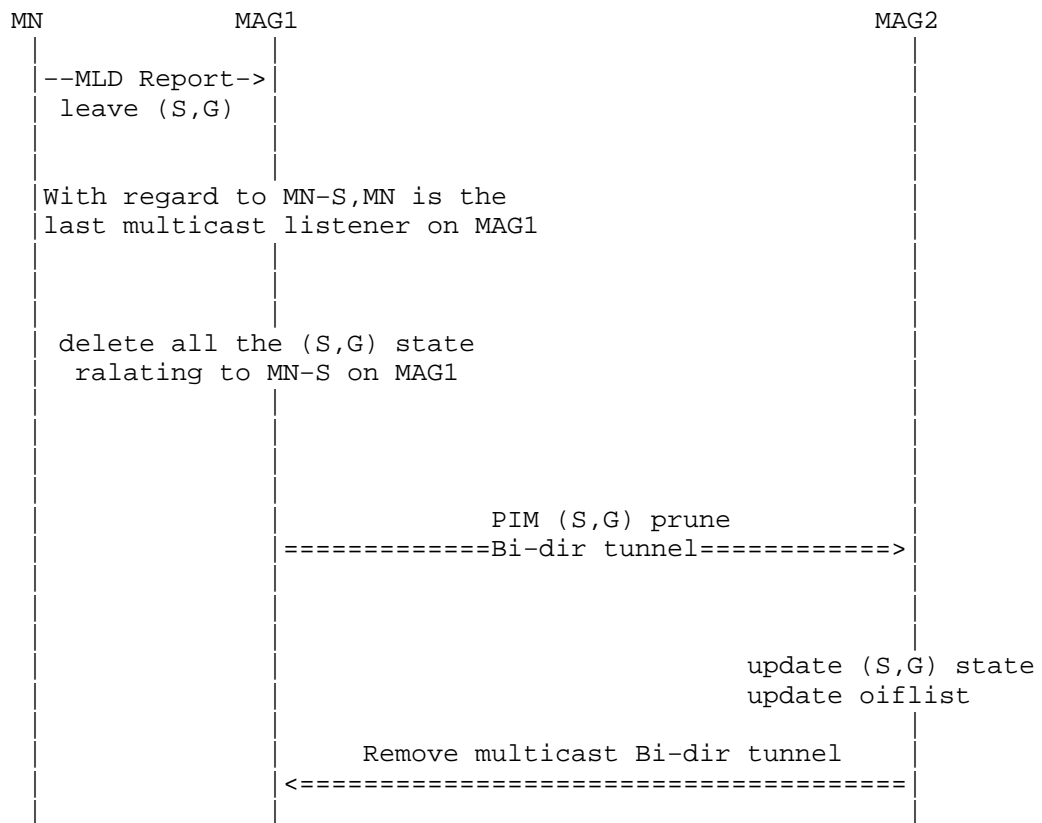


Figure4 Procedure of deleting multicast Route

1. MN sends (HoA,G) leave message (MLD Report messages) specifying sender and multicast addresses to the access link.
2. On receiving the (HoA,G) leave message from the MN, if MAG1 figures that MN is the last multicast listener subscribed to the MN-S, MAG1 performs the following steps; otherwise, MAG1 simply deletes the multicast state of MN as normal.
3. MAG1 deletes all the multicast state related to MN-S.
4. MAG1 removes the tunnel route from the MRIB and leaves the corresponding multicast channels by sending the PIM Prune message to the RPF Neighbor MAG2 through the MAG1-MAG2 tunnel.
5. On the reception of PIM Prune message from MAG1, MAG2 updates the oiflist of the multicast state by removing the MAG2-MAG1 tunnel interface from the oiflist.

6. Remove bi-directional tunnel between MAG1 and MAG2. Refer to [RFC5213] for the detailed tunnel negotiation mechanism.

## 5. Local Mobility Anchor Operation

On receiving a PBU-F message from MAG, the LMA must perform the following operations.

1. Check if the PBU-F message contains the F flag set to 1.
2. Find the CoA of MN-S by looking up the binding cache of LMA.
3. If the corresponding HoA-CoA entry is found in the binding cache, LMA will respond to MAG of MN with a PBA-F message containing a success indication. Otherwise, if not found, LMA will respond with the PBA-F containing a failure indication.

The responding PBA-F message from LMA to MAG of MN is constructed as follows.

1. Source address field in the IP header must be set to IP address of LMA
2. Destination address field in the IP header must be set to IP address of the MAG of MN
3. The PBA message MUST include the CoA of MN-S.

## 6. Mobile Access Gateway Operation

The MAG MUST operate as an "SSM-aware" router. [RFC4604] provide the behavior of an "SSM-aware" router.

The PBU-F message from MAG to LMA MUST be constructed, as specified below.

1. Source address field in the IP header must contain the IP address of MAG.
2. Destination address field in the IP header must contain the IP address of LMA.
3. The PBU-F message must include the HoA of MN-S.

On receiving a PBA-F message from LMA, MAG1(MAG of MN) MUST perform the following operations.

1. Check if the PBA-F message contains the F flag set to 1.
2. MAG1 MUST establish a tunnel with MAG2(MAG of MN-S) for muticast data delivery.
- 3.MAG1 MUST add route to Multicast Routing Information Base (MRIB) and send PIM Join/Prune messages through MAG1-MAG2 tunnel interface.
- 4.MAG1 MUST create/update multicast state for MN,the iif of the multicast state MUST be set to MAG1-MAG2 tunnel interface.

On receiving a PIM Join/Prune messages from MAG2-MAG1 tunnel interface,MAG2 MUST create/update multicast state for MN.

- 1.Add MAG2-MAG1 tunnel interface to the oiflist of the multicast state on receiving a PIM Join message from MAG2-MAG1 tunnel interface.
- 2.Delete MAG2-MAG1 tunnel interface from the oiflist of the multicast state on receiving a PIM Prune message from MAG2-MAG1 tunnel interface.

## 7. Mobile Node Operation

In this document,MN's MAG acquire MN-S's CoA from LMA according to MN-S's HoA,so A mobile node sends MLD Report messages including source and multicast addresses when it subscribes a multicast channel.

The MN MUST operate as an "SSM-aware" host . [RFC4604] provide the behavior of an "SSM-aware" host.

## 8. Message Format Extension

### 8.1. Proxy Binding Update with Source Address Finding Extension



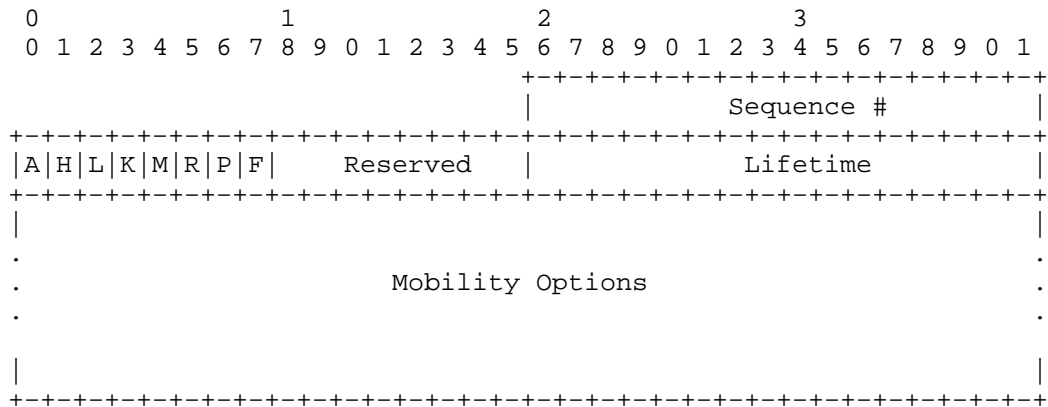


Figure5 Proxy Binding Update with Source Address Finding Extension

A Binding Update message that is sent by MAG to LMA is referred to as the "Proxy Binding Source Address Finding" message. A new flag (F) is included in the Proxy Binding Update message with Source Address Finding extension (PBU-F). The rest of the Binding Update message format remains the same as defined in[RFC3775] and with the additional (R), (M), and (P) flags, as specified in [RFC3963], [RFC4140], and [RFC5213], respectively.

#### Source Address Finding Flag

A new flag (F) is included in the Binding Update message to indicate to LMA that the Binding Update message is a Source Address Finding message. In the normal PMIP operation, the flag must be set to 0.

The PBU-F message is transferred for finding the MN-S's care-of address. The rest of the PBU message remains unchanged.

#### 8.2. Proxy Binding Acknowledgement Message with Source Address Finding Extension

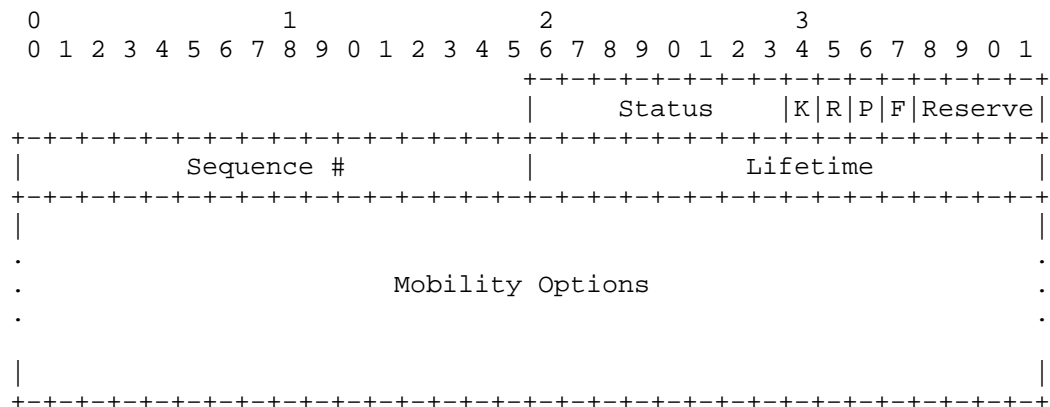


Figure6 Proxy Binding Update with Source Address Finding Extension

A "Proxy Binding Acknowledgement" message is sent from LMA to MAG in response to a Proxy Binding Update message. A new flag (F) is included in the Proxy Binding Acknowledgement message with Source Address Finding extension (PBA-F). The rest of the Binding Acknowledgement message format remains the same as defined in [RFC3775] and with the additional (R) flag, as specified in [RFC3963] and [RFC5213], respectively.

## Source Address Finding Flag

A new flag (F) is included in the Binding Acknowledgement message to indicate to MAG that the Binding Acknowledgement message is a Source Address Finding message. In the normal PMIP operation, the flag must be set to 0.

When (F) flag is specified in PBA-F message, the mobility options field includes "MN-S's care-of address"(Section 8.3).

### 8.3. Care-of Address Option

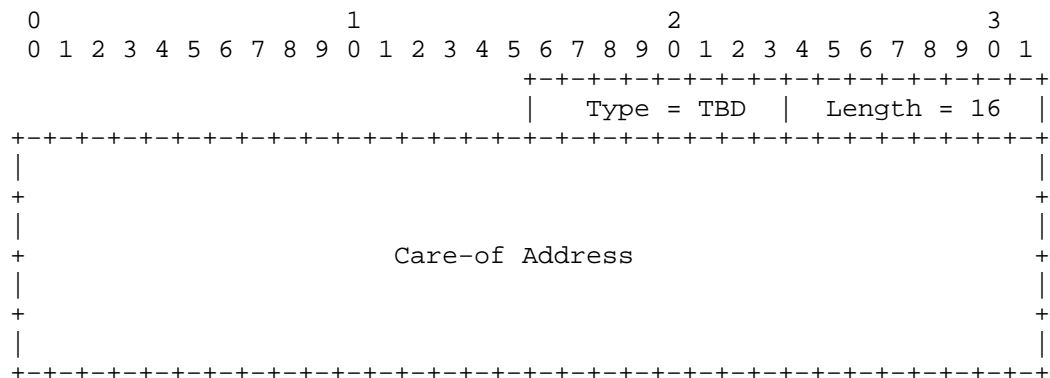


Figure7 Care-of Address Option

The Care-of Address field contains the care-of address of MN-S.

This option is valid only in PBA-F message. On the reception of PBU-F, the LMA responds with a PBA-F message including the Care-of Address Option.

## 9. Security Considerations

TBD

## 10. IANA Considerations

## 11. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", January 2005.
- [RFC4140] Soliman, H., Castelluccia, C., El Malki, K., and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", August 2005.
- [RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas,

"Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", August 2006.

[RFC4604] Holbrook, H., Cain, B., and B. Haberman, "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast", August 2006.

[RFC4605] Fenner, B., He, H., Haberman, B., and H. Sandick, "Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")", August 2006.

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

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

[draft-asaeda-multimob-pmip6-extension-07]  
Asaeda, H., Seite, P., and J. Xia, "PMIPv6 Extensions for PIM-SM", October 2011.

[draft-zuniga-multimob-pmip6-ropt-01]  
Zuniga, J., Contreras, L., Bernardos, C., and S. Jeon, "Multicast Mobility Routing Optimizations for Proxy Mobile IPv6", October 2011.

#### Authors' Addresses

Juan Liu  
ZTE Corporation  
RD Building 1,Zijinghua Road No.68  
Yuhuatai District,Nanjing 210012  
P.R.China

Email: liu.juan45@zte.com.cn

Wen Luo  
ZTE Corporation  
RD Building 1,Zijinghua Road No.68  
Yuhuatai District,Nanjing 210012  
P.R.China

Wei Yan  
ZTE Corporation  
RD Building 1,Zijinghua Road No.68  
Yuhuatai District,Nanjing 210012  
P.R.China

Email: yan.wei@zte.com.cn



MULTIMOB Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: January 10, 2013

J. Liu  
W. Luo  
W. Yan  
ZTE Corporation  
July 9, 2012

Routes Optimization for Multicast Sender in Proxy Mobile IPv6 Domain  
draft-liu-multimob-pmipv6-multicast-ro-01

Abstract

To support IP multicasting in PMIPv6 domain, MULTIMOB WG has issued several proposals including the base solution, dedicated schemes and direct routing which requires all communications to go through the local mobility anchor(LMA), the dedicated server and the native multicasting infrastructure, respectively. As this can be suboptimal, this document describes multicast routes optimization mechanisms for multicast sender. Multicast sender attached to the same or different mobile access gateways(MAG) with multicast listener sends multicast data via the tunnel between the gateways without any dedicated devices or dependence of the native multicasting infrastructure. The MAG and the LMA are the mobility entities defined in the PMIPv6 protocol and act as PIM-SM routers.

Status of this Memo

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

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

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

This Internet-Draft will expire on January 10, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal

Provisions Relating to IETF Documents  
(<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

## Table of Contents

1. Introduction . . . . .	3
2. Terminology . . . . .	4
3. Overview . . . . .	5
4. Protocol Operation . . . . .	6
4.1. Add Route to MRIB . . . . .	6
4.2. Optimized Multicast Route Establishment . . . . .	7
4.3. Multicast Route Deletion . . . . .	8
5. Local Mobility Anchor Operation . . . . .	10
6. Mobile Access Gateway Operation . . . . .	10
6.1. MN1 and MN2 attach to the same MAG . . . . .	10
6.2. MN1 and MN2 attach to different MAG . . . . .	11
7. Mobile Node Operation . . . . .	11
8. Message Format Extension . . . . .	12
8.1. Proxy Binding Update with Source Address Query Extension . . . . .	12
8.2. Proxy Binding Acknowledgement Message with Source Address Query Extension . . . . .	12
8.3. Care-of Address Option . . . . .	13
9. Security Considerations . . . . .	14
10. IANA Considerations . . . . .	14
11. Normative References . . . . .	14
Authors' Addresses . . . . .	15



## 1. Introduction

Proxy Mobile IPv6 (PMIPv6) [RFC5213] enables network-based mobility for IPv6 mobile nodes (MNs) that do not implement any mobility protocols. The Local Mobility Anchor (LMA) is the topological anchor point to manages the mobile node's binding state. The Mobile Access Gateway (MAG) is an access router or gateway that manages the mobility- related signaling for an MN. An MN is attached to the Proxy Mobile IPv6 Domain (PMIPv6-Domain) that includes LMA and MAG(s), and is able to receive data coming from outside of the PMIPv6-Domain through LMA and MAG.

Network-based mobility support for unicast is addressed in [RFC5213], while multicast support in PMIPv6 is not discussed in it. In order to deploy the multicast service in the PMIPv6 domain, many schemes have been proposed:

The base solution described in [RFC6224] provides options for deploying multicast listener functions in PMIPv6-Domains without modifying mobility and multicast protocol standards. However, in this specification, MAG MUST act as an MLD proxy [RFC4605] and hence MUST dedicate a tunnel link between LMA and MAG to an upstream interface for all multicast traffic. It requires all the LMA to forward multicast packets to MAG via PMIPv6 tunnel which can be suboptimal.

[draft-ietf-multimob-pmipv6-ropt-00]uses a multicast tree mobility anchor(MTMA) as the topological anchor point for multicast traffic, as well as a direct routing option where the MAG can provide access to multicast content in the local network. All the multicast traffic has to go through the MAG-MTMA tunnel which result in suboptimal multicast routing path like the base solution. And the direct routing solution needs native multicasting infrastructure as a requirement.

[draft-ietf-multimob-pmipv6-source-00]describes the support of multicast senders in Proxy Mobile IPv6 domains. MLD proxy functions are deployed at the MAG. Multicast traffic MUST be tunneled up to the LMA of the multicast sender, transferred to the LMA of the multicast listener and then tunneled downwards to the MAG of the multicast listener. The problem is especially manifested when multicast listener and sender attach to the same MAG but different LMAs, the traffic has to go up to one LMA, cross over to the other LMA, and then be tunneled back to the same MAG, causing non-optimal multicast routes and redundant flows at the MAG. In the direct routing scenario, multicast traffic MUST be tunneled up to the common multicast router(MR) and then tunneled downwards to the MAG. In both scenarios, multicast traffic has to always go through the LMA-MAG or

MR-MAG bi-directional tunnel which can be suboptimal.

This document describes multicast routes optimization mechanisms for multicast sender. Figure 1 shows the Architecture of Multicast Deployment with listener and sender in the same PMIPv6 domain.

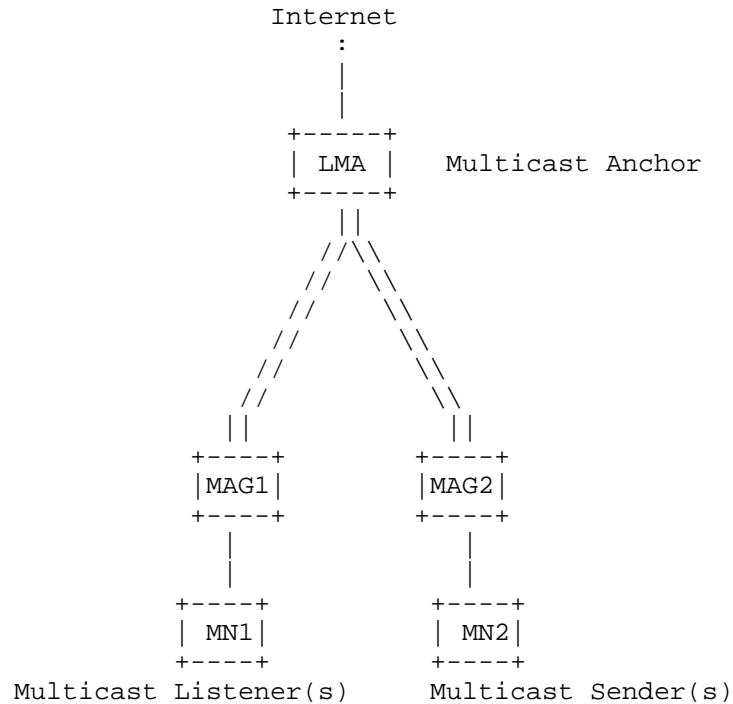


Figure1 Architecture of Multicast Deployment with listener and source in the same PMIPv6 domain

The proposed protocol assumes that both LMA and MAG enable the Protocol- Independent Multicast - Sparse Mode (PIM-SM) multicast routing protocol [RFC4601], and further MAG MUST operate as an "SSM-aware" router [RFC4604]. The proposed protocol supports seamless handover. In this document, because routes optimization for multicast sender is mainly focused on, the detail specification of source mobility is not described.

## 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

The following terms used in this document are to be interpreted as defined in [RFC5213]; Home Address(HoA), Mobile Access Gateway (MAG), Local Mobility Anchor (LMA), Mobile Node (MN), Proxy Mobile IPv6 Domain (PMIPv6-Domain), LMA Address (LMAA), Proxy Care-of Address (Proxy-CoA), Proxy Binding Update (PBU), and Proxy Binding Acknowledgement (PBA).

Terms DR(Designated Router), MRIB(Multicast Routing Information Base), RPF(Reverse Path Forwarding), RPF Neighbor, SPT(shortest-path tree), PIM Join, Pim Prune, iif(incoming interface),oiflist(outgoing interface list), Source-Specific Multicast(SSM) are to be interpreted as defined in[RFC4601]

### 3. Overview

In the SSM scenario, the multicast Listeners actively send the (S,G) subscribe message, S is the multicast sender's Home Address (HoA) .

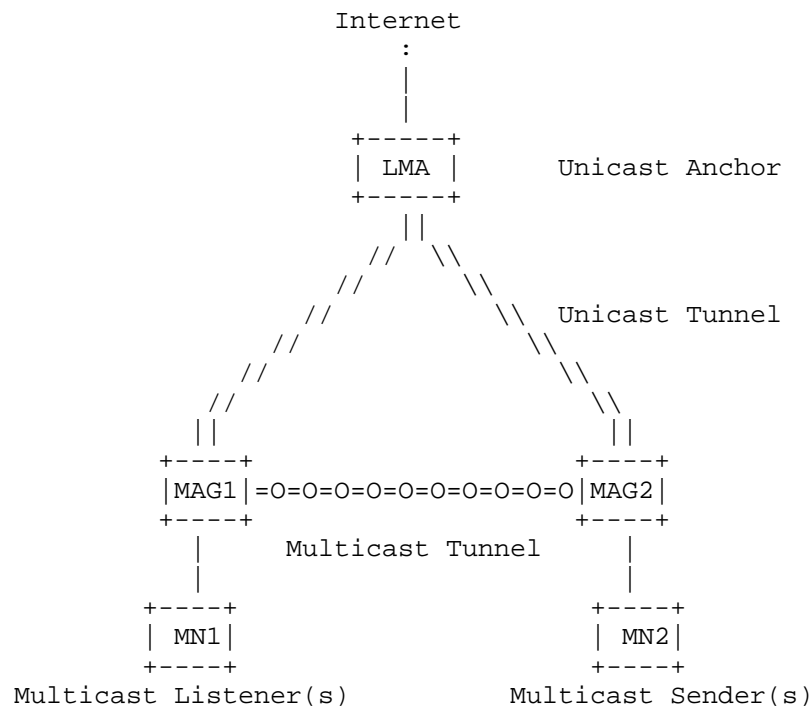


Figure2 Architecture of Optimized Multicast Routing

As shown in Figure 2, MN1(the multicast Listener) and MN2(the multicast sender) are both mobile nodes in the same PMIPv6 domain,

they both have binding cache entry in the LMA. MN1 sends (S,G) subscribe message(MLD Report messages) to the access link to establish the SPT, MN1 has to operate as an "SSM-aware" host [RFC4604]. On receiving the (S,G) subscribe message from MN1, the attached MAG1 sends a PBU-Q message to LMA to query the CoA (i. e., IP address of MAG2) of MN2. On the reception of PBU-Q, the LMA responds with a PBA-Q message including the CoA of MN2 to MAG1. After acquiring the CoA of MN2, MAG1 establishes bi-directional tunnel with MAG2, and sends PIM Join message to MAG2 through this tunnel, MAG1 and MAG2 establish the related multicast state. So the MAG-based SPT is established successfully and the subsequent multicast data flow will be transmitted through the MAG-based SPT which is represented by "=0" in Figure 2. Unicast data flow will be transmitted through base PMIPv6 tunnel which is represented by "||" in Figure 2.

The tunnel between MAG1 and MAG2 is used for multicast packets(including signaling and data flow) transmission only.

As described in [RFC4601], on receipt of data from S to G on interface iif (incoming interface of the packet), the DR will firstly check whether the source is directly connected and the iif is identical to the Reverse Path Forwarding (RPF) interface. As shown in Figure 2, MAG2 is the DR of MN2, MAG1 is the DR of MN1. After tunnel establishment between MAG1 and MAG2, MAG1 add the tunnel route to the MRIB, the RPF check will be successful.

This draft assumes that every MN supporting multicast service is previously registered in the PMIPv6 unicast domain to get a unicast IP address(HoA).

#### 4. Protocol Operation

##### 4.1. Add Route to MRIB

In PIM-SM, the MRIB is used to decide where to send Join/Prune messages. on receiving the MLD Report message from MN,the MAG of MN has to choose a RPF Neighbor that the MRIB indicates should be used to forward packets to, and then send the Join/Prune message to the RPF Neighbor.

After tunnel establishment between MAG1 and MAG2, MAG1 add the tunnel route to the MRIB, so that the RPF Neighbor of MAG1 is MAG2, MAG1 send PIM Join/Prune message through this tunnel.

#### 4.2. Optimized Multicast Route Establishment

This section provides the multicast routes optimization procedure. The procedures are described as follows and illustrated in Figure 3.

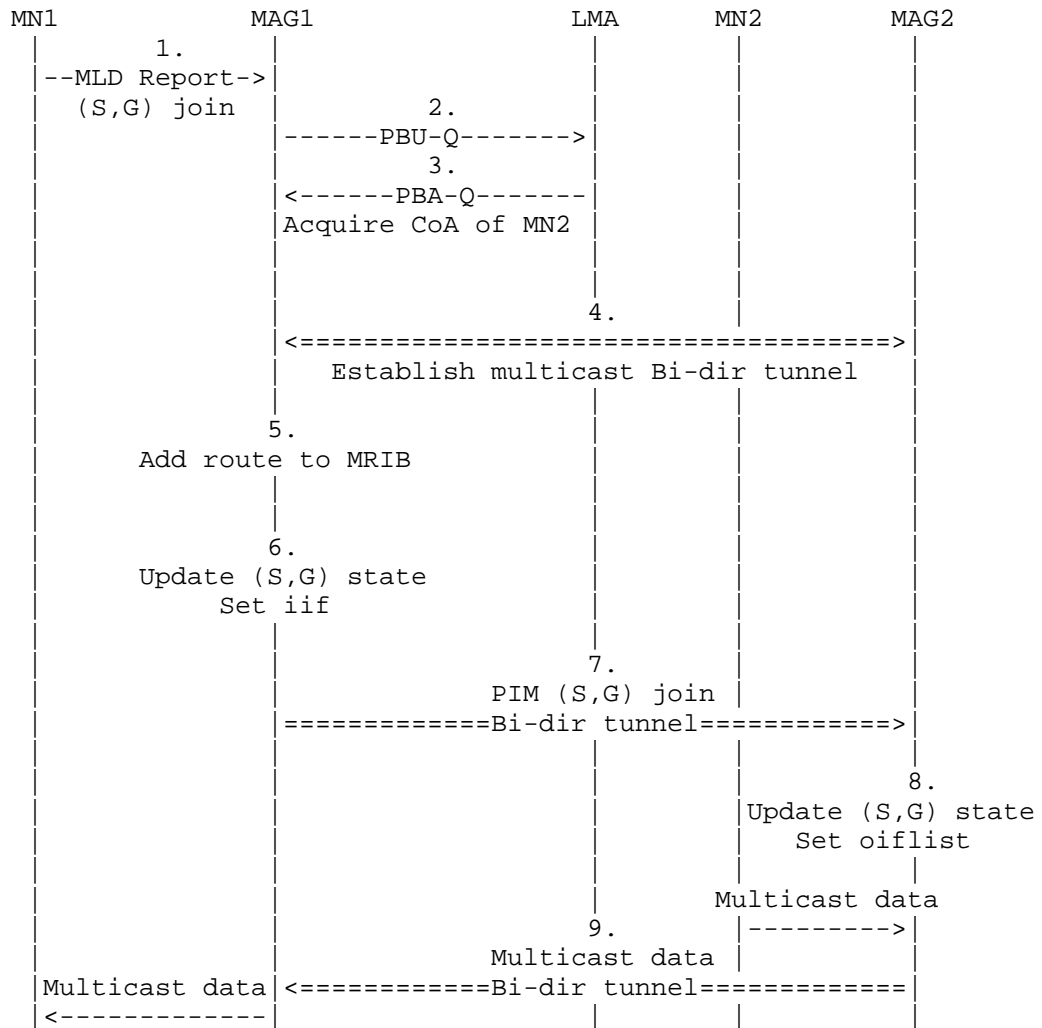


Figure3 Procedure of establishing multicast Route

1. MN1 sends (S,G) subscribe message to the access link, S is the HoA of MN2.

2. On receiving the (S,G) subscribe message from MN1, the attached MAG1 sends a PBU-Q message to LMA to query the CoA (i. e., IP address

of MAG2) of MN2.

3. On the reception of PBU-Q, the LMA responds with a PBA-Q message including the CoA of MN2.

4. After acquire the CoA of MN2, MAG1 establish bi-directional tunnel with MAG2. Refer to [RFC5213] for the detailed tunnel negotiation mechanism.

5. After tunnel establishment, MAG1 add the tunnel route to the MRIB, so that the RPF Neighbor of MAG1 is MAG2.

6. If there are multicast channels the MN1 has subscribed but MAG1 has not yet subscribed, MAG1 establishes multicast state for the channel, and sets the iif of the multicast state as MAG1-MAG2 tunnel interface. if MAG1 already subscribed the channel, MAG1 updates the iif of the multicast state as MAG1-MAG2 tunnel interface.

7. MAG1 joins the corresponding multicast channels by sending the PIM Join message to the RPF Neighbor MAG2 through the MAG1-MAG2 tunnel.

8. On the reception of PIM Join message from MAG1, If MAG2 has not yet subscribed the multicast channel, MAG2 establishes multicast state for the channel, and adds the MAG2-MAG1 tunnel interface to the oiflist of the multicast state. if MAG2 already subscribed the channel, MAG2 updates the oiflist of the multicast state by adding the MAG2-MAG1 tunnel interface to the oiflist.

9. The subsequent multicast data flow will be transmitted through the optimized multicast route (MAG1-MAG2 bi-directional tunnel).

#### 4.3. Multicast Route Deletion

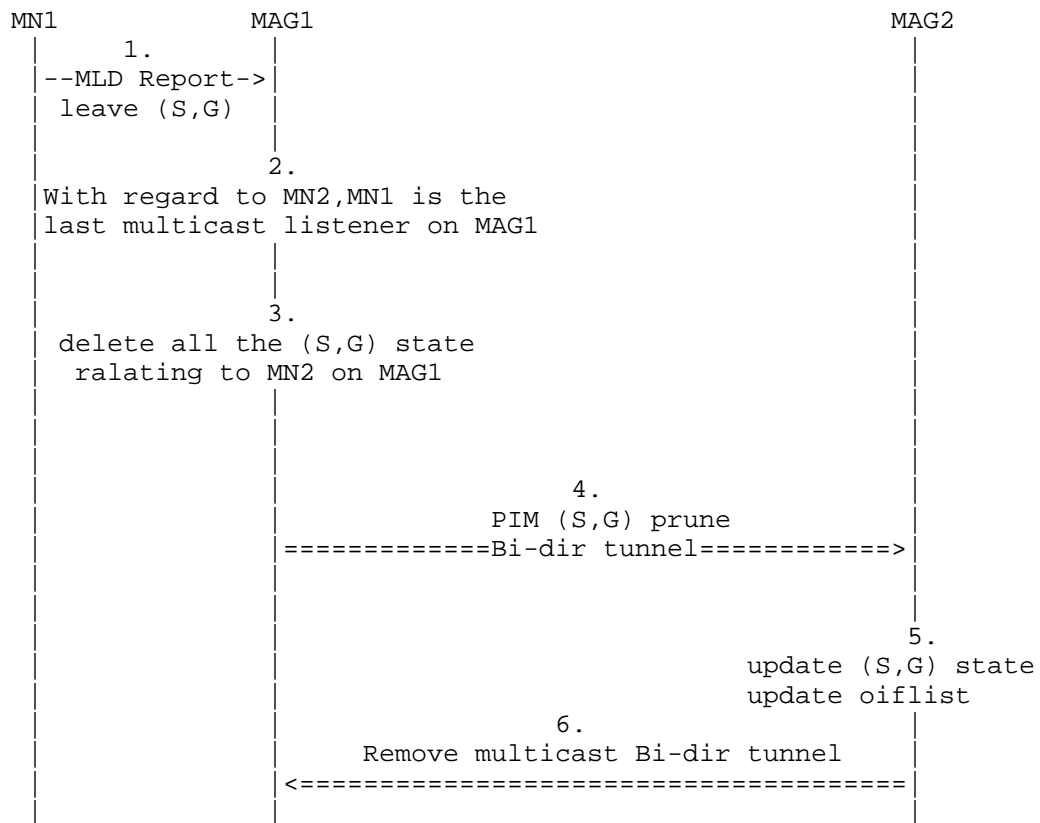


Figure4 Procedure of deleting multicast Route

1.MN1 sends (S,G) leave message(MLD Report messages) to the access link, S is the HoA of MN2.

2.On receiving the (S,G) leave message from the MN1, if MAG1 figures that MN1 is the last multicast listener subscribed to the MN2, MAG1 perform the following steps, otherwise, MAG1 simply delete the multicast state of MN1 as normal, which is removing MAG1-MN1 interface from the oiflist of the multicast state.

3.MAG1 delete all the multicast state related to MN2.

4.MAG1 remove the tunnel route from the MRIB and leave the corresponding multicast channels by sending the PIM Prune message to the RPF Neighbor MAG2 through the MAG1-MAG2 tunnel.

5.On the reception of PIM Prune message from MAG1, MAG2 updates the oiflist of the multicast state by removing the MAG2-MAG1 tunnel

interface from the oiflist.

6.Remove bi-directional tunnel between MAG1 and MAG2. Refer to [RFC5213] for the detailed tunnel negotiation mechanism.

## 5. Local Mobility Anchor Operation

On receiving a PBU-Q message from MAG1, the LMA must perform the following operations.

- 1.Check if the PBU-Q message contains the Q flag set to 1.
- 2.Query the CoA of MN2 by looking up the binding cache of LMA.
- 3.If the corresponding HoA-CoA entry is found in the binding cache, LMA will respond PBA-Q message containing a success indication. Otherwise, if not found, LMA will respond PBA-Q message containing a failure indication.

The responding PBA-Q message from LMA to MAG1 is constructed as follows.

- 1.Source address field in the IP header must be set to IP address of LMA.
- 2.Destination address field in the IP header must be set to IP address of the MAG1.
- 3.The PBA-Q message MUST include the CoA of MN2.

## 6. Mobile Access Gateway Operation

The MAG MUST operate as an "SSM-aware" router. [RFC4604] provide the behavior of an "SSM-aware" router.

### 6.1. MN1 and MN2 attach to the same MAG

On receiving the (S,G) subscribe message from the MN1, MAG1 could decide whether MN2 attaches to itself according to MN2's HoA which is included in the (S,G) subscribe message. If MAG1 figures that MN1 and MN2 both attach to it. MAG1 operates as below:

If there are multicast channels the MN1 has subscribed but MAG1 has not yet subscribed, MAG1 establishes multicast state for the channel, and adds the MAG1-MN1 interface to the oiflist of the multicast state.



If MAG1 already subscribed the channel, MAG1 updates the oiflist of the multicast state by adding the MAG1-MN1 interface to the oiflist.

MAG1 will send the multicast data flow from MN2 to MN1 locally.

#### 6.2. MN1 and MN2 attach to different MAG

The PBU-Q message from MAG1 to LMA MUST be constructed, as specified below.

1. Source address field in the IP header must contain the IP address of MAG1.

2. Destination address field in the IP header must contain the IP address of LMA.

3. The PBU-Q message must include the HoA of MN2.

On receiving a PBA-Q message from LMA, MAG1 MUST perform the following operations.

1. Check if the PBA-Q message contains the Q flag set to 1.

2. MAG1 MUST establish a tunnel with MAG2 for multicast data delivery.

3. MAG1 MUST add route to Multicast Routing Information Base (MRIB) and send PIM Join/Prune messages through MAG1-MAG2 tunnel interface.

4. MAG1 MUST create/update multicast state for the channel, the iif of the multicast state MUST be set to MAG1-MAG2 tunnel interface.

On receiving a PIM Join/Prune messages from MAG2-MAG1 tunnel interface, MAG2 MUST create/update multicast state for the channel.

1. Add MAG2-MAG1 tunnel interface to the oiflist of the multicast state on receiving a PIM Join message from MAG2-MAG1 tunnel interface.

2. Delete MAG2-MAG1 tunnel interface from the oiflist of the multicast state on receiving a PIM Prune message from MAG2-MAG1 tunnel interface.

#### 7. Mobile Node Operation

The MN MUST operate as an "SSM-aware" host . [RFC4604] provide the behavior of an "SSM-aware" host.

## 8. Message Format Extension

### 8.1. Proxy Binding Update with Source Address Query Extension

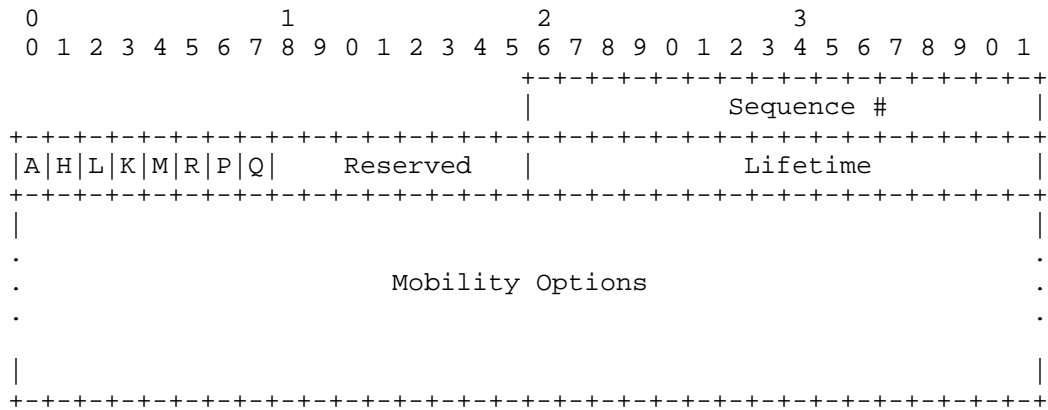


Figure5 Proxy Binding Update with Source Address Query Extension

A Binding Update message that is sent by MAG to LMA is referred to as the "Proxy Binding Source Address Query" message. A new flag (Q) is included in the Proxy Binding Update message with Source Address Query extension (PBU-Q). The rest of the Binding Update message format remains the same as defined in [RFC3775] and with the additional (R), (M), and (P) flags, as specified in [RFC3963], [RFC4140], and [RFC5213], respectively.

#### Source Address Query Flag

A new flag (Q) is included in the Binding Update message to indicate to LMA that the Binding Update message is a Source Address Query message. In the normal PMIP operation, the flag must be set to 0.

The PBU-Q message is transferred for querying the MN2's CoA. The rest of the PBU message remains unchanged.

### 8.2. Proxy Binding Acknowledgement Message with Source Address Query Extension

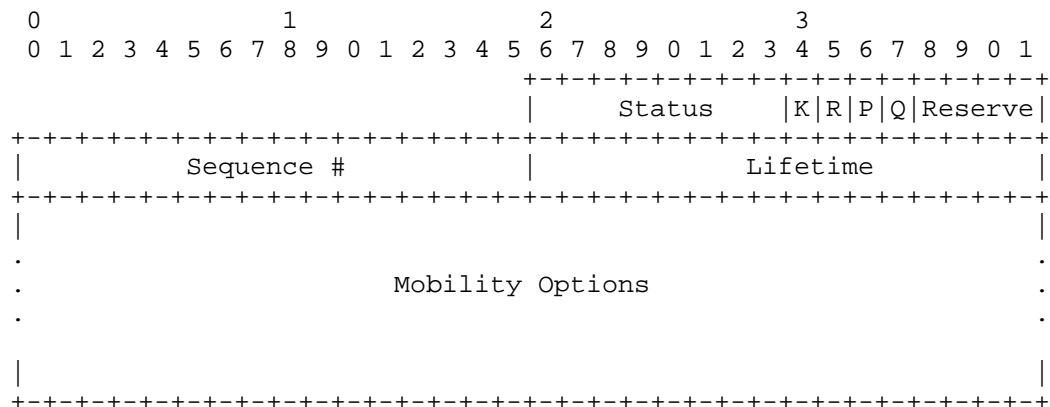


Figure6 Proxy Binding Update with Source Address Query Extension

A "Proxy Binding Acknowledgement" message is sent from LMA to MAG in response to a Proxy Binding Update message. A new flag (Q) is included in the Proxy Binding Acknowledgement message with Source Address Query extension (PBA-Q). The rest of the Binding Acknowledgement message format remains the same as defined in [RFC3775] and with the additional (R) flag, as specified in [RFC3963] and [RFC5213], respectively.

## Source Address Query Flag

A new flag (Q) is included in the Binding Acknowledgement message to indicate to MAG that the Binding Acknowledgement message is a Source Address Query message. In the normal PMIP operation, the flag must be set to 0.

When (Q) flag is specified in PBA-Q message, the mobility options field includes "MN2's CoA"(Section 8.3).

### 8.3. Care-of Address Option

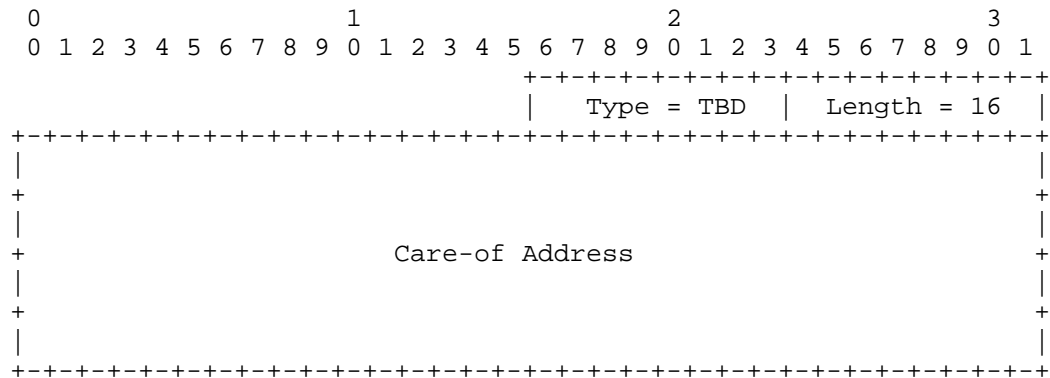


Figure7 Care-of Address Option

The Care-of Address field contains the care-of address of MN2.

This option is valid only in PBA-Q message. On the reception of PBU-Q, the LMA responds with a PBA-Q message including the Care-of Address Option.

## 9. Security Considerations

TBD

## 10. IANA Considerations

## 11. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", January 2005.
- [RFC4140] Soliman, H., Castelluccia, C., El Malki, K., and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", August 2005.
- [RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas,

"Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", August 2006.

[RFC4604] Holbrook, H., Cain, B., and B. Haberman, "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast", August 2006.

[RFC4605] Fenner, B., He, H., Haberman, B., and H. Sandick, "Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")", August 2006.

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

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

[draft-ietf-multimob-pmipv6-ropt-00]  
Zuniga, JC., Contreras, LM., Bernardos, CJ., and S. Jeon,  
"Multicast Mobility Routing Optimizations for Proxy Mobile IPv6", March 2012.

[draft-ietf-multimob-pmipv6-source-00]  
Schmidt, TC., Gao, S., Zhang, H., and M. Waehlis,  
"Mobile Multicast Sender Support in Proxy Mobile IPv6 (PMIPv6) Domains", January 2012.

#### Authors' Addresses

Juan Liu  
ZTE Corporation  
RD Building 1,Zijinghua Road No.68  
Yuhuatai District,Nanjing 210012  
P.R.China

Email: liu.juan45@zte.com.cn

Wen Luo  
ZTE Corporation  
RD Building 1,Zijinghua Road No.68  
Yuhuatai District,Nanjing 210012  
P.R.China

Email: [luo.wen@zte.com.cn](mailto:luo.wen@zte.com.cn)

Wei Yan  
ZTE Corporation  
RD Building 1,Zijinghua Road No.68  
Yuhuatai District,Nanjing 210012  
P.R.China

Email: [yan.wei@zte.com.cn](mailto:yan.wei@zte.com.cn)



MULTIMOB Group  
Internet-Draft  
Intended status: Standards Track  
Expires: November 9, 2012

T C. Schmidt  
HAW Hamburg  
M. Waehlich  
link-lab & FU Berlin  
R. Koodli  
Cisco Systems  
G. Fairhurst  
University of Aberdeen  
May 8, 2012

Multicast Listener Extensions for MIPv6 and PMIPv6 Fast Handovers  
draft-schmidt-multimob-fmipv6-pfmipv6-multicast-06

Abstract

Fast handover protocols for MIPv6 and PMIPv6 define mobility management procedures that support unicast communication at reduced handover latency. Fast handover base operations do not affect multicast communication, and hence do not accelerate handover management for native multicast listeners. Many multicast applications like IPTV or conferencing, though, are comprised of delay-sensitive real-time traffic and will benefit from fast handover execution. This document specifies extension of the Mobile IPv6 Fast Handovers (FMIPv6) and the Fast Handovers for Proxy Mobile IPv6 (PFMIPv6) protocols to include multicast traffic management in fast handover operations. This multicast support is provided first at the control plane by a management of rapid context transfer between access routers, second at the data plane by an optional fast traffic forwarding that MAY include buffering.

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 November 9, 2012.



## Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	4
2. Terminology . . . . .	5
3. Protocol Overview . . . . .	5
3.1. Multicast Context Transfer between Access Routers . . . . .	6
3.2. Protocol Operations Specific to FMIPv6 . . . . .	8
3.3. Protocol Operations Specific to PFMIPv6 . . . . .	10
4. Protocol Details . . . . .	13
4.1. Protocol Operations Specific to FMIPv6 . . . . .	13
4.1.1. Operations of the Mobile Node . . . . .	13
4.1.2. Operations of the Previous Access Router . . . . .	14
4.1.3. Operations of the New Access Router . . . . .	15
4.2. Protocol Operations Specific to PFMIPv6 . . . . .	15
4.2.1. Operations of the Mobile Node . . . . .	15
4.2.2. Operations of the Previous MAG . . . . .	15
4.2.3. Operations of the New MAG . . . . .	16
4.2.4. IPv4 Support Considerations . . . . .	17
5. Message Formats . . . . .	18
5.1. Multicast Indicator for Proxy Router Advertisement (PrRtAdv) . . . . .	18
5.2. Extensions to Existing Mobility Header Messages . . . . .	18
5.3. New Multicast Mobility Option . . . . .	18
5.4. New Multicast Acknowledgement Option . . . . .	20
5.5. Length Considerations: Number of Records and Addresses . . . . .	22
5.6. MLD (IGMP) Compatibility Aspects . . . . .	22
6. Security Considerations . . . . .	22
7. IANA Considerations . . . . .	23
8. Acknowledgments . . . . .	23
9. References . . . . .	23
9.1. Normative References . . . . .	23
9.2. Informative References . . . . .	24

Appendix A. Change Log . . . . .	25
Authors' Addresses . . . . .	26

## 1. Introduction

Mobile IPv6 [RFC3775] defines a network layer mobility protocol involving mobile nodes participation, while Proxy Mobile IPv6 [RFC5213] provides a mechanism without requiring mobility protocol operations at a Mobile Node (MN). Both protocols introduce traffic disruptions on handovers that may be intolerable in many application scenarios. Mobile IPv6 Fast Handovers (FMIPv6) [RFC5568], and Fast Handovers for Proxy Mobile IPv6 (PFMIPv6) [RFC5949] improve these handover delays for unicast communication to the order of the maximum delay needed for link switching and signaling between Access Routers (ARs) or Mobile Access Gateways (MAGs) [FMIPv6-Analysis].

No dedicated treatment of seamless multicast data reception has been proposed by any of the above protocols. MIPv6 only roughly defines multicast for Mobile Nodes using a remote subscription approach or a home subscription through bi-directional tunneling via the Home Agent (HA). Multicast forwarding services have not been specified at all in [RFC5213], but are subject to current specification [RFC6224]. It is assumed throughout this document that mechanisms and protocol operations are in place to transport multicast traffic to ARs. These operations are referred to as 'JOIN/LEAVE' of an AR, while the explicit techniques to manage multicast transmission are beyond the scope of this document.

Mobile multicast protocols need to serve applications such as IPTV with high-volume content streams to be distributed to potentially large numbers of receivers, and therefore should preserve the multicast nature of packet distribution and approximate optimal routing [RFC5757]. It is undesirable to rely on home tunneling for optimizing multicast. Unencapsulated, native multicast transmission requires establishing forwarding state, which will not be transferred between access routers by the unicast fast handover protocols. Thus multicast traffic will not experience expedited handover performance, but an MN - or its corresponding MAG in PMIPv6 - can perform remote subscriptions in each visited network.

This document specifies extensions of FMIPv6 and PFMIPv6 for including multicast traffic management in fast handover operations. The solution common to both underlying protocols defines the per-group transfer of multicast contexts between ARs or MAGs. The protocol defines corresponding message extensions necessary for carrying group context information independent of the particular handover protocol. ARs or MAGs are then enabled to treat multicast traffic according to fast unicast handovers and with similar performance. No protocol changes are introduced that prevent a multicast unaware node from performing fast handovers with multicast aware ARs or MAGs.

This specification is applicable when a mobile node has joined and maintains one or several multicast group subscriptions prior to undergoing a fast handover. It does not introduce any requirements on the multicast routing protocols in use, nor are the ARs or MAGs assumed to be multicast routers. It assumes network conditions, though, that allow native multicast reception in both, the previous and new access network. Methods to bridge regions without native multicast connectivity are beyond the scope of this document.

## 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119]. The use of the term, "silently ignore" is not defined in RFC 2119. However, the term is used in this document and can be similarly construed.

This document uses the terminology of [RFC5568], [RFC5949], [RFC3775], and [RFC5213]. In addition, the following terms are introduced:

## 3. Protocol Overview

The reference scenario for multicast fast handover is illustrated in Figure 1.

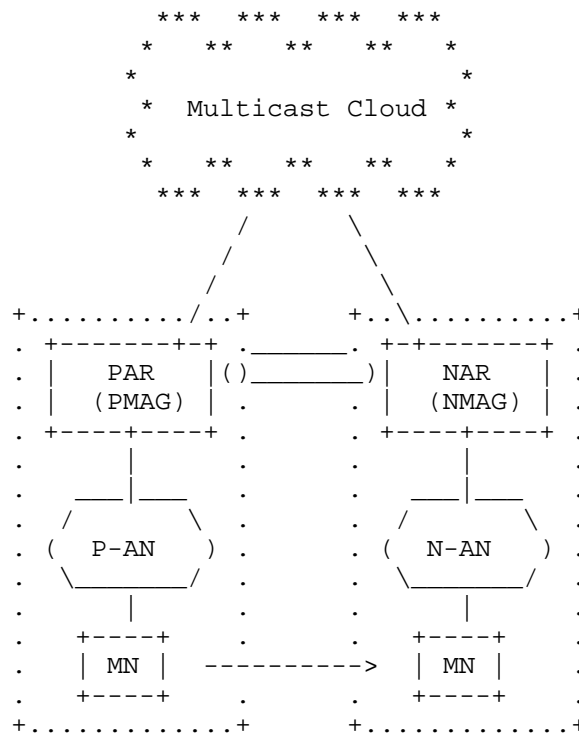


Figure 1: Reference Network for Fast Handover

### 3.1. Multicast Context Transfer between Access Routers

In a fast handover scenario (cf. Figure 1), ARs/MAGs establish a mutual binding and provide the capability to exchange context information concerning the MN. This context transfer will be triggered by detecting MN's forthcoming move to a new AR and assist the MN to immediately resume communication on the new subnet link using its previous IP address. In contrast to unicast, multicast stream reception does not primarily depend on address and binding cache management, but requires distribution trees to adapt so that traffic follows the movement of the MN. This process may be significantly slower than fast handover management [RFC5757]. Multicast listeners at handover may take the twofold advantage of including the multicast groups under subscription in context transfer. First, the NAR can proactively join the desired groups as soon as it gains knowledge of them. Second, multicast streams MAY be included in traffic forwarding via the tunnel established from PAR to NAR.

There are two modes of operation in FMIPv6 and in PFMIPv6. The

predictive mode allows for AR-binding and context transfer prior to an MN handover, while in the reactive mode, these steps are executed after detection that the MN has re-attached to NAR. Details of the signaling schemes differ between FMIPv6 and PFMIPv6 and are outlined in Section 3.2 and Section 3.3.

In a predictive fast handover, the access router (i.e., PAR (PMAG) in Figure 1) learns about the impending movement of the MN and simultaneously about the multicast group context as specified in Section 3.2 and Section 3.3. Thereafter, PAR will initiate an AR-binding and context transfer by transmitting a HI message to NAR (NMAG). HI is extended by multicast group states carried in mobility header options as defined in Section 5.3. On reception of the HI message, NAR returns a multicast acknowledgement in its HACK answer that indicates its ability to support each requested group (see Section 5.4). NAR (NMAG) expresses its willingness to receive multicast traffic from forwarding by PAR using standard MLD signaling. There are several reasons to waive forwarding, e.g., the group could already be under native subscription or capacity constraints can hinder decapsulation of additional streams at the NAR. On the previous network side, forwarding of multicast traffic can be in conflict with capacity or policy constraints of PAR.

For the groups requested, PAR MAY add the tunnel interface to its multicast forwarding database, so that multicast streams can be forwarded in parallel to unicast traffic. NAR, taking the role of an MLD proxy [RFC4605] with upstream router PAR, will submit an MLD report on this upstream tunnel interface to request the desired groups, but will terminate multicast forwarding [RFC3810] from PAR, as soon as group traffic natively arrives. In addition, NAR immediately joins all groups that are not already under subscription using its native multicast upstream interface and loopback as downstream. It starts to downstream multicast forwarding after the MN has arrived.

In a reactive fast handover, PAR will learn about the movement of the MN, after the latter has re-associated with the new access network. Also from the new link, it will be informed about the multicast context of the MN. As group membership information are present at the new access network prior to context transfer, MLD join signaling can proceed in parallel to HI/HACK exchange. Following the context transfer, multicast data can be forwarded to the new access network using the PAR-NAR tunnel of the fast handover protocol. Depending on the specific network topology though, multicast traffic for some groups may natively arrive before it is forwarded from PAR.

In both modes of operation, it is the responsibility of the PAR (PMAG) to properly react on the departure of the MN in the context of

local group management. Depending on the multicast state management, link type and MLD parameters deployed (cf., [RFC5757]), it is requested to take appropriate actions to adjust multicast service to requirements of the remaining nodes.

In this way, the MN will be able to participate in multicast group communication with a handover performance comparable to that for unicast, while network resource consumption is minimized.

### 3.2. Protocol Operations Specific to FMIPv6

ARs that provide multicast support in FMIPv6 will advertise this general service by setting an indicator bit (M-bit) in its PrRtAdv message as defined in Section 5.1. Additional details about the multicast service support, e.g., flavors and groups, will be exchanged within HI/HACK dialogs later at handovers.

An MN operating FMIPv6 will actively initiate the handover management by submitting a fast binding update (FBU). The MN, which is aware of the multicast groups it wishes to maintain, will attach mobility options containing its group states (see Section 5.3) to the FBU, and thereby inform ARs about its multicast context. ARs will use these multicast context options for inter-AR context transfer.

In predictive mode, FBU is issued on the previous link and received by PAR as displayed in Figure 2. PAR will extract the multicast context options and append them to its HI message. From the HACK message, PAR will redistribute the multicast acknowledgement by adding the corresponding mobility options to its FBACK message. From receiving FBACK, the MN will learn about a per group multicast support in the new access network. If some groups or a multicast flavour are not supported, it MAY decide on taking actions to compensate the missing service. Note that the proactive multicast context transfer may proceed successfully, even if the MN misses the FBACK message on the previous link.

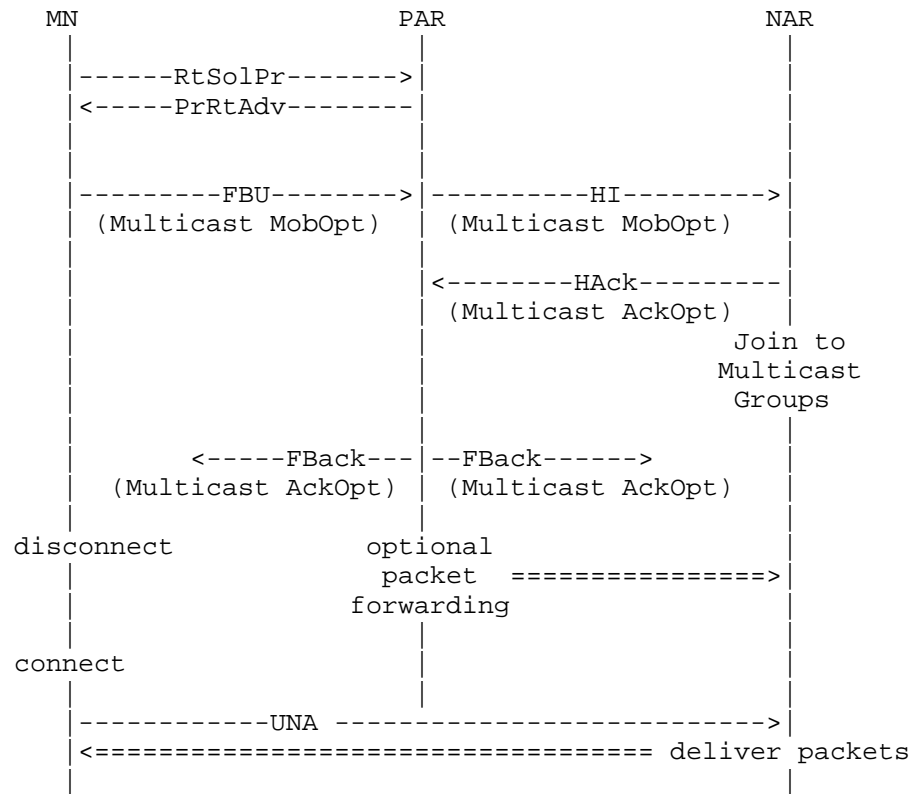


Figure 2: Predictive Multicast Handover for FMIPv6

The call flow for reactive mode is visualized in Figure 3. After attaching to the new access link and performing an unsolicited neighbor advertisement (UNA), the MN issues an FBU which NAR forwards to PAR without processing. At this time, the MN is able to re-join all desired multicast groups without relying on AR assistance. Nevertheless, multicast context options are exchanged in the HI/HACK dialog to facilitate intermediate forwarding of requested streams. Note that group traffic possibly already arrives from a MN's subscription at the time NAR receives the HI message. Such streams may be transparently excluded from forwarding by setting an appropriate multicast acknowledge option. In any case, NAR MUST ensure that not more than one stream of the same group is forwarded to the MN.



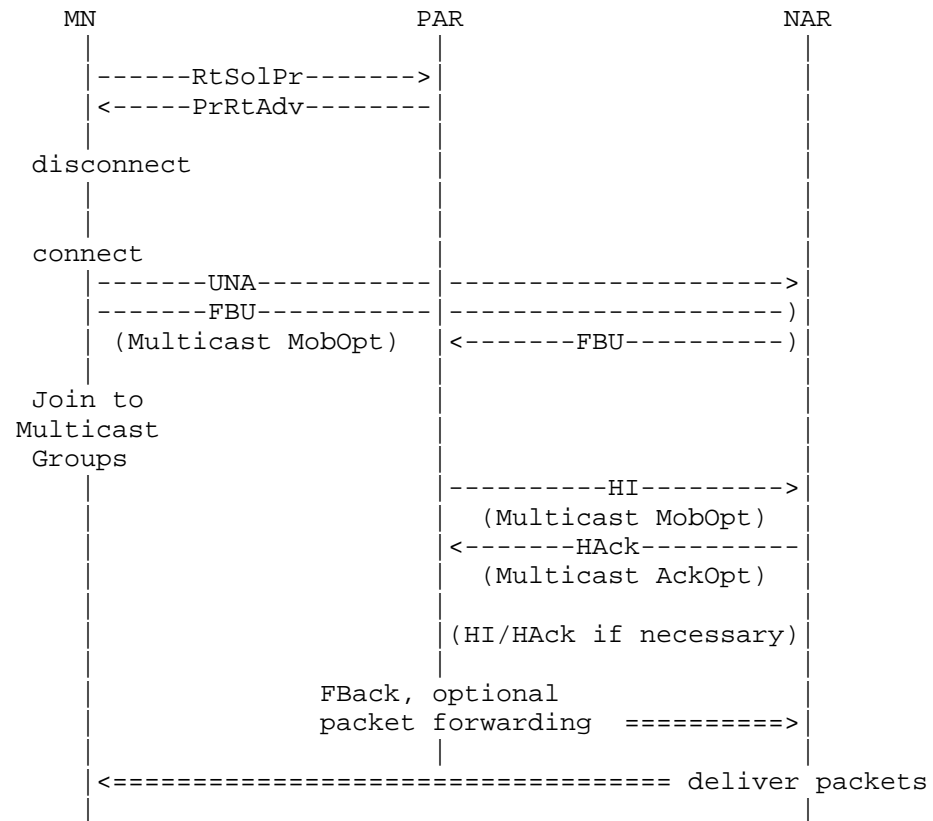


Figure 3: Reactive Multicast Handover for FMIPv6

### 3.3. Protocol Operations Specific to PFMIPv6

In a proxy mobile IPv6 environment, the MN remains agnostic of network layer changes, and fast handover procedures are operated by the access routers or MAGs. The handover initiation, or the re-association respectively are managed by the access networks. Consequently, access routers need to be aware of multicast membership state at the mobile node. There are two ways to obtain record of MN's multicast membership. First, MAGs MAY perform an explicit tracking (cf., [RFC4605], [RFC6224]) or extract membership status from forwarding states at node-specific point-to-point links. Second, routers can perform general queries at handovers. Both methods are equally applicable. However, a router that does not operate explicit tracking MUST query its downstream links subsequent to handovers. In either case, the PAR will become knowledgeable about multicast group subscriptions of the MN.

In predictive mode, the PMAG (PAR) will learn about the upcoming movement of the mobile node. Without explicit tracking, it will immediately submit a general MLD query and learn about the multicast groups under subscription. As displayed in Figure 4, it will initiate binding and context transfer with the NMAG (NAR) by issuing a HI message that is augmented by multicast contexts in the mobility options defined in Section 5.3. NAR will extract multicast context information and act as described in Section 3.1.

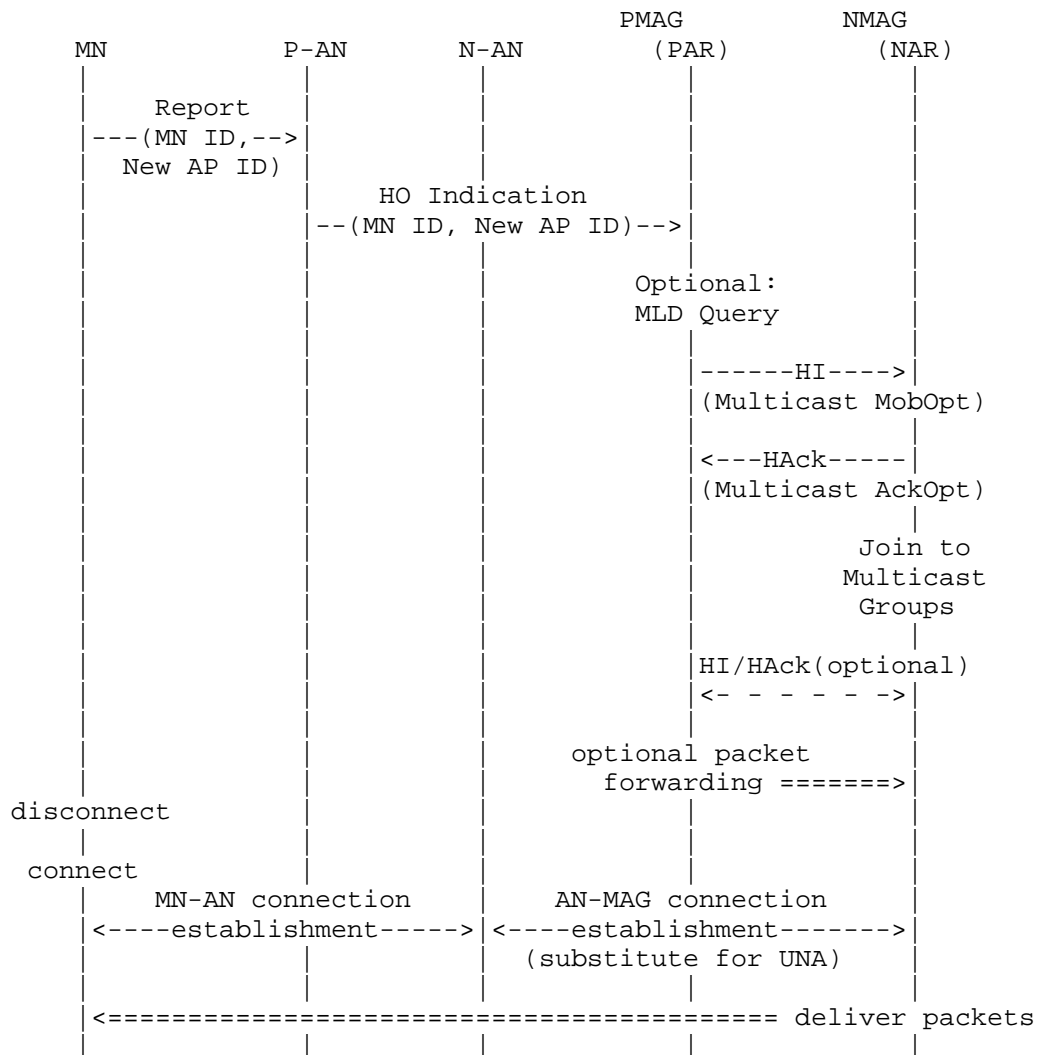


Figure 4: Predictive Multicast Handover for PFMIPv6

In reactive mode, the NMAG (NAR) will learn about MN's attachment to the N-AN and establish connectivity by means of PMIPv6 protocol operations. However, it will have no knowledge about multicast state at the MN. Triggered by a MN attachment, the NMAG will send a general MLD query and thereafter join the requested groups. In the case of a reactive handover, the binding is initiated by NMAG, and the HI/HACK message semantic is inverted (see [RFC5949]). For multicast context transfer, the NMAG attaches to its HI message those group identifiers it requests to be forwarded from PMAG. Using the identical syntax in its multicast mobility option headers as defined in Section 5.4, PMAG acknowledges those requested groups in its HACK answer that it is willing to forward. The corresponding call flow is displayed in Figure 5.

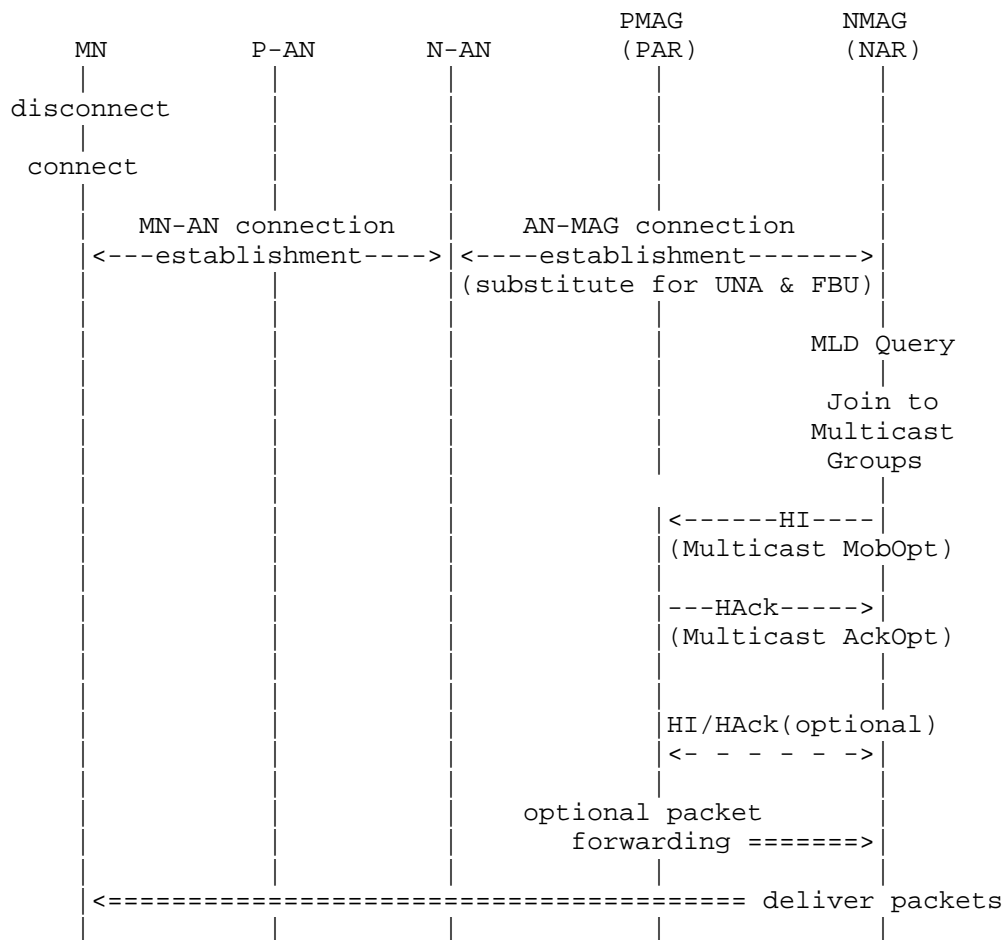


Figure 5: Reactive Multicast Handover for PFMIPv6

#### 4. Protocol Details

##### 4.1. Protocol Operations Specific to FMIPv6

###### 4.1.1. Operations of the Mobile Node

A Mobile Node willing to manage multicast traffic within fast handover operations will inform about its MLD listener state records within handover signaling.

When sensing a handover in predictive mode, an MN will build a

Multicast Mobility Option as described in Section 5.3 that contains the MLD (IGMP) multicast listener state and append it to the Fast Binding Update (FBU) prior to signaling with PAR. It will receive the Multicast Acknowledgement Option(s) as part of Fast Binding Acknowledge (FBack) (see Section 5.4) and learn about unsupported or prohibited groups at the NAR. The MN MAY take appropriate actions like home tunneling to bridge missing multicast services in the new access network. No multicast-specific operation is required by the MN when re-attaching in the new network besides standard FMIPv6 signaling.

In reactive mode, the MN appends an identical Multicast Mobility Option to FBU sent after its reconnect. In response, it will learn about the Multicast Acknowledgement Option(s) from FBACK and expect corresponding multicast data. Concurrently it joins all desired multicast groups (channels) directly on its newly established access link.

#### 4.1.1.2. Operations of the Previous Access Router

A PAR will advertise its multicast support by setting the M-bit in PrRtAdv.

In predictive mode, a PAR will receive the multicast listener state of a MN prior to handover from the Multicast Mobility Option appended to the FBU. It will forward these records to NAR within HI messages and will expect Multicast Acknowledgement Option(s) in HACK, which itself is returned to the MN as an appendix to FBACK. In performing multicast context exchange, the AR is instructed to include the PAR-to-NAR tunnel obtained from unicast handover management in its multicast downstream interfaces and await MLD listener reports from NAR. In response to receiving multicast subscriptions, PAR will normally forward group data acting as a normal multicast router or proxy. However, NAR MAY refuse to forward some or all of the multicast streams.

In reactive mode, PAR will receive the FBU augmented by the Multicast Mobility Option from the new network, but will continue with an identical multicast record exchange in the HI/HACK dialog. As in the predictive case, it will configure the PAR-to-NAR tunnel for multicast downstream and forward data according to MLD reports obtained from NAR, if capable of forwarding.

In both modes, PAR will interpret the first of the two events, the departure of the MN or the reception of the Multicast Acknowledgement Option(s) as a multicast LEAVE message of the MN and react according to the signaling scheme deployed in the access network (i.e., MLD querying, explicit tracking).

#### 4.1.3. Operations of the New Access Router

NAR will advertise its multicast support by setting the M-bit in PrRtAdv.

In predictive mode, a NAR will receive the multicast listener state of an expected MN from the Multicast Mobility Option appended to the HI message. It will extract the MLD/IGMP records from the message and intersect the request subscription with its multicast service offer. Further on it will adjoin the supported groups (channels) to the MLD listener state using loopback as downstream interface. This will lead to suitable regular subscriptions on its native multicast upstream interface without additional forwarding. Concurrently, NAR builds a Multicast Acknowledgement Option(s) (see Section 5.4) listing those groups (channels) unsupported on the new access link and returns them within HACK. As soon as the bidirectional tunnel from PAR to NAR is operational, NAR joins the groups desired for forwarding on the tunnel link.

In reactive mode, NAR will learn about the multicast listener state of a new MN from the Multicast Mobility Option appended to HI at a time, when the MN has already performed local subscriptions of the multicast service. Thus NAR solely determines the intersection of requested and supported groups (channels) and issues the join requests for group forwarding on the PAR-NAR tunnel interface.

In both modes, NAR MUST send a LEAVE message to the tunnel immediately after forwarding of a group (channel) becomes unneeded, e.g., after native multicast traffic arrives or group membership of the MN terminates.

#### 4.2. Protocol Operations Specific to PMIPv6

##### 4.2.1. Operations of the Mobile Node

A Mobile Node willing to participate in multicast traffic will join, maintain and leave groups as if located in the fixed Internet. It will cooperate in handover indication as specified in [RFC5949] and required by its access link-layer technology. No multicast-specific mobility actions nor implementations are required at the MN in a PMIPv6 domain.

##### 4.2.2. Operations of the Previous MAG

A MAG receiving a handover indication for one of its MNs follows the predictive fast handover mode as a PMAG. It MUST issue an MLD General Query immediately on its corresponding link unless it performs an explicit tracking on that link. After gaining knowledge

of the multicast subscriptions of the MN, the PMAG builds a Multicast Mobility Option as described in Section 5.3 that contains the MLD (IGMP) multicast listener state. If not empty, this Mobility Option is appended to the regular fast handover HI messages, or - in the case of unicast HI message being submitted prior to multicast state detection - sent in an additional HI message to the NMAG. PMAG then waits for receiving the Multicast Acknowledgement Option(s) with HACK (see Section 5.4) and the creation of the bidirectional tunnel with NMAG. Thereafter PMAG will add the tunnel to its downstream interfaces in the multicast forwarding database. For those groups (channels) reported in the Multicast Acknowledgement Option(s), i.e., not supported in the new access network, PMAG normally takes appropriate actions (e.g., forwarding, termination) in concordance with the network policy. It SHOULD start forwarding traffic down the tunnel interface for those groups it receives an MLD listener report message from NMAG. However, it MAY deny forwarding service. After the departure of the MN and on the reception of LEAVE messages for groups/channels, PMAG MUST terminate forwarding of the specific groups and update its multicast forwarding database. Correspondingly it issues a group/channel LEAVE to its upstream link, if no more listeners are present on its downstream links.

A MAG receiving a HI message with Multicast Mobility Option for a currently attached node follows the reactive fast handover mode as a PMAG. It will return Multicast Acknowledgement Option(s) (see Section 5.4) within HACK listing those groups/channels unsupported at NMAG. It will add the bidirectional tunnel with NMAG to its downstream interfaces and will start forwarding multicast traffic for those groups it receives an MLD listener report message from NMAG. At the reception of LEAVE messages for groups (channels), PMAG MUST terminate forwarding of the specific groups and update its multicast forwarding database. According to its multicast forwarding states, it MAY need to issue a group/channel LEAVE to its upstream link, if no more listeners are present on its downstream links.

In both modes, PMAG will interpret the departure of the MN as a multicast LEAVE message of the MN and react according to the signaling scheme deployed in the access network (i.e., MLD querying, explicit tracking).

#### 4.2.3. Operations of the New MAG

A MAG receiving a HI message with Multicast Mobility Option for a currently unattached node follows the predictive fast handover mode as NMAG. It will decide on those multicast groups/channels it wants forwarded from the PMAG and builds a Multicast Acknowledgement Option (see Section 5.4) that enumerates only unwanted groups/channels. This Mobility Option is appended to the regular fast handover HACK

messages, or - in the case of unicast HACK message being submitted prior to multicast state acknowledgement - sent in an additional HACK message to the PMAG. Immediately thereafter, NMAG SHOULD update its MLD listener state by the new groups/channels obtained from the Multicast Mobility Option. Until the MN re-attaches, NMAG uses its loopback interface for downstream and does not forward traffic to the potential link of the MN. NMAG SHOULD issue JOIN messages for those newly adopted groups to its regular multicast upstream interface. As soon as the bidirectional tunnel with PMAG is established, NMAG additionally joins those groups/channels on the tunnel interface that it wants to receive by forwarding from PMAG. NMAG MUST send a LEAVE message to the tunnel immediately after forwarding of a group/channel becomes unneeded, e.g., after native multicast traffic arrives or group membership of the MN terminates.

A MAG experiencing a connection request for a MN without prior reception of a corresponding Multicast Mobility Option is operating in the reactive fast handover mode as NMAG. Following the re-attachment, it immediately issues an MLD General Query to learn about multicast subscriptions of the newly arrived MN. Using standard multicast operations, NMAG joins the missing groups (channels) on its regular multicast upstream interface. Concurrently, it selects groups (channels) for forwarding from PMAG and builds a Multicast Mobility Option as described in Section 5.3 that contains the MLD (IGMP) multicast listener state. If not empty, this Mobility Option is appended to the regular fast handover HI messages with the F flag set, or - in the case of unicast HI message being submitted prior to multicast state detection - sent in an additional HI message to the PMAG. Upon reception of the Multicast Acknowledgement Option and upcoming of the bidirectional tunnel, NMAG additionally joins those groups/channels on the tunnel interface that it wants to receive by forwarding from PMAG. When multicast streams arrive, the NMAG forwards data to the appropriate downlink(s). NMAG MUST send a LEAVE message to the tunnel immediately after forwarding of a group/channel becomes unneeded, e.g., after native multicast traffic arrives or group membership of the MN terminates.

#### 4.2.4. IPv4 Support Considerations

An MN in a PMIPv6 domain may use an IPv4 address transparently for communication as specified in [RFC5844]. For this purpose, LMAs can register IPv4-Proxy-CoAs in its Binding Caches and MAGs can provide IPv4 support in access networks. Correspondingly, multicast membership management will be performed by the MN using IGMP. For multiprotocol multicast support on the network side, IGMPv3 router functions are required at both MAGs (see Section 5.6 for compatibility considerations with previous IGMP versions). Context transfer between MAGs can transparently proceed in HI/HACK message



exchanges by encapsulating IGMP multicast state records within Multicast Mobility Options (see Section 5.3 and Section 5.4 for details on message formats).

It is worth mentioning the scenarios of a dual-stack IPv4/IPv6 access network, and the use of GRE tunneling as specified in[RFC5845]. Corresponding implications and operations are discussed in the PMIP Multicast Base Deployment document, cf., [RFC6224].

## 5. Message Formats

### 5.1. Multicast Indicator for Proxy Router Advertisement (PrRtAdv)

An FMIPv6 AR will indicate its multicast support by activating the M-bit in its Proxy Router Advertisements (PrRtAdv). The message extension has the following format.

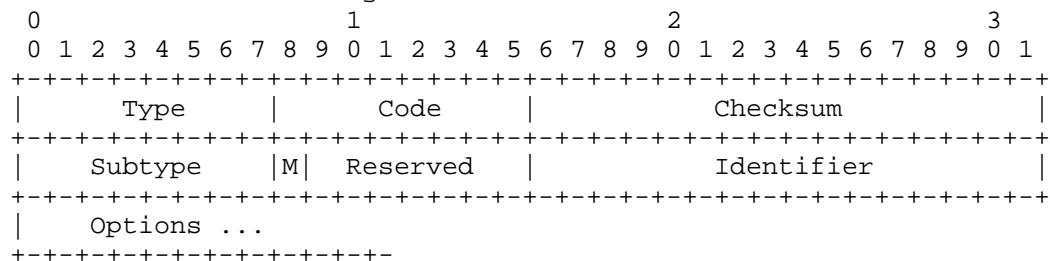


Figure 6: Multicast Indicator Bit for Proxy Router Advertisement (PrRtAdv) Message

### 5.2. Extensions to Existing Mobility Header Messages

The fast handover protocols use a new IPv6 header type called Mobility Header as defined in [RFC3775]. Mobility headers can carry variable Mobility Options.

Multicast listener context of an MN is transferred in fast handover operations from PAR/PMAG to NAR/NMAG within a new Multicast Mobility Option, and acknowledged by a corresponding Acknowledgement Option. Depending on the specific handover scenario and protocol in use, the corresponding option is included within the mobility option list of HI/HACK only (PFMIPv6), or of FBU/FBACK/HI/HACK (FMIPv6).

### 5.3. New Multicast Mobility Option

The Multicast Mobility Option contains the current listener state record of the MN obtained from the MLD Report message, and has the format displayed in Figure 7.

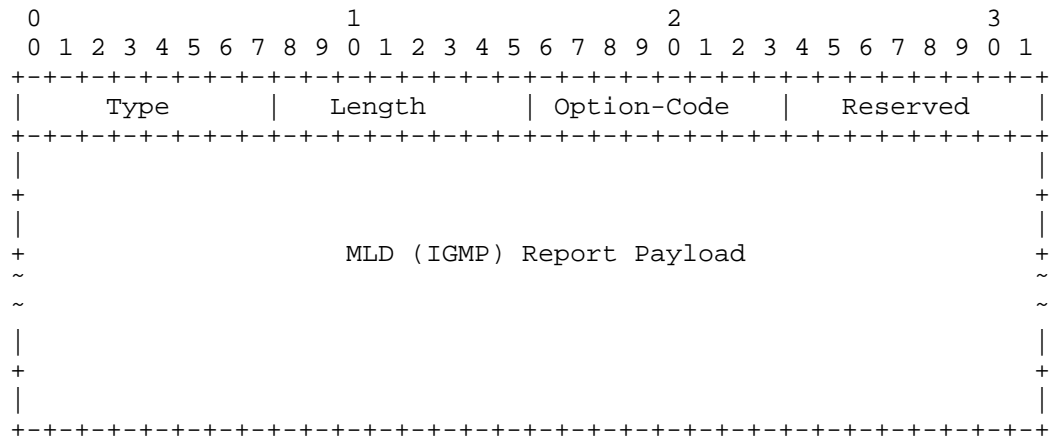


Figure 7: Mobility Header Multicast Option

Type: TBD

Length: 8-bit unsigned integer. The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code:

- 1: IGMPv3 Payload Type
- 2: MLDv2 Payload Type
- 3: IGMPv3 Payload Type from IGMPv2 Compatibility Mode
- 4: MLDv2 Payload Type from MLDv1 Compatibility Mode

Reserved: MUST be set to zero by the sender and MUST be ignored by the receiver.

MLD (IGMP) Report Payload: this field is composed of the MLD (IGMP) Report message after stripping its ICMP header. Corresponding message formats are defined for MLDv2 in [RFC3810], and for IGMPv3 in [RFC3376].

Figure 8 shows the Report Payload for MLDv2, while the payload format for IGMPv3 is defined corresponding to the IGMPv3 payload format (see Section 5.2. of [RFC3810], or Section 4.2 of [RFC3376]) for the definition of Multicast Address Records).

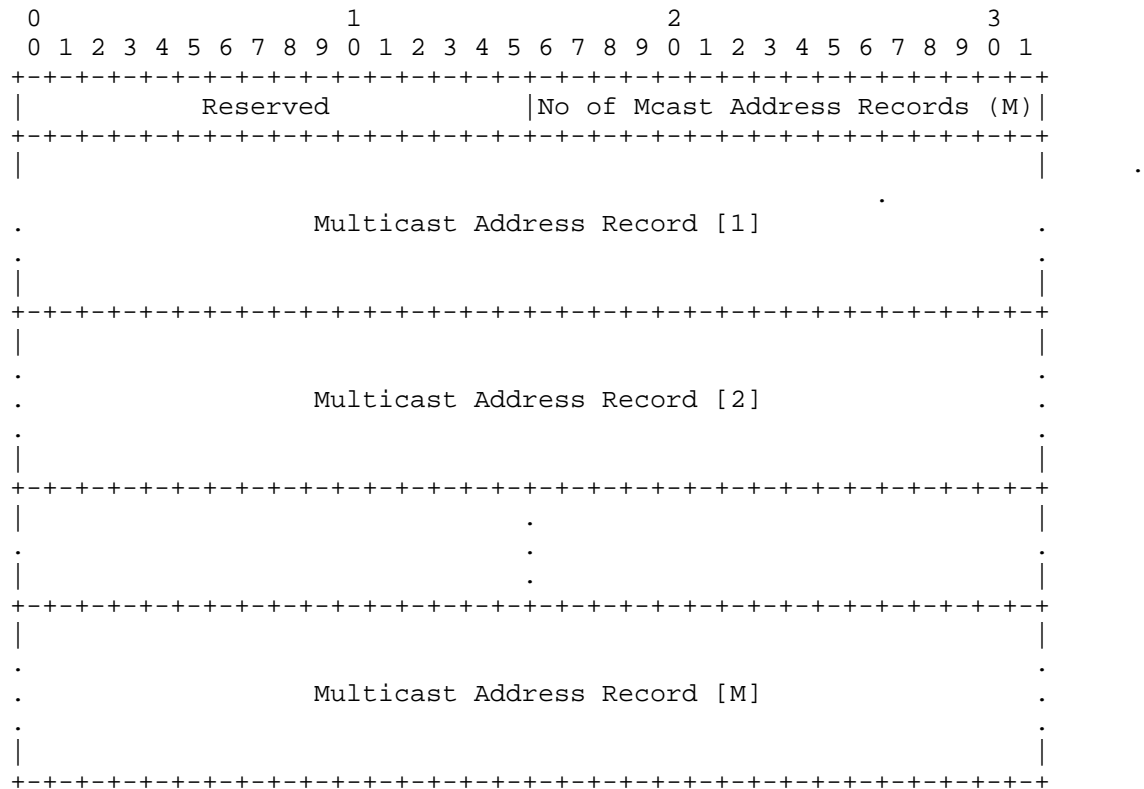


Figure 8: MLDv2 Report Payload

#### 5.4. New Multicast Acknowledgement Option

The Multicast Acknowledgement Option reports the status of the context transfer and contains the list of state records that could not be successfully transferred to the next access network. It has the format displayed in Figure 9.

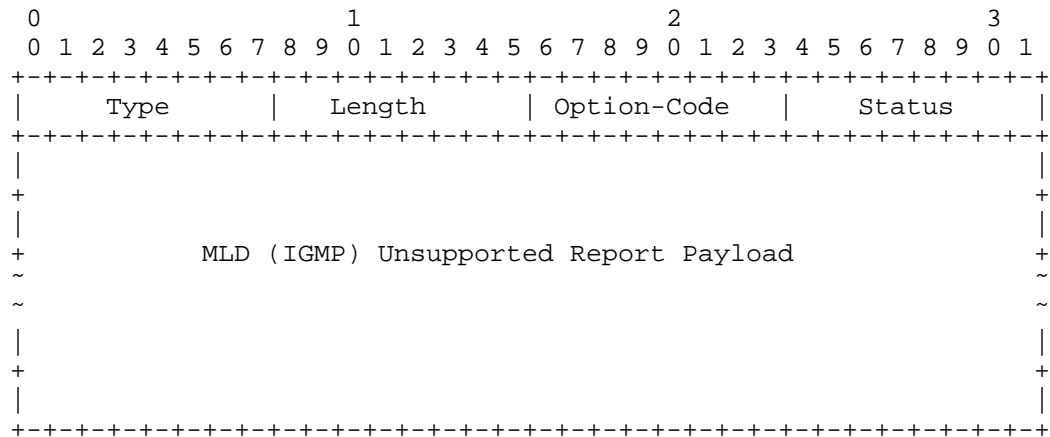


Figure 9: Mobility Header Multicast Acknowledgement Option

Type: TBD

Length: 8-bit unsigned integer. The size of this option in 8 octets. The length is 1 when the MLD (IGMP) Unsupported Report Payload field contains no Mcast Address Record.

Option-Code: 0

Status:

- 1: Report Payload type unsupported
- 2: Requested group service unsupported
- 3: Requested group service administratively prohibited

Reserved: MUST be set to zero by the sender and MUST be ignored by the receiver.

MLD (IGMP) Unsupported Report Payload: this field is syntactically identical to the MLD (IGMP) Report Payload field described in Section 5.3, but is only composed of those multicast address records that are not supported or prohibited in the new access network. This field MUST always contain the first header line (reserved field and No of Mcast Address Records), but MUST NOT contain any Mcast Address Records, if the status code equals 1.

Note that group subscriptions to specific sources may be rejected at the destination network, and thus the composition of multicast address records may differ from initial requests within an MLD (IGMP)

Report Payload option.

#### 5.5. Length Considerations: Number of Records and Addresses

Mobility Header Messages exchanged in HI/HACK and FBU/FBACK dialogs impose length restrictions on multicast context records. The maximal payload length available in FBU/FBACK messages is the PATH-MTU - 40 octets (IPv6 Header) - 6 octets (Mobility Header) - 6 octets (FBU/FBACK Header). For example, on an Ethernet link with an MTU of 1500 octets, not more than 72 Multicast Address Records of minimal length (without source states) may be exchanged in one message pair. In typical handover scenarios, this number reduces further according to unicast context and Binding Authorization data. A larger number of MLD Report Payloads MAY be sent within multiple HI/HACK or FBU/FBACK message pairs. In PFMIPv6, context information can be fragmented over several HI/HACK messages. However, a single MLDv2 Report Payload MUST NOT be fragmented. Hence, for a single Multicast Address Record on an Ethernet link, the number of source addresses is limited to 89.

#### 5.6. MLD (IGMP) Compatibility Aspects

Access routers (MAGs) MUST support MLDv2 (IGMPv3). To enable multicast service for MLDv1 (IGMPv2) listeners, the routers MUST follow the interoperability rules defined in [RFC3810] ([RFC3376]) and appropriately set the Multicast Address Compatibility Mode. When the Multicast Address Compatibility Mode is MLDv1 (IGMPv2), a router internally translates the following MLDv1 (IGMPv2) messages for that multicast address to their MLDv2 (IGMPv2) equivalents and uses these messages in the context transfer. The current state of Compatibility Mode is translated into the code of the Multicast Mobility Option as defined in Section 5.3. A NAR (nMAG) receiving a Multicast Mobility Option during handover will switch to the minimum obtained from its previous and newly learned value of MLD (IGMP) Compatibility Mode for continued operation.

### 6. Security Considerations

Security vulnerabilities that exceed issues discussed in the base protocols of this document ([RFC5568], [RFC5949], [RFC3810], [RFC3376]) are identified as follows.

Multicast context transfer at predictive handovers implements group states at remote access routers and may lead to group subscriptions without further validation of the multicast service requests. Thereby a NAR (nMAG) is requested to cooperate in potentially complex multicast re-routing and may receive large volumes of traffic.

Malicious or inadvertent multicast context transfers may result in a significant burden of route establishment and traffic management onto the backbone infrastructure and the access router itself. Rapid re-routing or traffic overload can be mitigated by a rate control at the AR that restricts the frequency of traffic redirects and the total number of subscriptions. In addition, the wireless access network remains protected from multicast data injection until the requesting MN attaches to the new location.

## 7. IANA Considerations

This document defines new flags and status codes in the HI and HAcK messages as well as two new mobility options. The Type values for these mobility options are assigned from the same numbering space as allocated for the other mobility options defined in [RFC3775]. Those for the flags and status codes are assigned from the corresponding numbering space defined in [RFC5568], or [RFC5949] and requested to be created as new tables in the IANA registry (marked with asterisks). New values for these registries can be allocated by Standards Action or IESG approval [RFC5226].

## 8. Acknowledgments

Protocol extensions to support multicast in Fast Mobile IPv6 have been loosely discussed since several years. Repeated attempts have been taken to define corresponding protocol extensions. The first draft [fmcast-mip6] was presented by Suh, Kwon, Suh, and Park already in 2004.

This work was stimulated by many fruitful discussions in the MobOpts research group. We would like to thank all active members for constructive thoughts and contributions on the subject of multicast mobility. Comments, discussions and reviewing remarks have been contributed by (in alphabetical order) Carlos J. Bernardos, Luis M. Contreras, Dirk von Hugo, Marco Liebsch, Behcet Sarikaya, Stig Venaas and Juan Carlos Zuniga.

## 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.
- [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support

in IPv6", RFC 3775, June 2004.

- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5568] Koodli, R., "Mobile IPv6 Fast Handovers", RFC 5568, July 2009.
- [RFC5949] Yokota, H., Chowdhury, K., Koodli, R., Patil, B., and F. Xia, "Fast Handovers for Proxy Mobile IPv6", RFC 5949, September 2010.
- [RFC1112] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, August 1989.
- [RFC4605] Fenner, B., He, H., Haberman, B., and H. Sandick, "Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")", RFC 4605, August 2006.
- [RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.
- [RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.
- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

## 9.2. Informative References

- [RFC5757] Schmidt, T., Waehlich, M., and G. Fairhurst, "Multicast Mobility in Mobile IP Version 6 (MIPv6): Problem Statement and Brief Survey", RFC 5757, February 2010.
- [fmcast-mip6]  
Suh, K., Kwon, D., Suh, Y., and Y. Park, "Fast Multicast Protocol for Mobile IPv6 in the fast handovers environments", draft-suh-mipshop-fmcast-mip6-00 (work in progress), July 2004.
- [FMIPv6-Analysis]  
Schmidt, TC. and M. Waehlich, "Predictive versus Reactive - Analysis of Handover Performance and Its Implications on IPv6 and Multicast Mobility", Telecommunication Systems Vol 33, No. 1-3, pp. 131-154, November 2005.

- [RFC6224] Schmidt, T., Waehlis, M., and S. Krishnan, "Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains", RFC 6224, April 2011.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.
- [RFC5845] Muhanna, A., Khalil, M., Gundavelli, S., and K. Leung, "Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6", RFC 5845, June 2010.

#### Appendix A. Change Log

The following changes have been made from  
draft-schmidt-multimob-fmipv6-pfmipv6-multicast-04.

1. Following working group feedback, multicast traffic forwarding is now a two-sided option between PAR (PMAG) and NAR (NMAG): Either access router can decide on its contribution to the data plane.
2. Several editorial improvements.

The following changes have been made from  
draft-schmidt-multimob-fmipv6-pfmipv6-multicast-03.

1. References updated.

The following changes have been made from  
draft-schmidt-multimob-fmipv6-pfmipv6-multicast-02.

1. Detailed operations on PFMIPv6 entities completed.
2. Some editorial improvements & clarifications.
3. References updated.

The following changes have been made from  
draft-schmidt-multimob-fmipv6-pfmipv6-multicast-01.

1. First detailed operations on PFMIPv6 added.
2. IPv4 support considerations for PFMIPv6 added.
3. Section on length considerations for multicast context records corrected.



4. Many editorial improvements & clarifications.

5. References updated.

The following changes have been made from  
draft-schmidt-multimob-fmipv6-pfmipv6-multicast-00.

1. Editorial improvements & clarifications.

2. Section on length considerations for multicast context records added.

3. Section on MLD/IGMP compatibility aspects added.

4. Security section added.

#### Authors' Addresses

Thomas C. Schmidt  
HAW Hamburg  
Dept. Informatik  
Berliner Tor 7  
Hamburg, D-20099  
Germany

Email: schmidt@informatik.haw-hamburg.de

Matthias Waehlich  
link-lab & FU Berlin  
Hoenower Str. 35  
Berlin D-10318  
Germany

Email: mw@link-lab.net

Rajeev Koodli  
Cisco Systems  
30 International Place  
Xuanwu District,  
Tewksbury MA 01876  
USA

Email: rkoodli@cisco.com

Godred Fairhurst  
University of Aberdeen  
School of Engineering  
Aberdeen AB24 3UE  
UK

Email: [gorry@erg.abdn.ac.uk](mailto:gorry@erg.abdn.ac.uk)



MULTIMOB Working Group  
Internet-Draft  
Intended status: Informational  
Expires: December 9, 2010

D. von Hugo  
Deutsche Telekom Laboratories  
H. Asaeda  
Keio University  
B. Sarikaya  
Huawei USA  
P. Seite  
France Telecom - Orange  
June 8, 2010

Evaluation of further issues on Multicast Mobility: Potential future  
work for WG MultiMob  
<draft-von-hugo-multimob-future-work-02.txt>

## Abstract

The WG MultiMob aims at defining a basic mobile multicast solution leveraging on network localized mobility management, i.e. Proxy Mobile IPv6 protocol. The solution would be basically based on multicast group management, i.e. IGMP/MLD, proxying at the access gateway. If such a basic solution is essential from an operational point of view, challenges with efficient resource utilization and user perceived service quality still persist. These issues may prevent large scale deployments of mobile multicast applications.

This document attempts to identify topics for near future extension of work such as modifying multimob base solution, PMIPv6 and MLD/IGMP for optimal multicast support, and adaptation of Handover optimization. Far future items such as extending to and modifying of MIPv4/v6 and DSMIP, sender (source) mobility, consideration of multiple flows and multihoming will be dealt with in a future version.

## Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at

<http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on December 9, 2010.

#### Copyright Notice

Copyright (c) 2010 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 BSD License.

## Table of Contents

1. Introduction . . . . .	4
2. Terminology . . . . .	7
3. IGMP/MLD Proxy Architecture . . . . .	7
4. Problem Description . . . . .	8
4.1. Modification of base PMIPv6 for optimal multicast support . . . . .	8
4.2. Modification of MLD/IGMP for optimal multicast support . .	8
4.3. Consideration of Handover Optimization . . . . .	9
4.4. Specific PMIP deployment issues . . . . .	9
5. Requirements on Solutions . . . . .	10
6. Security Considerations . . . . .	11
7. IANA Considerations . . . . .	11
8. Acknowledgements . . . . .	11
9. References . . . . .	11
9.1. Normative References . . . . .	11
9.2. Informative References . . . . .	12
Authors' Addresses . . . . .	14

## 1. Introduction

Chartered work of WG MultiMob focuses on documentation of proper configuration and usage of existing (specified standard) protocols within both mobility and multicast related areas to enable and support mobility for multicast services and vice versa. The current WG document [I-D.ietf-multimob-pmipv6-base-solution] does not address specific optimizations and efficiency improvements of multicast routing for network-based mobility and thus the operation may be not resource efficient nor grant the service quality expected by the end user.

The described solution resolves the problem to ensure multicast reception in PMIPv6-enabled [RFC5213] networks without appropriate multicast support. However it neither automatically minimizes multicast forwarding delay to provide seamless and fast handovers for real-time services nor minimizes packet loss and reordering that result from multicast handover management as stated in [RFC5757]. Also Route Optimization is out of scope of the basic solution - an issue for reducing amount of transport resource usage and transmission delay. Thus possible enhancements and issues for solutions beyond a basic solution need to be described to enable current PMIPv6 protocols to fully support efficient mobile multicast services. Such extensions may include protocol modifications for both mobility and multicast related protocols to achieve optimizations for resource efficient and performance increasing multimob approaches. The document includes the case of mobile multicast senders using Any Source Multicast (ASM) and Source Specific Multicast (SSM) [RFC4607].

This document focuses on discussion work on multicast protocols such as IGMP/MLD operational tuning (e.g. as proposed in [I-D.asaeda-igmp-mld-optimization]) and enhancements of IGMP/MLD protocol behaviors and messages for optimal multicast support (proposed in [I-D.asaeda-igmp-mld-mobility-extension]).

An alternative approach proposes the addition of acknowledgement messages on group management ([I-D.liu-multimob-reliable-igmp-mld]) and changes the unreliable protocol concept.

Furthermore a modification of PMIPv6 by introducing a dedicated multicast tunnel and support of local routing is discussed in [I-D.asaeda-multimob-pmipv6-extension]. Other performance improvements have been outlined in [I-D.schmidt-multimob-fmipv6-pfmipv6-multicast] where extensions to Mobile IPv6 Fast Handovers (FMIPv6) [RFC5568], and the corresponding extension for Proxy MIPv6 operation [I-D.ietf-mipshop-pfmipv6].

Another type of multimob work aims directly at enhancements of the current multimob base solution [I-D.ietf-multimob-pmipv6-base-solution] towards introduction of multicast traffic replication mechanisms and a reduction of the protocol complexity in terms of time consuming tunnel set-up by definition of pre- or post-configured tunnels (as provided by e.g. [I-D.zuniga-multimob-smsspmpip]). Further work within this topic deals with direct routing (e.g. [I-D.sijeon-multimob-mms-pmip6]) and with dynamic or automatic tunnel configuration (see e.g. [I-D.ietf-mboned-auto-multicast]).

A large field of additional investigations which are partly described in detail in [RFC5757] will be mentioned for completeness and may be subject of a later WG re-chartering.

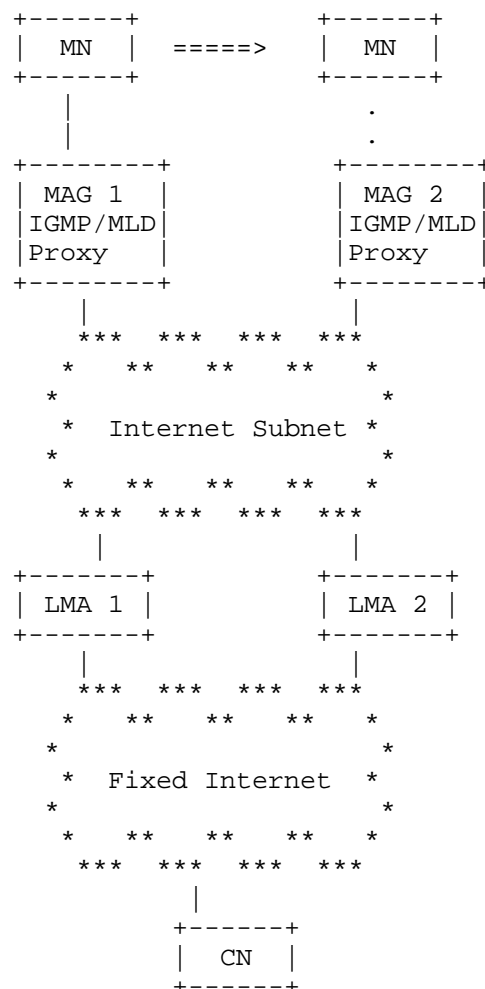


Figure 1: MultiMob Scenario for chartered PMIP6 issue



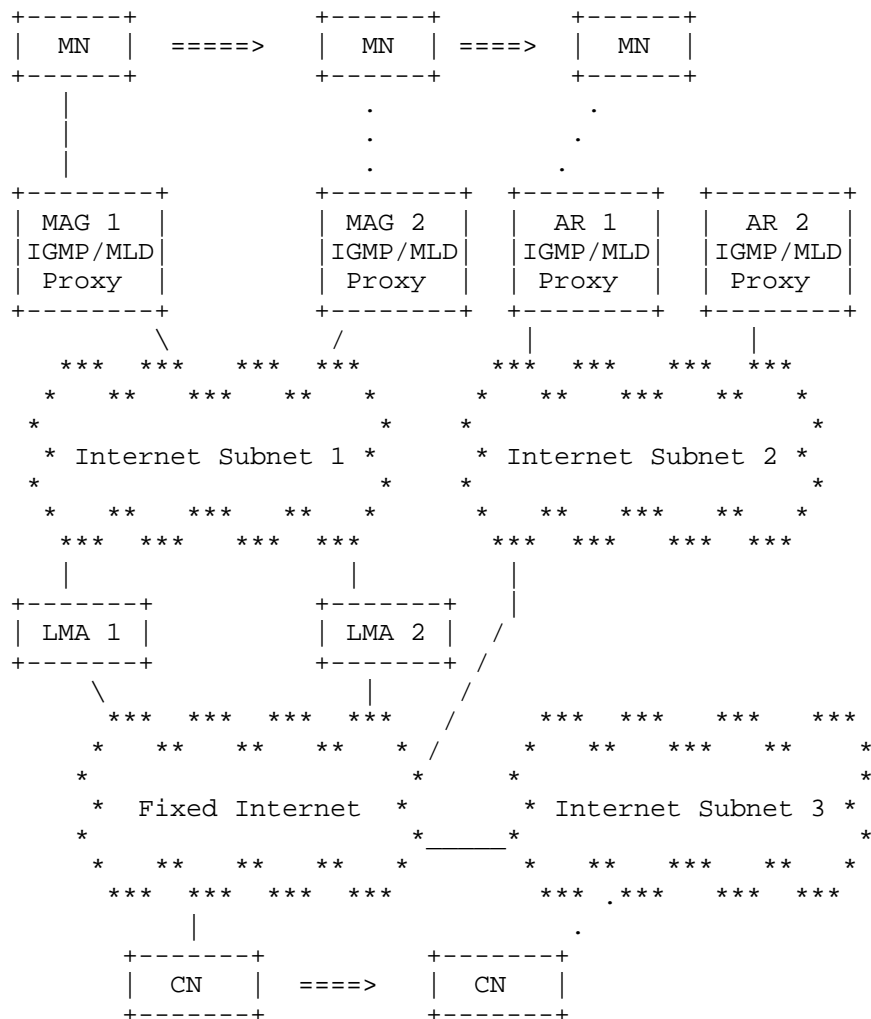


Figure 2: MultiMob scenario for extended MultiMob issues

Figure 1 illustrates the key components of the foreseen basic Multimob solution. The extended multicast mobility scenario, leading to above issues, is sketched in Figure 2.

In summary additional to a 'Single hop, link, flow' Proxy MIP mobility for listening MNs (scenario shown in Figure 1), future work towards a complete performance-optimized scenario of a 'Multi-hop, -homed, -flow' client mobility (i.e. including MIPv6 [RFC3775] and DSMIPv6 [RFC5555]) would cover a plurality of issues. For the near

future we see the following issues as most important:

- o Extension of multimob base solution
- o Modification of base PMIPv6 and MLD/IGMP for optimal multicast support.
- o Consideration of Handover optimization.

All further issues which would include extensions to and modifications of MIPv4/v6 and DSMIP using IGMP/MLD Proxy and the Foreign Agent/Access Router, consideration of sender (source) mobility, support of multiple flows on multihomed mobile nodes, multi-hop transmission, Routing optimization, and so forth will be topics for a potential next stage of future work extension.

## 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119].

This document uses the terminology defined in [RFC3775], [RFC3376], [RFC3810], [RFC5213], [RFC5757].

## 3. IGMP/MLD Proxy Architecture

Multimob basic solution is based on IGMPv3/MLDv2 Proxy support at the mobile access gateway (MAG) of Proxy Mobile IPv6 as shown in Figure 1. IGMPv3/MLDv2 proxy keeps multicast state on the subscriptions of the mobile nodes and only an aggregate state is kept at the local mobility anchor (LMA). When LMA receives multicast data it can forward it to the MAG without duplication because MAG takes of the packet duplication. This leads to solving the avalanche problem.

By keeping multicast state locally, IGMPv3/MLDv2 Proxy introduces mobility related problems such as possible packet loss when a mobile node does a handover to another MAG and its multicast state is not modified fast enough at the LMA.

IGMPv3/MLDv2 introduces tunnel convergence problem which occurs when a given MAG serves MNs that belong to different LMAs and MNs subscribe to the same multicast group. In that case MNs receive duplicate multicast data forwarded from more than one LMA.

It can be foreseen that mobile access gateways will serve both mobile and fixed terminals concurrently. The tuning of multicast-related

protocol parameters based on the terminal characteristics is needed. Parameters only applicable to mobile users need to be distinguished from the parameters applicable to fixed users. It should be also possible to distinguish between slow and fast movement and handover frequency to form corresponding tunnels for mobile users.

Based on the above observations we will state the problems next and then list the requirements on possible solutions.

#### 4. Problem Description

The general issues of multicast mobility are extensively discussed and described in [RFC5757]. To reduce the complexity of the plethora of requirements listed in [RFC5757] and also in [I-D.deng-multimob-pmip6-requirement] this document summarises some lightweight solutions for multicast mobility which allow for easy deployment within realistic scenarios and architectures. Moreover we focus on approaches building directly on basic MultiMob solution [I-D.ietf-multimob-pmipv6-base-solution] which is based on IGMP/MLD Proxy functionality at the mobile access gateway, and for which already solution proposals have been described.

##### 4.1. Modification of base PMIPv6 for optimal multicast support

Currently discussed aspects of multicast optimization for PMIPv6 include introduction of multicast tunnels and support of local routing such as described in [I-D.asaeda-multimob-pmip6-extension]. For a PMIPv6 domain the establishment of a dedicated multicast tunnel is proposed which may either be dynamically set up and released or be pre-configured in a static manner. Both mobility entities MAG and LMA may operate as MLD proxy or multicast router. Since further functional enhancements of PMIPv6 are currently under way in NETEXT WG, both the impact of new features on Mobile Multicast as well as such a Multicast-initiated proposal for PMIPv6 modification have to be considered in a continuous exchange process between MultiMob and NETEXT WGs.

##### 4.2. Modification of MLD/IGMP for optimal multicast support

Potential approaches for enhancement of group management as specified e.g. by MLDv2 [RFC3810] include operational improvements such as proper tuning in terms of default timer value modification, specific query message introduction, and standard (query) reaction suppression, beside introducing multicast router attendance control in terms of e.g. specification of a Listener Hold message as proposed in [I-D.asaeda-multimob-igmp-ml-d-mobility-extensions].

#### 4.3. Consideration of Handover Optimization

Ideally the customer experience while using multicast services should not be affected by transmission issues whether the terminal is operated in a fixed or a mobile environment. This implies not only that the terminal should be unaware of changes at network layer connectivity (seamless communication) as is typically the case in a PMIPv6 domain, but also that any impact of connectivity changes (handover) should be minimized. In the framework of Multimob this relates to reduction of delay, packet loss, and packet reordering effort for mobile multicast by applying fast handover mechanisms, which have originally been developed for unicast traffic to multicast group management. [I-D.schmidt-multimob-fmipv6-pfmipv6-multicast] works on specification of extension of the Mobile IPv6 Fast Handovers (FMIPv6) [RFC5568] and the Fast Handovers for Proxy Mobile IPv6 (PFMIPv6) [I-D.ietf-mipshop-pfmipv6] protocols to include multicast traffic management in fast handover operations. Issues for further work are details of including multicast group messaging in context transfer, for both predictive and reactive handover mode, as well as details of corresponding message exchange protocols and message design.

#### 4.4. Specific PMIP deployment issues

Currently several proposals are under work which describe extensions of the base protocol WG draft [I-D.ietf-multimob-pmipv6-base-solution]. While MAG operation will remain that of an MLD proxy additional LMA functionalities are described in [I-D.zuniga-multimob-smspmip] which allow for replication of multicast traffic and solution of the tunnel convergence problem. The dedicated multicast LMA may either set up dedicated multicast tunnels dynamically or a-priori via pre-configuration or a delayed release.

Another solution on dynamic and/or automatic tunnel configuration is proposed within multicast WG MBONED [I-D.ietf-mboned-auto-multicast].

A direct or local routing approach is described in [I-D.sijeon-multimob-mms-pmipv6]. This scenario may hold for short term deployment focusing on an architecture where multicast traffic is provided via the home network. However, depending on the network topology, namely the location of the content delivery network, the LMA may not be on the optimal multicast service delivery path. This enables mobile nodes to access locally available multicast services such as local channels.

Figure 3 illustrates the use-case for local routing.

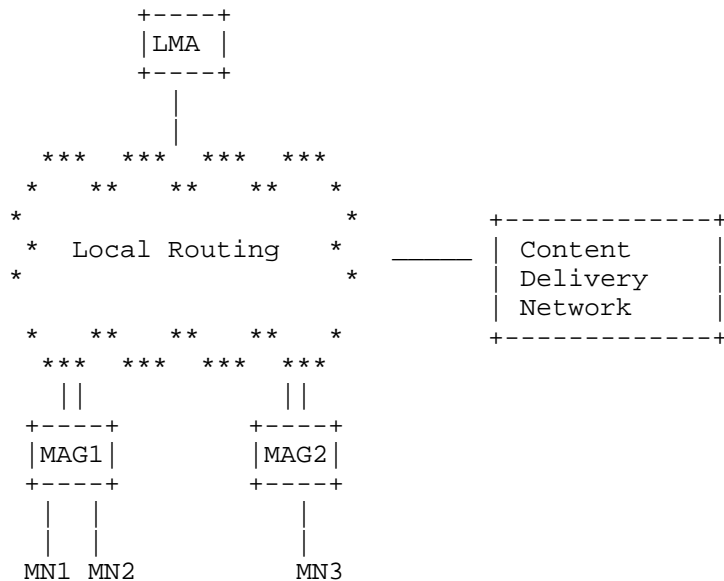


Figure 3: local Multicast routing

In such a case, the MAG should act as a multicast router to construct the optimal multicast delivery path. If the MAG also supports MLD proxy function issue raises up on the dual mode behaviour. In such a case, a pragmatic approach could be to leverage only on multicast routing at the MAG in the PMIP domain.

Whatever is the MAG operation mode, the multicast state is locally kept at the access gateway, so unknown from the mobility anchor. In other words, the multicast service is independent from the mobility service that the mobile node is receiving from the network in the form of PMIPv6 or DSMIPv6. However, handover support is still desirable but cannot be provided by the mobility anchor (i.e. HA or LMA). In such a case mobility support for locally available multicast should be provided by extending multicast protocols of IGMP or MLD.

## 5. Requirements on Solutions

This section tries to identify requirements from the issues discussed in previous section.

- o Seamless handover (low latency and during the handover).
- o Similar packet loss to unicast service.
- o Multiple LMAs architecture.
- o Agnostic mobile host re-subscription. So, MAGs must be able to retrieve multicast contexts of the mobile nodes.
- o Solution address IPv6, IPv4 only and dual stack nodes.
- o Supports sender (source) mobility.
- o Optimal local routing.
- o To be completed...

## 6. Security Considerations

This draft introduces no additional messages. Compared to [RFC3376], [RFC3810], [RFC3775], and [RFC5213] there have no additional threats been introduced.

## 7. IANA Considerations

Whereas this document does not explicitly introduce requests to IANA some of the proposals referenced above (such as [I-D.asaeda-multimob-pmip6-extension] and [I-D.schmidt-multimob-fmipv6-pfmipv6-multicast]) specify flags for mobility messages or options. For details please see those documents.

## 8. Acknowledgements

The authors would thank all active members of MultiMob WG, especially (in no specific order) Gorrry Fairhurst, Jouni Korhonen, Thomas Schmidt, Suresh Krishnan and Matthias Waehlich for providing continuous support and helpful comments.

## 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.
- [RFC3314] Wasserman, M., "Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards", RFC 3314, September 2002.
- [RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.

- [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.
- [RFC4607] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5555] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.

## 9.2. Informative References

- [23246] "3GPP TS 23.246 V8.2.0, Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description (Release 8).", 2008.
- [23401] "3GPP TS 23.401 V8.2.0, General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 8).", 2008.
- [23402] "3GPP TS 23.402 V8.4.1, Architecture enhancements for non-3GPP accesses (Release 8).", 2009.
- [I-D.asaeda-multimob-igmp-mld-mobility-extensions]  
Asaeda, H. and T. Schmidt, "IGMP and MLD Hold and Release Extensions for Mobility",  
draft-asaeda-multimob-igmp-mld-mobility-extensions-03  
(work in progress), July 2009.
- [I-D.asaeda-multimob-igmp-mld-optimization]  
Asaeda, H. and S. Venaas, "Tuning the Behavior of IGMP and MLD for Mobile Hosts and Routers",  
draft-asaeda-multimob-igmp-mld-optimization-02 (work in progress), March 2010.
- [I-D.asaeda-multimob-pmip6-extension]  
Asaeda, H., Seite, P., and J. Xia, "PMIPv6 Extensions for Multicast", draft-asaeda-multimob-pmip6-extension-02 (work in progress), July 2009.
- [I-D.deng-multimob-pmip6-requirement]  
Deng, H., Chen, G., Schmidt, T., Seite, P., and P. Yang, "Multicast Support Requirements for Proxy Mobile IPv6",  
draft-deng-multimob-pmip6-requirement-02 (work in progress), July 2009.

- [I-D.liu-multimob-reliable-igmp-ml]  
Liu, H. and Q. Wu, "Reliable IGMP and MLD Protocols in Wireless Environment",  
draft-liu-multimob-reliable-igmp-ml-00 (work in progress), March 2010.
- [I-D.schmidt-multimob-fmipv6-pfmipv6-multicast]  
Schmidt, T., Waehlich, M., Koodli, R., and G. Fairhurst, "Multicast Listener Extensions for MIPv6 and PMIPv6 Fast Handovers",  
draft-schmidt-multimob-fmipv6-pfmipv6-multicast-01 (work in progress), March 2010.
- [I-D.sijeon-multimob-mms-pmip6]  
Jeon, S. and Y. Kim, "Mobile Multicasting Support in Proxy Mobile IPv6", draft-sijeon-multimob-mms-pmip6-02 (work in progress), March 2010
- [I-D.zuniga-multimob-smspmip]  
Zuniga, J., Lu, G., and A. Rahman, "Support Multicast Services Using Proxy Mobile IPv6",  
draft-zuniga-multimob-smspmip-02 (work in progress), June 2010.
- [I-D.ietf-mboned-auto-multicast]  
Thaler, D., Talwar, M., Aggarwal, A., Vicisano, L., and T. Pusateri, "Automatic IP Multicast Without Explicit Tunnels (AMT)", draft-ietf-mboned-auto-multicast-10 (work in progress), March 2010
- [I-D.ietf-16ng-ipv4-over-802-dot-16-ipcs]  
Madanapalli, S., Park, S., Chakrabarti, S., and G. Montenegro, "Transmission of IPv4 packets over IEEE 802.16's IP Convergence Sublayer",  
draft-ietf-16ng-ipv4-over-802-dot-16-ipcs-07 (work in progress), June 2010.
- [I-D.ietf-manet-smf]  
Macker, J. (editor), "Simplified Multicast Forwarding",  
draft-ietf-manet-smf-10 (work in progress), March 2010.
- [I-D.ietf-mipshop-pfmipv6]  
Yokota, H., Chowdhury, K., Koodli, R., Patil, B., and F. Xia, "Fast Handovers for Proxy Mobile IPv6",  
draft-ietf-mipshop-pfmipv6-14 (work in progress), May 2010



- [I-D.ietf-multimob-pmipv6-base-solution]  
Schmidt, T., Waehlich, M., and S. Krishnan, "Base Deployment for Multicast Listener Support in PMIPv6 Domains",  
draft-ietf-multimob-pmipv6-base-solution-02 (work in progress), May 2010.
- [RFC5757] Schmidt, T., Waehlich, M., and G. Fairhurst, "Multicast Mobility in MIPv6: Problem Statement and Brief Survey", RFC 5757, June 2010.
- [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.
- [RFC5121] Patil, B., Xia, F., Sarikaya, B., Choi, JH., and S. Madanapalli, "Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks", RFC 5121, February 2008.

#### Authors' Addresses

Dirk von Hugo  
Deutsche Telekom Laboratories  
Deutsche-Telekom-Allee 7  
64295 Darmstadt, Germany  
  
Email: [dirk.von-hugo@telekom.de](mailto:dirk.von-hugo@telekom.de)

Hitoshi Asaeda  
Keio University  
Graduate School of Media and Governance  
5322 Endo  
Fujisawa, Kanagawa 252-8520  
Japan  
  
Email: [asaeda@wide.ad.jp](mailto:asaeda@wide.ad.jp)  
URI: <http://www.sfc.wide.ad.jp/~asaeda/>

Behcet Sarikaya  
Huawei USA  
1700 Alma Dr. Suite 500  
Plano, TX 75075  
  
Email: [sarikaya@ieee.org](mailto:sarikaya@ieee.org)

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

Email: [pierrick.seite@orange-ftgroup.com](mailto:pierrick.seite@orange-ftgroup.com)



MULTIMOB Group  
Internet-Draft  
Intended status: Experimental  
Expires: September 6, 2012

D. von Hugo  
Telekom Innovation Laboratories  
H. Asaeda  
Keio University  
P. Seite  
France Telecom - Orange  
March 5, 2012

Context Transfer for Multicast support in Distributed Mobility  
Management (DMM)  
draft-vonhugo-multimob-dmm-context-00

Abstract

This document describes a context transfer based concept to support overarching IP multicast services applicable to various existing approaches for Distributed Mobility Management.

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 September 6, 2012.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

## Table of Contents

1. Introduction . . . . .	3
2. Conventions and Terminology . . . . .	5
3. Handover Process . . . . .	6
3.1. Multicast Context Transfer Data Format . . . . .	7
3.2. Multicast Context Transfer with MLD Proxy . . . . .	7
3.3. Multicast Context Transfer with PIM-SM . . . . .	10
4. IANA Considerations . . . . .	11
5. Security Considerations . . . . .	12
6. Acknowledgements . . . . .	13
7. References . . . . .	14
7.1. Normative References . . . . .	14
7.2. Informative References . . . . .	14
Authors' Addresses . . . . .	16

## 1. Introduction

This document describes an application of various existing approaches for Distributed Mobility Management (DMM) [15] to support overarching IP multicast services with Proxy Mobile IPv6 (PMIPv6) [3] and Client Mobile IPv6 (MIPv6) [2], respectively. Key concept of Distributed Mobility Management (DMM) in a flat network architecture where core entities and functionalities are deployed in a distributed manner assumes a mobile node to use the first access router (AR) it attaches to as principal mobility anchor, i.e. Home Agent (HA) in MIPv6 or Local Mobility Anchor (LMA) in PMIPv6. Current proposals for DMM based Mobility such as MIP-based Distributed Mobility Anchoring (DMA) [16] and [21] as well as PMIP-based solutions for Distributed Mobility Management [17], [20] ... and so forth define new AR capabilities applicable to a flat architecture. Common idea of the various approaches is to distribute functionalities for local attachment of a MN to the network and for dynamically keeping track of a MN and its current sessions, also in case of MN attachment to a different AR, to all Access Routers. These ARs are denoted here by DMM ARs (DARs) which are responsible for hosting (anchoring) newly attached MNs and their started sessions (flows), and for relaying old sessions to the MNs' previous DAR(s), respectively. Some solutions refer to a common data base containing all relevant MN information for retrieval which may be co-located with existing logical entities such as DMM-defined Local Mobility Anchor (LMA) or a new common central Mobility Database (MDB).

The MultiMob Base Protocol [12] specifies a mechanism for supporting multicast reception within a PMIPv6 domain using Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying") [7]. Several extensions have been proposed to optimize Routing or session continuity during Handover of a MN. While some approaches rely on the LMA anchoring of a MN to speed up the subscription process during handover as proposed in [19] others apply on an extension of Context Transfer Protocol (CTXP) [10] specification directly [11] or via the established fast HO approach using FPMIP/FMIP [14] to support forwarding of multicast group subscription and traffic data between MAGs. Within a DMM-like approach where location (i.e. anchoring) and access functionality can be handled by the same entity a data exchange between the current AR and a prior one to ensure low delay and loss could be achieved without enhancing complexity too much by applying the CTPX modification directly. In case of node mobility during an ongoing multicast reception session the node should be able to continuously receive the multicast data through the new AR just after handover completion without any MLD signaling on the new wireless link. This procedure is multicast context transfer that provides multicast session continuity and avoids extra packet loss and session disruption. Multicast context transfer will be the

required function to support seamless handover, while for its effective procedure, interaction with multicast communication protocols should be taken into account. To synchronize multicast with unicast traffic measures to prevent delay extension due to waiting for multicast information should be established as proposed in [19]

The Context Transfer Protocol (CXTF) specification [10] describes the mechanism that allows better support for minimizing service disruption during handover. This document proposes to extend CXTF for forwarding of multicast context transfer in a DMM domain. "Multicast-Context Transfer Data (M-CTD)" message as defined in [11] is applied here for transferring multicast membership states between the previously attached DAR (p-DAR) to a newly attached DAR (n-DAR) within a DMM domain. The context transfer is either started from the n-DAR on its own after attachment of the mobile node or initiated by the p-DAR after being informed by the access network of the planned handover. Existing DMM proposals assume that for data exchange between p-DAR and n-DAR a dedicated tunnel already is in place. Details of the set-up procedure for this tunnel are therefore out of scope of this document.

Depending on the scenario of multicast application the real-time delivery of content may be more important than lossless and error-free transmission. Thus to allow for temporary storage or buffering at a previous access router during handover and subsequent forwarding may be advantageous to some file transmission use cases whereas for real-time video services such as live IPTV the focus is on low delay. Here only transfer of the MN's subscription context shall be considered for simplicity reasons.

To decide on a multicast flow quality requirements dedicated flags may be defined to be stored in and retrieved from the common data base or policy storage. Detailed considerations on these parameters are out of scope of this document.

## 2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].

The following terms used in this document are to be interpreted as defined in existing proxy and client mobility protocols and in future upcoming Distributed Mobility Management (DMM) protocol specifications, see e.g. [15]: Distributed Access Router (DAR), Mobility Data Base (MDB), Mobile Node (MN), Proxy Care-of Address (Proxy-CoA), Mobile Node Identifier (MN-Identifier), Distributed Binding Update (DBU), and Distributed Binding Acknowledgement (DBA).



### 3. Handover Process

DAR is responsible for detecting the mobile node's movements to and from the access link and for initiating a per-flow binding registration either as mobility anchor (primary point of attachment). In case a MN attaches to the DAR which was already previously assigned to another (previous or primary) DAR (p-DAR) the new DAR (n-DAR) tracks the mobile node's movements to and from the access link and performs signaling of the status to that p-DAR and to a common MDB. In DMM Multicast, it SHOULD NOT be required for mobile nodes to initiate re-subscription to multicast channels, and DAR SHOULD keep multicast membership state for mobile nodes even if they attach a different DAR during the ongoing session.

For multicast context transfer, an IGMP/MLD-based explicit membership tracking function [18] MAY be enabled on DAR (whether the DAR behaves as a router or proxy). The explicit tracking function enables a router to keep track of downstream multicast membership state created by downstream hosts attached on the router's link. When a mobile node attaches to a new network, thanks to the explicit tracking function, the p-DAR extracts the mobile node's multicast membership state from complete multicast membership state the p-DAR has maintained and transmits it to the n-DAR.

The assumed architecture for a DMM-based multicast mobility is shown in Figure 1.

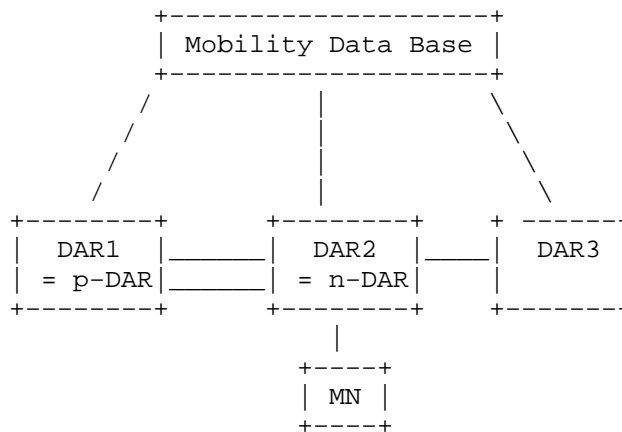


Figure 1: Distributed mobility for flat architecture

### 3.1. Multicast Context Transfer Data Format

Multicast Context Transfer Data (M-CTD) is a message used with CXTP to transfer multicast membership state from p-DAR to n-DAR. The following information is included in M-CTD to recognize mobile node's membership state.

1. Receiver address - indicates the address of the MN sending the Current-State Report.
2. Filter mode - indicates either INCLUDE or EXCLUDE as defined in [5].
3. Source addresses and multicast addresses - indicates the address pairs the MN has joined.

The M-CTD message MUST contain the 'A' bit set as defined for the CTD message format in [10] for to initiate the transmission of a reply message by the new DAR.

The following information included in a reply to M-CTD (similar to the CTDR message defined in [10]) is used to request the old DAR to store still incoming multicast data, to forward them to the new DAR, and finally to leave the multicast group after successful handover from n-DAR to p-DAR.

1. Receiver address - indicates the address of the MN sending the Current-State Report.
2. Flag indicating the p-DAR to start (B) buffering the received multicast data (in case the new connection is not yet fully set up), to forward (F) the buffered data after successful handover, or to leave (L) the multicast groups unless there are still other active subscriptions for the corresponding groups on the p-DAR.
3. Source addresses and multicast addresses - indicates the address pairs the MN has joined.

The M-CTDR message MUST contain the 'S' bit set as defined for the CTD message format in [10] for to indicate the successful reception of context data at the new DAR.

### 3.2. Multicast Context Transfer with MLD Proxy

This section describes the case that DAR operates as an MLD proxy, as defined in [7] and specified in the base MultiMob solution [12].

The MLD listener handover with CXTF and MLD proxy shown in Figure 2 is defined as follows.

1. A MN is assumed to be attached to the p-DAR wishing to receive multicast content and sending the corresponding MLD Report. The serving p-DAR subscribes to the group as MLD proxy and forwards the multicast traffic to the MN via the access link. In case the MN's multicast session is completed while being attached to p-DAR no corresponding entry into the Mobility Data Base needs to be created (regular IPv6 routing). However in case the MN wants to maintain the multicast session (together with ongoing unicast connections) during movement it either registers the address configured at the p-DAR as home address, as described in [21] or the p-DAR has to create a binding entry in the central MDB as proposed e.g. in [20] or [16].
2. When the MN moves to another DAR with the multicast session ongoing the p-DAR detects the detachment and subsequently sends a request to create a Binding Cache Entry for the MN in the MBD, denoted by BCE Create Request (BC-Req).
3. After attaching a new DAR, the mobile node sends a Router Solicitation (RS) as specified in [8]. In case the MN shall remain unaware of any change in connectivity the n-DAR has to identify the p-DAR address during retrieving the MN's BCE from the mobile node's MDB e.g. via newly specified Distributed Binding Update (DBU) and corresponding Acknowledgement (DBA). n-DAR then sends a request for context transfer (CT-Req) to the p-DAR as defined in [10]. Since the MN cannot initiate the related Context Transfer Activate Request (CTAR) message that may be sent by the MDB. In case the mobile node has the capability and the chance to signal to the p-DAR the link status and the potential new DAR address (e.g. as is specified in terms of Event Services by [9]) the p-DAR will send a CTAR message to n-DAR on behalf of the mobile node. Alternatively the p-DAR or the n-DAR may have information on potential DARs in their vicinity to which such a CTAR or CT-Req message may be multicasted.
4. p-DAR provides together with the other feature data the multicast states corresponding to the moving MN-Identifier to n-DAR. p-DAR utilizes a context transfer protocol to deliver MN's Policy Profile to n-DAR, and sends Multicast Context Transfer Data (M-CTD) (defined in Section 3.1) to n-DAR.

5. If there are multicast channels the MN has subscribed but the n-DAR has not yet subscribed, n-DAR subscribes via sending (potentially aggregated) MLD [5][6] Membership Report messages (i.e. Join) to the corresponding MDB.
6. After successful completion of MN attachment the n-DAR replies to M-CTD with a Multicast Context Transfer Response message signalling the handover completion upon which p-DAR may leave the multicast group in case no other MN attached to p-DAR has subscribed to that group.

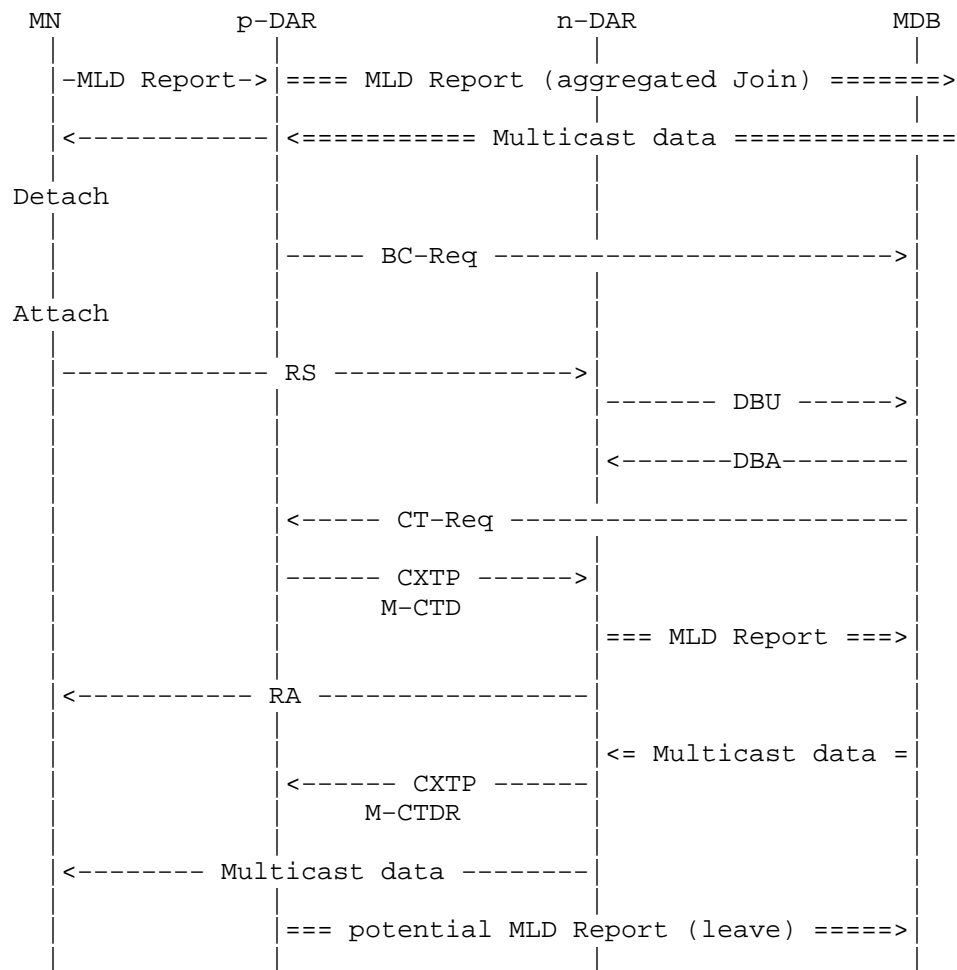


Figure 2: MLD listener handover with CXTF and MLD proxy

After MN attaches to n-DAR, the forwarded multicast data from p-DAR will be delivered to the MN immediately. Afterwards the current multicast data are delivered as received from MDB and the MN's multicast membership state at the p-DAR is cancelled.

### 3.3. Multicast Context Transfer with PIM-SM

This section describes the case that DAR operates as a PIM-SM [4] router, as described in a proposed solution [13].

The MLD listener handover with CXTF and PIM-SM is identical as described in Section 3.2 except that instead of "MLD report (aggregated Join)" the DARs will send "PIM Join" messages and that the "MLD Report (leave)" , to be sent if there are no attached mobile nodes listening the multicast channels at p-DAR, is replaced by "PIM Prune" message.

#### 4. IANA Considerations

TBD.

## 5. Security Considerations

TBD.

## 6. Acknowledgements

Many of the specifications described in this document are discussed and provided by the multimob mailing-list. Detailed comments by Luis Miguel Contreras Murillo are gratefully acknowledged.



## 7. References

### 7.1. Normative References

- [1] Bradner, S., "Key words for use in RFCs to indicate requirement levels", RFC 2119, March 1997.
- [2] Perkins, C, Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
- [3] Gundavelli, S, Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [4] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.
- [5] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.
- [6] Liu, H., Cao, W., and H. Asaeda, "Lightweight IGMPv3 and MLDv2 Protocols", RFC 5790, February 2010.
- [7] Fenner, B., He, H., Haberman, B., and H. Sandick, "Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")", RFC 4605, August 2006.
- [8] Singh, H., Beebee, W., and E. Nordmark, "IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes", RFC 5942, July 2010.
- [9] "IEEE Standard for Local and Metropolitan Area Networks - Part 21: Media Independent Handover Services, IEEE LAN/MAN Std 802.21-2008", January 2009.

### 7.2. Informative References

- [10] Loughney, Ed., J., Nakhjiri, M., Perkins, C., and R. Koodli, "Context Transfer Protocol (CTP)", RFC 4067, July 2005.
- [11] von Hugo, D. and H. Asaeda, "Context Transfer Protocol extensions for Multicast", draft-vonhugo-multimob-CXTP-extension-01.txt (work in progress), January 2012.
- [12] Schmidt, T., Waehlich, M., and S. Krishnan, "Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6)

Domains", RFC 6224, April 2011.

- [13] Asaeda, H., Seite, P., and J. Xia, "PMIPv6 Extensions for PIM-SM", draft-asaeda-multimob-pmip6-extension-07.txt (work in progress), October 2011.
- [14] Schmidt, TC., Waehlich, M., Koodli, R., and G. Fairhurst, "Multicast Listener Extensions for MIPv6 and PMIPv6 Fast Handovers", draft-schmidt-multimob-fmip6-pfmip6-multicast-05.txt (work in progress), November 2011.
- [15] Patil, B., Williams, C., and J. Korhonen, "Approaches to Distributed mobility management using Mobile IPv6 and its extensions", draft-patil-mext-dmm-approaches-02.txt (work in progress), October 2011.
- [16] Seite, P. and P. Bertin, "Distributed Mobility Anchoring", draft-seite-dmm-dma-00.txt (work in progress), February 2012.
- [17] Liu, D., Song, J., and W. Luo, "PMIP Based Distributed Mobility Management Approach", draft-liu-dmm-pmip-based-approach-01.txt (work in progress), December 2011.
- [18] Asaeda, H. and N. Leymann, "IGMP/MLD-Based Explicit Membership Tracking Function for Multicast Routers", draft-ietf-pim-explicit-tracking-00.txt (work in progress), October 2011.
- [19] Contreras, LM., Bernardos, CJ., and I. Soto, "Rapid acquisition of the MN multicast subscription after handover", draft-contreras-multimob-rams-03.txt (work in progress), October 2011.
- [20] Bernardos, CJ., de la Oliva, A., Giust, F., and T. Melia, "A PMIPv6-based solution for Distributed Mobility Management", draft-bernardos-dmm-pmip-00.txt (work in progress), January 2012.
- [21] Bernardos, CJ., de la Oliva, A., and F. Giust, "A IPv6 Distributed Client Mobility Management approach using existing mechanisms", draft-bernardos-mext-dmm-cmip-00.txt (work in progress), March 2011.

## Authors' Addresses

Dirk von Hugo  
Telekom Innovation Laboratories  
Deutsche-Telekom-Allee 7  
Darmstadt 64295  
Germany

Phone:  
Email: Dirk.von-Hugo@telekom.de  
URI:

Hitoshi Asaeda  
Keio University  
Graduate School of Media and Governance  
5322 Endo  
Fujisawa, Kanagawa 252-0882  
Japan

Email: asaeda@wide.ad.jp  
URI: <http://www.sfc.wide.ad.jp/~asaeda/>

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

Email: pierrick.seite@orange.com  
URI:



Network working group  
Internet Draft  
Category: Informational  
Created: October 25, 2010  
Expires: April 2011

Q. Wu  
H. Liu  
Huawei

Proposal for Tuning IGMPv3/MLDv2 Protocol Behavior in Wireless and  
Mobile networks

draft-wu-multimob-igmp-mld-tuning-03

Abstract

This document proposes a variety of optimization approaches for tuning IGMPv3 and MLDv2 protocols. It aims to provide useful guideline to allow efficient multicast communication in wireless and mobile networks using the current IGMP/MLD protocols.

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 RFC-2119 [RFC2119].

Status of this Memo

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

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

This Internet-Draft will expire on August 15, 2009.

#### Copyright Notice

Copyright (c) 2010 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.

#### Table of Contents

1. Introduction.....	3
2. Impact of wireless and mobility on IGMP/MLD.....	3
2.1. Comparison analysis between wired and wireless multicast.	4
2.2. Link models analysis for wireless multicast.....	5
2.3. Requirements of wireless and mobile multicast on IGMP/MLD8	
3. Evaluation of IGMP/MLD on wireless and mobile multicast.....	9
4. IGMP/MLD tuning optimization for Wireless or Mobile Network..	11
4.1. Explicit Tracking and Query Suppression.....	11
4.2. Report Suppression for the hosts.....	13
4.3. Query Suppression for the routers.....	13
4.4. Minimizing Query Frequency by increasing interval each time	
.....	14
4.5. Switching Between Unicast Query and Multicast Query.....	15
4.6. Using General Query with Unicast Query.....	16
4.7. Retransmission of General Queries.....	16
4.8. General Query Suppression with no receiver.....	17
4.9. Tuning Response Delay according to link type and status.	17
4.10. Triggering reports and queries quickly during handover.	18
5. Security Considerations.....	19
6. Acknowledgement.....	19
7. References.....	19

7.1. Normative References.....	19
7.2. Informative References.....	20
Authors' Addresses.....	21

## 1. Introduction

Multicasting is more efficient a method of supporting group communication than unicasting. With the wide deployment of different wireless networks, multicast communication over wireless network comes to attract more and more interests from content and service providers, but still faces great challenges when considering dynamic group membership and constant update of delivery path due to node movement, which is highly required in the wireless or mobile network. On the other hand, unlike wired network, some of wireless networks often offer limited reliability, consume more power and cost more transmission overhead, thus in worse case are more prone to loss and congestion.

Multicast network is generally constructed by IGMP/MLD group management protocol to track valid receivers and by multicast routing protocol to build multicast delivery paths. This document focuses only on IGMP/MLD protocols, which are used by a mobile user to subscribe a multicast group and are most possibly to be exposed to wireless link to support terminal mobility. As IGMP and MLD are designed for fixed users using wired link, they does not work perfectly for wireless link types. They should be enhanced or tuned to adapt to wireless and mobile environment to meet the reliability and efficiency requirements in the scenarios described in [REQUIRE][RFC 5757].

This memo proposes a variety of optimization approaches for tuning IGMP/MLD protocols in wireless or mobile communication environment. It aims to make the minimum tuning on the protocol behavior without introducing interoperability issues, and to improve the performance of wireless and mobile multicast networks. These solutions can also be used in wired network when efficiency and reliability are required. They are discussed in detail in Section 4.

## 2. Impact of wireless and mobility on IGMP/MLD

This section analyzes the impact of wireless or mobility on IGMP/MLD by comparing wireless multicast with wired multicast and comparing different wireless link models. It then gives the requirements of

wireless and mobile multicast on IGMP/MLD protocols according to the analysis.

## 2.1. Comparison analysis between wired and wireless multicast

Existing multicast support for fixed user can be extended to mobile users in wireless environments. However applying such support to wireless multicast is difficult for the following five reasons.

- O Limited Bandwidth: In contrast with wired link, wireless link usually has limited bandwidth. This situation will be made even worse if wireless link has to carry high volume video multicast data. Also the bandwidth available in upstream direction and downstream direction may not be equal.
- O Large packets Loss: In contrast with wired multicast, wireless multicast has packet loss that range between 1% and 30%, based on the links types and conditions. And when packets have to travel between home and access networks e.g. through tunnel, the packets are prone to be lost if the distance between the two networks is long.
- O Frequent Membership change: In fixed multicast, membership change only happens when a user leave or joins a group while in the mobile multicast, membership changes may also occur when a user changes its location.
- O Prone to performance degradation: Due to possible unwanted interaction of protocols across layers and user movement, the wireless network may be overwhelmed with more excessive traffic than wired network. In worse case, this may lead to network performance degrading and network connection complete loss.
- O Increased Leave Latency: Unlike fixed multicast, the leave latency in the mobile multicast will be increased due to user movement. And if the traffic has to be transmitted between access network and the home network, or if the handshake is required between these two networks, the Leave Latency will be increased further more.

Figure 1 shows the details for the difference between wired/fixed multicast and wireless/mobile multicast.



Issues	Wired or fixed Multicast	Wireless/mobile multicast
Bandwidth	Plentiful	Limited and variable possibly asymmetric
Loss of Packets	Infrequent(<1%)	Frequent and variable (1%-30% based on links)
Membership Changes	Only when a user leaves and joins a group	Also when a user moves to another location
Reliability	Possible use of a transport-layer protocol(such as the Multicast File Transfer Protocol)	More complex due to wireless links and user mobility; possible unwanted interaction of protocols at transport and link layers
Leave Latency	not changed by user movement	Increased due to user movement and lost packet

Figure 1. Comparison between wired/fixed multicast and wireless/mobile multicast

## 2.2. Link models analysis for wireless multicast

There are various types of wireless links, each with different feature and performance. In this document, we according to the transmission mode categorize the wireless link type into three typical link models:

- O Point To Point (PTP) link model
- O Point To Multipoint (PTMP) link model
- O Broadcast link model

PTP link model is the model with one dedicated link that connects exactly two communication facilities. For multicast transmission, each PTP link has only one receiver and the bandwidth is dedicated

for each receiver. Also one unique prefix or set of unique prefixes will be assigned to each receiver. Such link model can be accomplished by running PPP on the link or having separate VLAN for each receiver.

PTMP link model is the model with multipoint link which consists of a series of receivers and one centralized transmitter. Unlike P2P link model, PTMP provide downlink common channels and dedicated uplink channel for each user. Bandwidth and prefix in this model are shared by all the receivers on the same link. Therefore Duplicate Address Detection (DAD) should be performed to check whether the assigned address is used by other receivers.

Broadcast link model is the model with the link connecting two or more nodes and supporting broadcast transmission. Such link model is quite similar to fixed Ethernet link model and its link resource is shared in both uplink and downlink directions. The bandwidth and prefix are shared by all the receivers and DAD is required to avoid address collision.

Figure 2 shows the details for the difference between different wireless link models.

Features	PTP link model	PTMP link model	Broadcast link model
Shared link/ Dedicated link	Dedicated uplink and downlink channels for each user	Common downlink channels and dedicated uplink channels for each user	common downlink Channel for each user
Shared Prefix /Dedicated Prefix	Per Prefix for each receiver No need DAD	Prefix shared by all receivers DAD is required	Prefix shared by all receivers DAD is required
Shared Service Support	Not Support	Support	Support
link layer Broadcast Multicast Support	Only one node On the link Forward multicast packets to the only receiver on the link	Link Layer Multicast Support using Backend (e.g.,AR) IGMP/MLD Snooping at AR	Broadcast Support at L2 using switch  IGMP/MLD Snooping at switch
Ethernet link Support	Not support	Not support	Ethernet Support By Implementing Bridge

Figure 2. Wireless Link Models Analysis

### 2.3. Requirements of wireless and mobile multicast on IGMP/MLD

Due to the characteristics of wireless and mobile multicast described in the section 2.1 and 2.2, it is desirable for IGMP and MLD to have the following characteristics when used in wireless and mobile networks [REQUIRE]:

- o Adaptive to different link characteristics: IGMP and MLD are originally designed for wired multicast and some of their processing is not applicable to wireless multicast for its asymmetrical link, limited bandwidth, larger packet loss rate, increased leave latency, and etc. Also Wireless network has various link types, each of them has different bandwidth and performance. These require IGMP/MLD protocol behavior should be tuned to adapt to different link model and link conditions.

- o Minimal Join and Leave Latency: Fast join and leave of a subscriber helps to improve the user's experience during channel join and channel zapping. Fast leave also facilitates releasing of unused network resources quickly. Besides, mobility and handover may cause a user to join and leave a multicast group frequently, which also require fast join and leave to accelerate service activation and to optimize resource usages.

- o Robustness to packet loss: Wireless link has the characteristic that packet transmission is unreliable due to instable link conditions and limited bandwidth. For mobile IP network, packets sometimes have to travel between home network and foreign network and have the possibility of being lost due to long distance transmission. These network scenarios have more strict robustness requirement on delivery of IGMP and MLD protocol messages.

- o Minimum packet transmission: Wireless link resources are usually more precious and limited compared to their wired counterpart, and are prone to be congested when carrying high volume multicast stream. Minimizing packet exchange without degrading general protocol performance should also be emphasized to improve efficiency and make good use of network capacity and processing capability.

- o Avoiding packet burst: Large number of packets generated within a short time interval may have the tendency to deteriorate wireless network conditions. IGMP and MLD when using in wireless and mobile networks should be optimized if their protocol message generation has the potential of introducing packet burst.

According to these requirements, in the following parts of the document, current versions of IGMP/MLD protocols are evaluated whether their various protocol aspects are applicable to wireless and mobile multicast communications. They will be optimized to meet these requirements without new features introduced on the wire or link, without new message type defined, and without interoperability issues introduced, which is referred to as "tuning" of IGMP/MLD protocols.

### 3. Evaluation of IGMP/MLD on wireless and mobile multicast

This section analyzes the applicability of IGMP and MLD to wireless communication in the following aspects:

- O General evaluation of different versions: IGMPv2 [RFC2236] and MLDv1 [RFC2710] only support ASM communication mode. They do not support SSM subscription and explicit tracking. IGMPv3 [RFC3376] and MLDv2 [RFC3810] and their lightweight version LW-IGMPv3/LW-MLDv2 [RFC5760] support all the features of ASM/SSM communication modes and explicit tracking. Because SSM is more efficient and secure than ASM for IPTV application, and explicit tracking enables faster channel zapping and better manageability capability, IGMPv3/MLDv2 and LW-IGMPv3/MLDv2 are more promising to be deployed widely than IGMPv2 and MLDv1.
- O Robustness: IGMP/MLD actively sends unsolicited Report or Leave message to join or leave a group, and solicited Report to respond to Queries. Unsolicited Report and Leave messages are more important for ensuring satisfactory user experience and should be guaranteed to improve service performance. Current IGMP and MLD provide the reliability for these messages by non responsive retransmission, which is not adequate from both the robustness and efficiency aspects when they are used on unreliable wireless link or have to be exchanged over the tunnel between home network and access network separated by long distance [ROBUST][ACK]. For IGMPv3/MLDv2, because unsolicited report and leave messages will not be suppressed by report from other host, it is possible to adopt acknowledgement-retransmission to improve reliability and reduce superfluous packet transmission [IGMP-ACK].

Besides, for IGMPv3/MLDv2, because the router could by explicit tracking establishes membership database recording each valid receiver, it is possible to deduce the possible loss of some protocol messages according to the feedback after their transmission, and to take some remedies (e.g. by retransmission)

to enable more reliable transmission of these messages in bad conditions.

- O Efficiency: IGMPv2 and MLDv1 use host suppression to suppress duplicated membership reports on the link. In IGMPv3 and MLDv2, because host suppression is not adopted, the report count will be numerous if the number of valid receivers on the network is large. IGMPv3 and MLDv2 should be optimized to try to minimize unnecessary packet transmission to compensate this drawback. As an example, because an IGMPv3/MLDv2 router has record of each user in its state database by explicit tracking, it is possible to eliminate the need for query timeouts when receiving leave messages and to improve the efficiency by reducing both the unnecessary Queries and reports generated on a network.

And as described in [REQUIRE] and [RFC5757], the default timer values and counter values specified in IGMP and MLD were not designed for the mobility context. This may result in a slow reaction following a client join or leave, in possible packet loss under worse conditions, or in overburdening the wireless link by excessive packets exchange than necessary. These issues can be addressed by tuning these parameters for the expected packet loss on a link to optimize service performance and resource usage.

The comparison between IGMPv2/MLDv1 and IGMPv3/MLDv2 is illustrated in figure 3. In summary, it is desirable to choose IGMPv3/MLDv2 or LW-IGMPv3/MLDv2 as the group management protocol for wireless or mobile multicast. They should be optimized to adapt to wireless and mobile networks to meet the efficiency and reliability requirement for these networks. These optimizations range from the tuning of the parameters (e.g. the Query Interval and other variables), to the tuning of protocol behavior without introducing interoperability issues. Considering an enhancement in one direction might introduce side effects in another one, balances should be taken carefully to avoid defects and improve protocol performance as a whole.

Issues	IGMPv2/MLDv1	IGMPv3/MLDv2
Default Timer and Robustness Variable	Not designed for Mobility context Need to be tuned	Not designed for Mobility context Need to be tuned
Explicit Tracking	Not Support	Support
ASM and SSM Subscription	Only Support ASM Subscription	Both Support
Explicit Join and Leave	Support	Support
Host Suppression	Support	Not Support

Figure 3. Comparison between IGMPv2/MLDv1 and IGMPv3/MLDv2

#### 4. IGMP/MLD tuning optimization for Wireless or Mobile Network

As mentioned in section 2, IGMPv3/MLDv2 or LW-IGMPv3/MLDv2 is recommended to be used as the basis for optimization of IGMP/MLD to adapt to wireless and mobile networks. In this section, taking these characteristics requirement into account, we will discuss several optimization approaches for tuning of IGMPv3 and MLDv2 in wireless environment. The optimizations try to minimize the packet transmission for both the Reports and Queries, and at the meanwhile take the factor of improving reliability into account, with minimum cost. Different link types are also considered for the tuning behavior.

##### 4.1. Explicit Tracking and Query Suppression

In IGMPv2/MLDv1, the member reports are suppressed if the same report has already been sent by another host in the network which is also referred to as host suppression. As described in the A.2 of [RFC3810], the suppression of multicast listener reports has been removed in MLDv2 due to the following reasons:

- o Routers may want to track per-host multicast listener status on an interface. This enables the router to track each individual host that is joined to a particular group or channel and allow minimal leave latencies when a host leaves a multicast group or channel.
- o Multicast Listener Report suppression does not work well on bridged LANs. Many bridges and Layer2/Layer3 switches that implement MLD snooping do not forward MLD messages across LAN segments in order to prevent multicast listener report suppression.
- o By eliminating multicast listener report suppression, hosts have fewer messages to process; this leads to a simpler state machine implementation.
- o In MLDv2, a single multicast listener report now bundles multiple multicast address records to decrease the number of packets sent. In comparison, the previous version of MLD required that each multicast address be reported in a separate message.

Without host suppression, it is possible to enable explicit tracking on a router by which the local replication can be used by the router to inspect incoming join and leave requests, record or refresh the membership state for each host on the interface, and take appropriate action to each received report. In the meanwhile, the router builds a table to track which channel being forwarded to each port. If the channel being requested to view is already being received at the router, it can replicate the stream and forward to this new requester which ensure good response time.

By using the tracking table mentioned above, the router has the capability to learn if a particular multicast address has any members on an attached link or if any of the sources from the specified list for the particular multicast address has any members on an attached link or not. Such capability makes Group specific Query or Source-and-Group Specific Queries, which are sent to query other members when a member leaves, unnecessary to be used because the router has already known who are active on the interface using explicit tracking. Therefore it is desirable that these two Queries are eliminated when explicit tracking is used. But General periodical Query by a router to solicit current state reports to refresh existing membership state database should still be used to prevent incorrectness of the database due to the possible loss of explicit join and leave message in some cases.

The main benefits of using explicit tracking without Group specific Query or Source-and-Group Specific Queries are that it provides:



- O minimizing packet number and packet burst: Elimination of Group and Source-Group specific Queries when a member leaves a group will reduce the number of transmitted Group Specific Queries. And finally the total number of Reports in response to Group Specific Queries can be drastically reduced.
- O Minimal leave latencies: an IGMPv3/MLDv2 router configured with explicit tracking can immediately stop forwarding traffic if the last host to request to receive traffic from the router indicates its leave from the group.
- O Faster channel changing: The channel change time of the receiver application depends on the leave latency, that is to say, single host can not receive the new multicast stream before forwarding of the old stream has stopped.
- O Reducing Power consumption: Due to elimination of the suppression of membership reports, the host does not need to spend processing power to hear and determine if the same report has already been sent by another host in the network, which is beneficial to mobile hosts that do not have enough battery power.

#### 4.2. Report Suppression for the hosts

The large number of Reports and bad link condition may result in packets burst. This packet burst can be mitigated by having the router aggregate the responses (membership reports) from multiple clients. The router can intercept IGMP/MLD reports coming from hosts, and forwards a summarized version to the upstream router only when necessary. Typically this means that the router will forward IGMP/MLD membership reports as follows:

- Unsolicited membership reports (channel change requests) are forwarded only when the first subscriber joins a multicast group, or the last subscriber leaves a multicast group. This tells the upstream router to begin or stop sending this channel to this router.
- Solicited membership reports (sent in response to a query) are forwarded once per multicast group. The router may also aggregate multiple responses together into a single membership report.

#### 4.3. Query Suppression for the routers

The large number of Queries and bad link condition may result in packets burst. This packet burst can be mitigated by having the downstream router stop forwarding IGMP/MLD Queries packets sent to

the hosts and respond with report as proxy to the upstream router. Typically this means that the router will:

- Never send a specific query to any client, and
- Send general queries only to those clients receiving at least one multicast group

#### 4.4. Minimizing Query Frequency by increasing interval each time

In IGMPv3/MLDv2, Group Specific Queries and Source and Group specific Queries are sent for [Last Member Query Count] times with short fixed [Last Member Query Interval], to learn whether there are valid members from an attached link. If the network is undergoing congestion, the multiple transmissions of the queries may further deteriorate the bad conditions. To eliminate the bad effects for this, these Queries can be slowed down when a router can not collect successfully expected members' report responses in the mean while it detects the network congestion is going to happen. The slowing down process of the Queries could be arranged in a prolonged time interval as described in [ADAPTIVE].

The slow down behavior is: a router after sending a Query, if acquires the expected responses from the receivers, refreshes its state database and stop the querying retransmission process, or if after a time interval fails to get the expected report responses, resends a Query with an increased (e.g. double) interval. This process can be repeated, for each time the retransmission is arranged in a prolonged time interval, till the router receives the expected responses, or determines the receiver is unreachable and then stops the sending of the Query ultimately. The router can make judgment on not getting expected response from the Queries in the following cases:

- O When Group Specific Query and Source and Group Specific Queries are used to track other numbers, the router can not collect any response from the link.
- O When all group members leave the group or move out of scope, the General Query sent by the router can not solicit any responses from the link, as mentioned in section 4.9.
- O When General Query is retransmitted due to possible loss deducing from no responses from valid members in the database.

- O When General Query is retransmitted by a router on startup [RFC3376][RFC3810], it gets no membership response from the interface.
- O When unicast Query is sent to solicit a particular receiver, if the router can not get responses from the receiver, as described in section 4.5 and 4.6.

In the above cases, if the router fails to get expected response from the network, and if the link condition is bad or in congestion, the router could retransmit the Queries in increased interval. This query retransmission with incremental interval enables the router to reduce the total packet retransmission times in the same time period comparing with retransmission for multiple times with fixed interval, and at the mean time gain some degree of reliability. The variable time interval and the termination condition should be configurable and could be set according to actual network condition, which is out the scope of this document.

#### 4.5. Switching Between Unicast Query and Multicast Query

IGMP/MLD protocols define the use of multicast Queries whose destination addresses are multicast addresses and also allow use of unicast Queries with unicast destination. The unicast Query is sent only for one destination and has the advantages of not affecting other host on the same link. This is especially desirable for wireless communication because the mobile terminal often has limited battery power. But if the number of valid receivers is large, using unicast Query instead of multicast Query will introduce large number of Queries because each Query will be generated for each member, which will not be an efficient use of link resources. In this case the normal multicast Query will be a good choice because only one Query needs to be sent. On the other hand of the number of receivers to be queried is small, the unicast Query is advantageous over multicast one.

The router can choose to switch between unicast and multicast Query according to the practical network conditions. For example, if the receiver number is small, the router could send unicast Queries respectively to each receiver to solicit their membership states, without arousing other host which is in the dormant state. When the receiver number reaches a predefined level, the router could change to use multicast Queries. The router could make the switching flexibly according to practical conditions to improve the efficiency.

#### 4.6. Using General Query with Unicast Query

Unicast Query also can be used in addition to General Query to improve the robustness of solicited reports when General Query fails to collect its valid members. It requires the explicit tracking to be enabled on the router. Its basic behavior is: a router after sending a periodical Query collects successfully all the members' report responses except for one or two which are currently still valid in its database. This may be because the non-respondent ones silently leave the network without any notification, or because their reports are lost due to some unknown reason. The router in this case could choose to unicast a Query respectively to each non-respondent receiver to check whether they are still alive for the multicast reception, without affecting the majority of receivers that have already responded. Unicast Queries under this condition could be sent for [Last Member Query Count] times, following the same rule of [3376] or [3810], or could be resent in incremental interval, as described in section 4.4.

#### 4.7. Retransmission of General Queries

In IGMPv3 and MLDv2, apart from the continuously periodical transmission, General Query is also transmitted during a router's startup. It will be transmitted for [Startup Query Count] times with [Startup Query Inteval], to improve reliability of General Query during startup. There are some other cases where retransmission of General Query is beneficial which are not covered by current IGMPv3/MLDv2 protocols as shown in the following.

For example, a router which keeps track of all its active receivers, if after sending a General Query, may fail to get any response from the receivers which are still valid in its membership database. This may be because all the valid receivers leaves the groups or moves out of the range of the link at the moment, or because all the responses of the receivers are lost, or because the sent Query does not arrive at the other side of the link. If current database indicates the number of the valid receiver is not small, the router could choose to compensate this situation by retransmitting the General Query to solicit its active members.

This compensating General Query could be sent several times, if the router can not get any feedback from the receivers which are previous in the database. The repetition of the transmission could in fixed

interval such as [Last Member Query Interval], or could in prolonged interval if the link condition is not good.

#### 4.8. General Query Suppression with no receiver

In IGMPv3 and MLDv2, General Query is multicast sent periodically and continuously without any limitations. It helps solicit the state of current valid member but has influence on all terminals, whether they are valid multicast receivers or not. When there is no receiver on the link, the transmission of the General Query is a waste of resources for both terminals and the router.

The IGMPv3/MLDv2 router could suppress its transmission of General Query if there is no valid multicast receiver on the link, e.g. in the following cases:

- O If the last member reports its leave for a group. This could be judged by an explicit tracking router checking its membership database, or by a non explicit tracking router sending Group and Source Group Specific Queries;
- O If the only member on a PTP link reports its leaving;
- O If the router after retransmission of General Queries on startup fails to get any response from any member;
- O If the router previously has valid members but fails to get any response from any member after several rounds of General Queries or Unicast Queries;

In these cases the router could make a decision that no member is on this link and totally stop its transmission of periodical General Queries. If afterwards there is valid multicast receiver joins a group, the router could resume the original cycle of transmission of General Queries. Because General Query has influences on all the terminals on the link, suppressing it when it is not needed is beneficial for both the link efficiency and terminal power saving.

#### 4.9. Tuning Response Delay according to link type and status

IGMPv3 and MLDv2 use delayed response mechanism to spread Report messages from different hosts over a longer interval which can greatly reduce possibility of packet burstiness. This is implemented by the host responding to a Query in a specific time randomly chosen between 0 and [Maximum Response Delay]. The value of [Maximum Response Delay] parameter is determined by the router and is carried

in Query messages to inform the valid hosts to make the selection. A long delay will lessen the burstiness but will increase leave latency (the time between when the last listener stops listening to a source or multicast address and when the traffic stops flowing).

In order to avoid burstiness of MLD messages and reduce leave latency, explicit tracking with Group Specific Query eliminated is recommended to be used first to reduce leave latency. Then the Response Delay may be dynamically calculated based on the expected number of Reporters for each Query and link type and link status.

- o If the expected number of Reporters is large and link condition is bad, the system administrator MUST choose the longer Maximum Response Delay; if the expected number of Reporters is small and the link condition is good, the administrator may choose the smaller Maximum response Delay. In this case, the IGMP/MLD packet burstiness can be reduced.
- o Another case is if the link type is PTP which means the resource is dedicated for one receiver on each link, then the Maximum Response Delay can be chosen smaller, if the link type is shared medium link or P2MP, then the Maximum Response Delay can be configured larger.

The Maximum Response Delay can be configured by the administrator as mentioned above, or be calculated automatically by software tool implemented according to experiential model on different link modes. As the router arrives at a value appropriate for current link type and conditions, it will encode the value in Query messages to inform the host to make the response. The determination of the instant Maximum Response Delay value is out of this document's scope.

#### 4.10. Triggering reports and queries quickly during handover

As a mobile terminal is moving from one network to another, if it is a multicast receiver from a group, its new access network should try to deliver the content to the receiver without disruption or performance deterioration. For the smooth switching between networks, the terminal's membership should be acquired as quickly as possible by the new access network.

For the access router, it could trigger a Query to the terminal as soon as it detects a new terminal on its link. This could be a General Query if the router does not know whether or not the terminal is a valid receiver or if the number of the entering terminals is not small. Or this Query could also be a unicast Query

for only a small quantity of terminals to prevent unnecessary action of other terminals in the switching area.

For the terminal, it could trigger a report if it is currently in the multicast reception state. This helps establish more quickly the membership states and enable faster multicast stream injection because active report from the host does not requires the router to wait for the query-response round in the passive reporting cases.

## 5. Security Considerations

They will be described in the later version of this draft.

## 6. Acknowledgement

The authors would like to thank Stig,Venaas, Gorrry Fairhurst, Thomas C. Schmidt, Marshall Eubanks, Suresh Krishnan, J.William Atwood, WeeSan Lee, Imed Romdhani, Hitoshi Asaeda, Liu Yisong and Wei Yong for their valuable comments and suggestions on this document.

## 7. References

### 7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to indicate requirement levels", RFC 2119, March 1997.

[RFC1112] Deering, S. "Host Extensions for IP Multicasting", RFC1112, August 1989.

[RFC2236] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.

[RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.

[RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2(MLDv2) for IPv6", RFC 3810, June 2004.

[RFC4607] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.

[RFC5790] Liu, H., Cao, W., and H. Asaeda, "Lightweight IGMPv3 and MLDv2 Protocols", RFC5790, February 2010.

## 7.2. Informative Referencess

[REQUIRE] H. Liu, Q. Wu, H. Asaeda and TM. Eubanks, "Mobile and Wireless Multicast Requirements on IGMP/MLD Protocols", draft-liu-multimob-igmp-mld-mobility-req-03.txt, March 2010.

[ROBUST] A. Sen Mazumder, "Facilitating Robust Multicast Group Management", NOSSDAV'05, June 13-14, 2005, Stevenson, Washington, USA.

[ACK] Nikaein, N. and Bonnet, C. "Wireless multicasting in an IP environment" In Proceedings of the 5th International Workshop on Mobile Multimedia Communication MoMuc'98 (Berlin, Germany, Oct. 12-14). IEEE Computer Society Press, 1998.

[IGMP-ACK] H. Liu, Q. Wu, "Reliable IGMP and MLD Protocols in Wireless Environment", draft-liu-multimob-reliable-igmp-mld-00.txt, February 2010.

[ADAPTIVE] I. Romdhani, J. Munoz, H. Bettahar, and A. Bouabdallah, "Adaptive Multicast Membership Management for Mobile Multicast Receivers", IEEE, 2006.

[RFC5757] Schmidt, T., Waehlich, M., and G. Fairhurst, "Multicast Mobility in Mobile IP Version 6 (MIPv6): Problem Statement and Brief Survey", RFC 5757, February 2010.



Authors' Addresses

Qin Wu  
Huawei Technologies Co., Ltd.  
Site B, Floor 12, Huihong Mansion, No.91 Baixia Rd.  
Nanjing, Jiangsu 21001  
China  
Phone: +86-25-84565892

EMail: sunseawq@huawei.com

Hui Liu  
Huawei Technologies Co., Ltd.  
Huawei Bld., No.3 Xixi Rd.  
Shang-Di Information Industry Base  
Hai-Dian District, Beijing 100085  
China

EMail: Liuhui47967@huawei.com

