

MULTIMOB Group
Internet-Draft
Intended status: Standards Track
Expires: May 3, 2012

H. Asaeda
Keio University
P. Seite
France Telecom
J. Xia
Huawei
October 31, 2011

PMIPv6 Extensions for PIM-SM
draft-asaeda-multimob-pmip6-extension-07

Abstract

This document describes Proxy Mobile IPv6 (PMIPv6) extensions to support IP multicast. 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 extension addresses the tunnel convergence problem and provides seamless handover. This document defines the Proxy Binding Update and the Proxy Binding Acknowledgement messages with multicast extension.

Status of this Memo

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

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

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

This Internet-Draft will expire on May 3, 2012.

Copyright Notice

Copyright (c) 2011 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	4
2. Conventions and Terminology	6
3. Overview	7
3.1. Multicast Communication in PMIPv6	7
3.2. Protocol Sequence for Multicast Channel Subscription	9
4. Multicast Messages over Bi-directional Tunnel	11
5. Local Mobility Anchor Operation	12
6. Mobile Access Gateway Operation	13
7. Mobile Node Operation	14
8. Smooth Handover	15
8.1. Handover with Policy Profile	15
8.2. Handover with Extended Proxy Binding Update and Acknowledgement	17
9. Message Format Extension	19
9.1. Proxy Binding Update with Multicast Extension	19
9.2. Proxy Binding Acknowledgement Message with Multicast Extension	22
10. IANA Considerations	23
11. Security Considerations	25
12. Acknowledgements	26
13. References	27
13.1. Normative References	27
13.2. Informative References	27
Authors' Addresses	29

1. Introduction

Proxy Mobile IPv6 (PMIPv6) [2] 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 [2], 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 [2], 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 [9] 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 [7] 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 PIM-SM 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 support source mobility. Furthermore, although it would be able to minimize the join latency for mobile nodes attached to a new network by tuning the Startup Query Interval value for the new MAG as proposed in [15], the base solution does not provide any seamless handover mechanism with a context transfer function.

This document describes PMIPv6 extensions to support IP multicast communication for mobile nodes in PMIPv6-Domain. The proposed protocol extension assumes that both LMA and MAG enable the Protocol-Independent Multicast - Sparse Mode (PIM-SM) multicast routing protocol [3]. The proposed extension 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 listener mobility is mainly focused on, the detail specification of source mobility is not described.

The PMIPv6 extension proposed in this document does not require to

change unicast communication methods or protocols defined in [2], 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 [1].

The following terms used in this document are to be interpreted as defined in the Proxy Mobile IPv6 specification [2]; 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) [8]. However, in order to explicitly participate in SSM, mobile nodes MUST support either MLDv2 [4] or Lightweight-MLDv2 (LW-MLDv2) [5].

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.

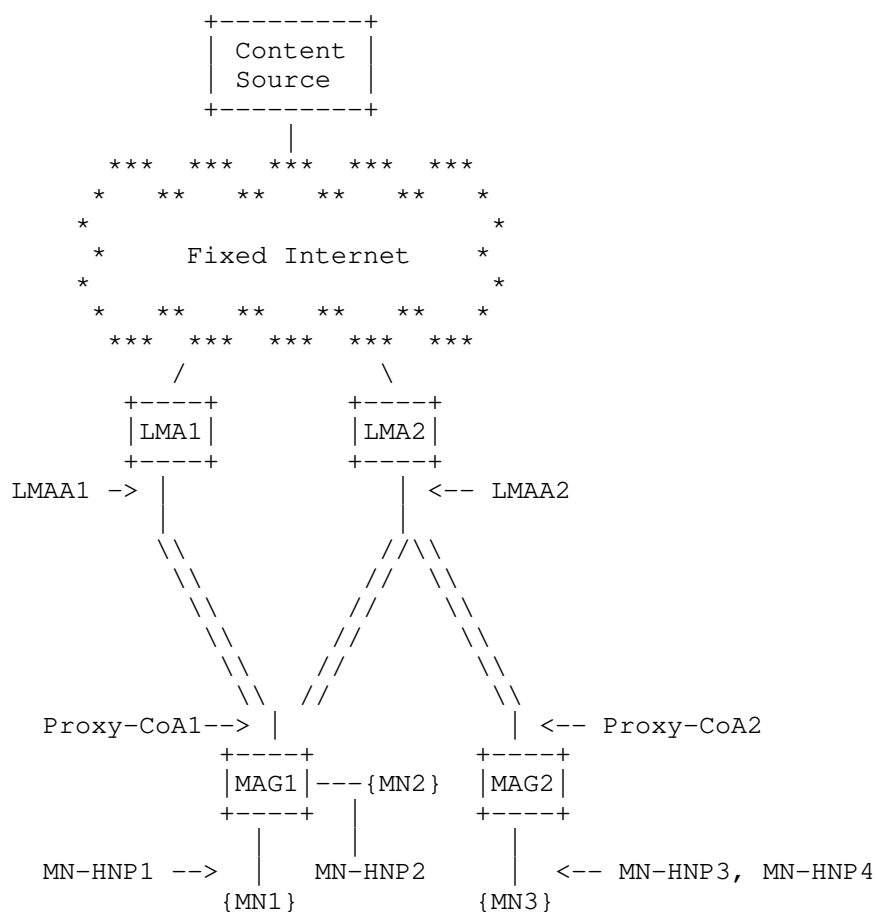


Figure 1: Proxy Mobile IPv6 Domain

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 the LMA-MAG bi-directional IPv6-in-IPv6 tunnel 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 [2]. Mobile node's Policy Profile is provided by "policy store" whose definition is the same as of [2].

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. Although MLDv2 specification [4] permits to use the unspecified address (::) for a host whose interface has not acquired a valid link-local address yet, MAG SHOULD send MLDv2 Report messages with a valid IPv6 link-local source address as defined in [15]. As well, MLDv2 Report messages MAY be sent with an IP destination address of FF02:0:0:0:0:0:0:16, to which all MLDv2-capable multicast routers listen, but the IP unicast address of the attached MAG SHALL be used for the destination of MLDv2 Report messages.

When the MAG operating as a PIM-SM router receives MLD Report messages from attached mobile nodes, it joins the multicast delivery tree by sending PIM Join messages to its neighboring routers (Figure 2). When the upstream router for the requested channel is LMA, the MAG sends the corresponding PIM Join messages over the regular LMA-MAG bi-directional tunnel, if the MAG has no multicast state for the requested channel. When the upstream router for the requested channel is an adjacent router that is not the LMA, the MAG sends the corresponding PIM Join messages to the adjacent upstream router natively, if the MAG has no multicast state for the requested channel. The LMA or the adjacent upstream router then joins the multicast delivery tree and forwards the packets to the downstream MAG.

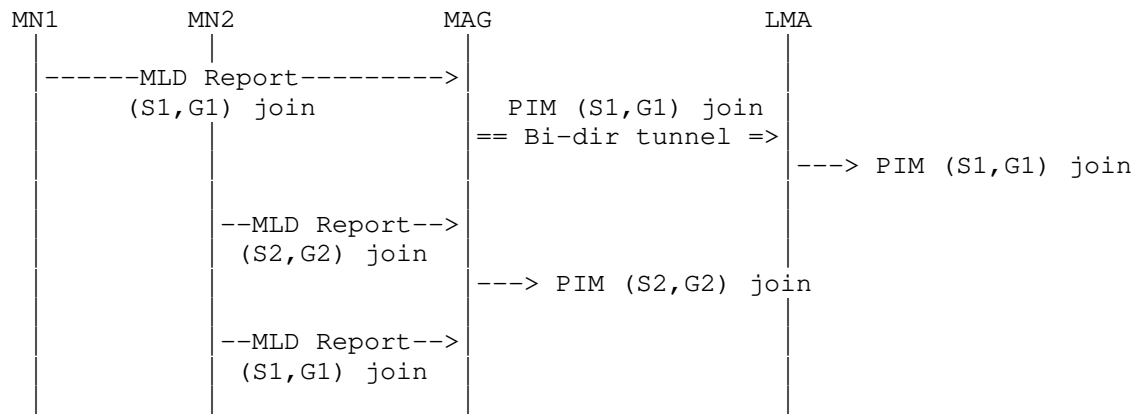


Figure 2: MLD Report Messages Transmission

The MAG selects only one upstream link for a multicast channel by the Reverse Path Forwarding (RPF) algorithm even if the MAG has established multiple bi-directional tunnels for unicast transmission to different LMAs. This does not cause the tunnel convergence problem, because Multicast Routing Information Base (MRIB) used by PIM-SM selects only one incoming interface for each multicast channel and hence duplicate packets are not forwarded to the MAG.

4. Multicast Messages over Bi-directional Tunnel

MLD messages, PIM messages, and IP multicast data are transmitted over the LMA-MAG bi-directional IPv6-in-IPv6 tunnel when the LMA is selected as the previous-hop router for the multicast channel as shown in Figure 3.

```

MC1
 \
  \-->
MC2----->LMA===MC1,MC2 for MNs====>MAG

```

MC: Multicast packets, ==>: Bi-dir tunnel

Figure 3: Multicast channel subscription through the bi-directional tunnel

The format of the tunneled multicast packet forwarded from LMA 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 */
  IPv6 header (src= S, dst= G)           /* Inner Header */
    Upper layer protocols                 /* Packet Content */

```

Figure 4: Tunneled IPv6 multicast packet from LMA to MAG

When an MLD or PIM message is sent from MAG to LMA, the src and dst addresses of tunnel header will be replaced to Proxy-CoA and LMAA, respectively. To convey an MLD or PIM message, the src address of the 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 MLD's condition (see Section 5.1.15 and 5.2.14 of [4]) or the PIM's condition (see [3]).

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 Protocol-Independent Multicast - Sparse Mode (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 LMA-MAG bi-directional 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. [2] 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 is the entity that performs the mobility management on behalf of a mobile node. This document assumes that MAG is capable of forwarding multicast packets to the corresponding mobile nodes attached to MAG by enabling the PIM-SM multicast routing protocol. In addition, 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 [4] or LW-MLDv2 [5], 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 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 LMA-MAG bi-directional tunnel.

The MAG also sends MLD Query messages to attached mobile nodes to maintain up-to-date membership states. Since the MAG may deal with a large number of the downstream mobile nodes, the MLD protocol scalability should be taken into account as described in [15]. Therefore it is RECOMMENDED that the explicit tracking function [16] is enabled on MAG.

7. Mobile Node Operation

Mobile nodes attached to MAG can behave as regular receiver hosts. A mobile node sends MLD messages to 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 [4], MLDv2 [4], or LW-MLDv2 [5], and SHOULD support MLDv2 or LW-MLDv2.

8. Smooth Handover

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. MAG tracks the mobile node's movements to and from the access link and for signaling the mobile node's LMA. In PMIPv6, it SHOULD NOT require for mobile nodes to initiate to re-subscribe multicast channels, and MAG SHOULD keep multicast channel subscription status for mobile nodes even if they move to a different MAG (i.e., n-MAG) in PMIPv6-Domain.

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 should seamlessly receive multicast data from the new MAG according to the multicast channel information stored in the "MN's Policy Profile" or by the "multicast context transfer mechanism". Whether the MN's Policy Profile or the multicast context transfer mechanism mobile operators use depend on their policy or implementation.

8.1. Handover with Policy Profile

When the multicast channel information subscribed by mobile nodes is maintained in "MN's Policy Profile" stored in a policy store [2], MAG can use the channel information to provide seamless handover. The procedures are described as follows and illustrated in Figure 5;

1. Figure 5 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 [14] 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 LMA, the PIM messages are encapsulated and transmitted over the LMA-MAG bi-directional tunnel (*4); otherwise the PIM messages are sent natively to the adjacent upstream router (*3).

4. The multicast data is forwarded from LMA through the bi-directional tunnel between the LMA and n-MAG (*4) or from the adjacent upstream router (*3).

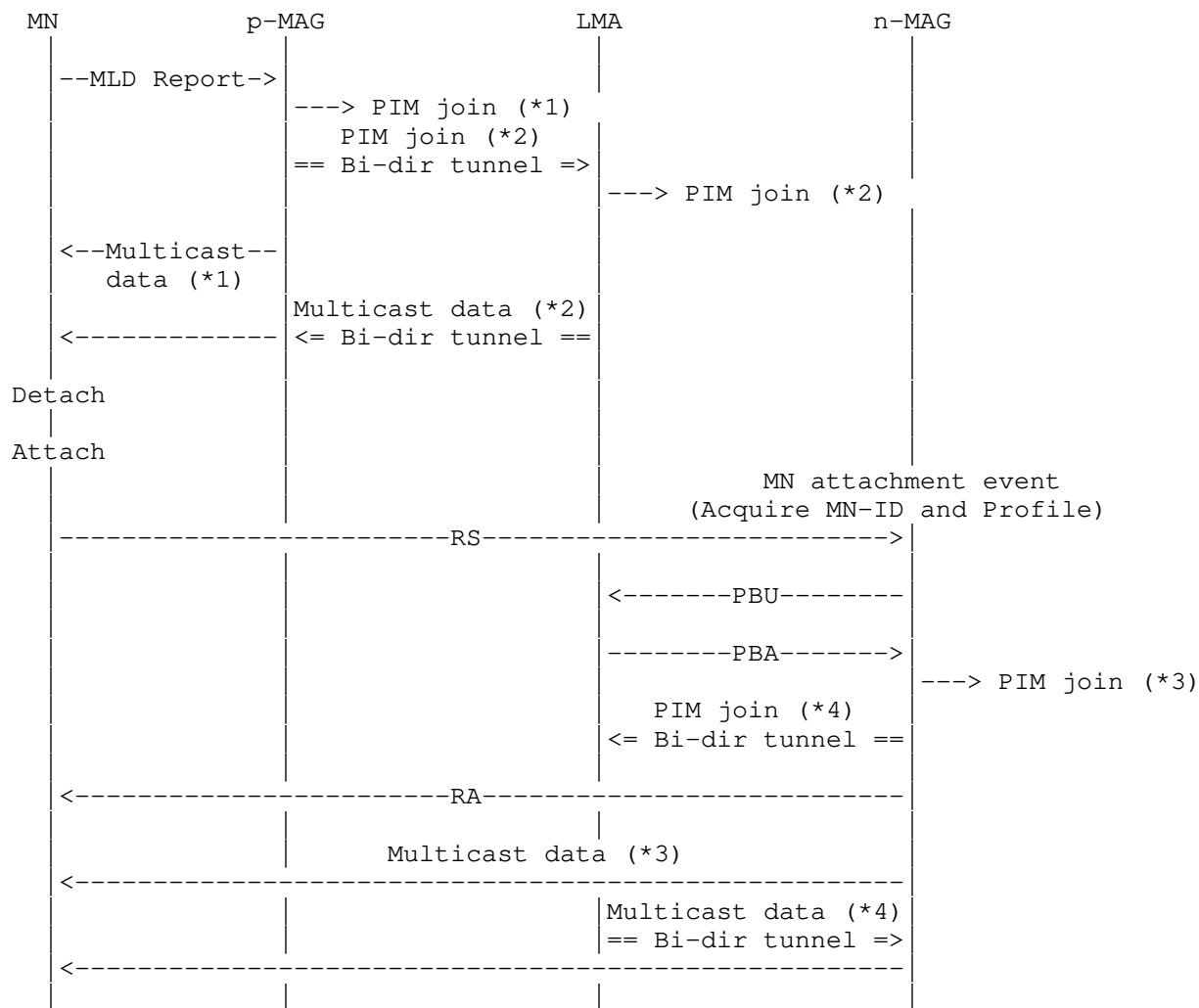


Figure 5: Handover with MN's Policy Profile

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 [16]), 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.

8.2. Handover with Extended Proxy Binding Update and Acknowledgement

This document provides the multicast extension for the PBU message, which is named "Proxy Binding Update with multicast extension (PBU-M)" (detailed in Section 9.1), and the PBA message, which is named "Proxy Binding Acknowledge with multicast extension (PBA-M)" (detailed in Section 9.2), to inform n-MAG to subscribe multicast channel(s) for moving mobile nodes.

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, the p-MAG sends de-registration PBU-M message having the lifetime value of zero (see Section 9.1) to the LMA. The LMA then transmits the PBA message and keeps the multicast channel information included in that message.
3. When the mobile node attaches to n-MAG, the n-MAG obtains the MN-Identifier (MN-ID) and transmits the regular PBU message.
4. Whenever the LMA receives the PBU message, it transmits the PBA-M message including multicast channel information that the mobile node has joined.
5. If there are multicast channels in the channel information the mobile node has subscribed but the n-MAG has not yet subscribed, the n-MAG joins the corresponding multicast channels by sending the PIM Join message to its upstream router.
6. Follow the procedures of step 3 and 4 in Section 8.1.

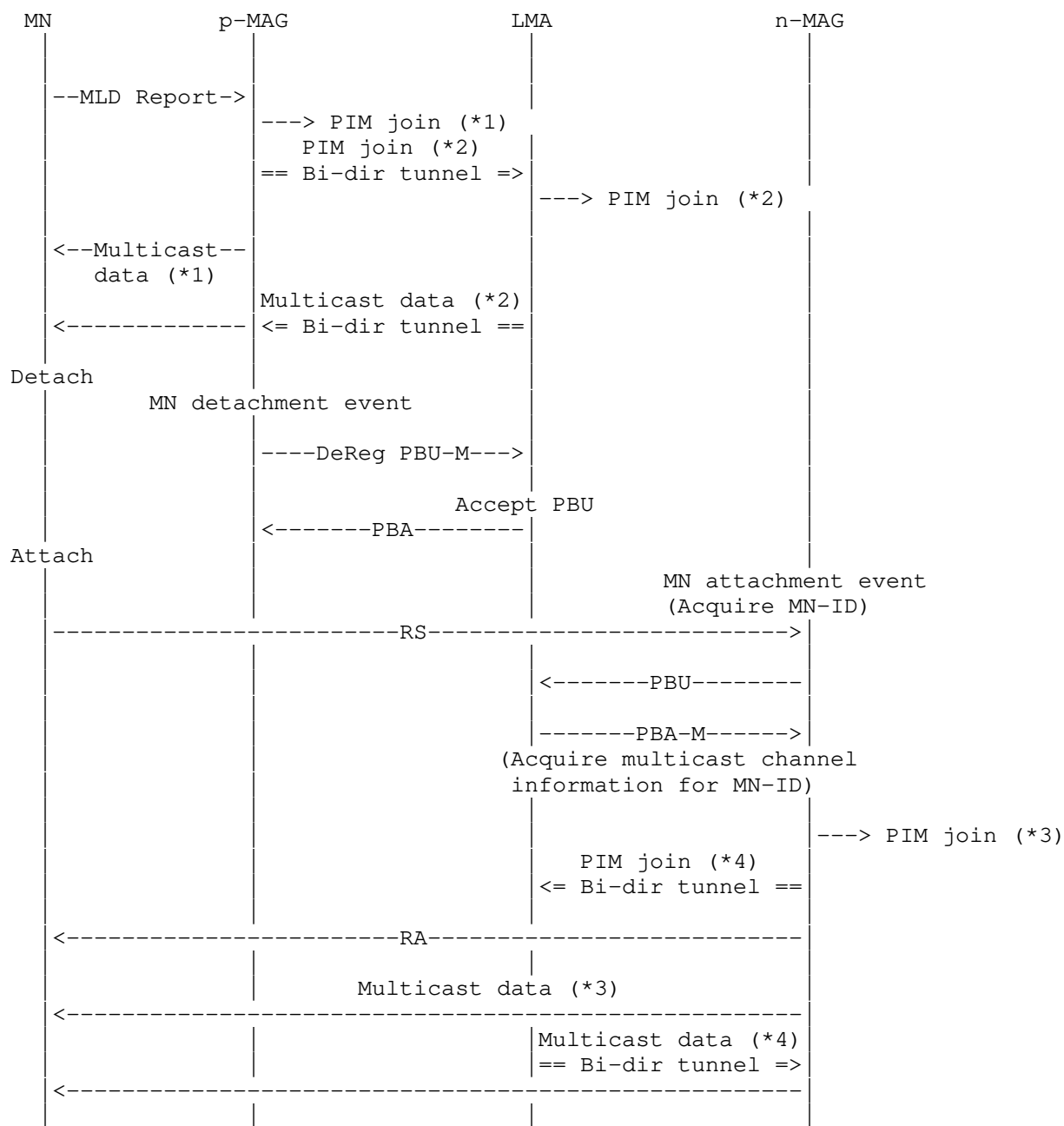


Figure 6: Handover with PBU-M and PBA-M

9. Message Format Extension

9.1. Proxy Binding Update with Multicast Extension

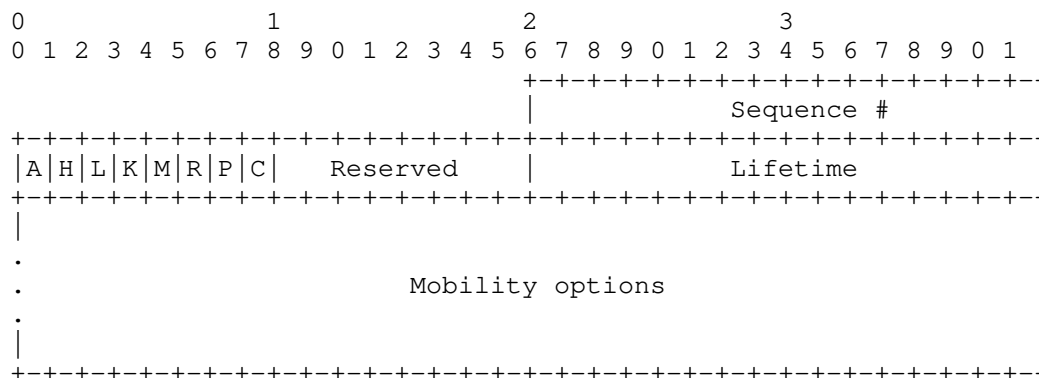


Figure 7: Proxy Binding Update Message with Multicast Extension

A Binding Update message that is sent by MAG to LMA is referred to as the "Proxy Binding Update" message. A new flag (C) is included in the Proxy Binding Update message with Multicast extension (PBU-M). The rest of the Binding Update message format remains the same as defined in [10] and with the additional (R), (M), and (P) flags, as specified in [11], [12], and [2], respectively.

Multicast Channel Subscription Flag

A new flag (C) is included in the Binding Update message to indicate to LMA that the Binding Update message is a multicast channel subscription.

The PBU-M message is transferred for binding de-registration from p-MAG to LMA as specified in Section 8.2, the Lifetime value MUST be zero.

When (C) flag is specified in PBU-M message, the Mobility options field includes "multicast channel information", which is the same information of MLDv2 Report message. The format of the Mobility options field uses the TLV format defined in [10] where the field contain Multicast Address Record with the same definitions in [4].

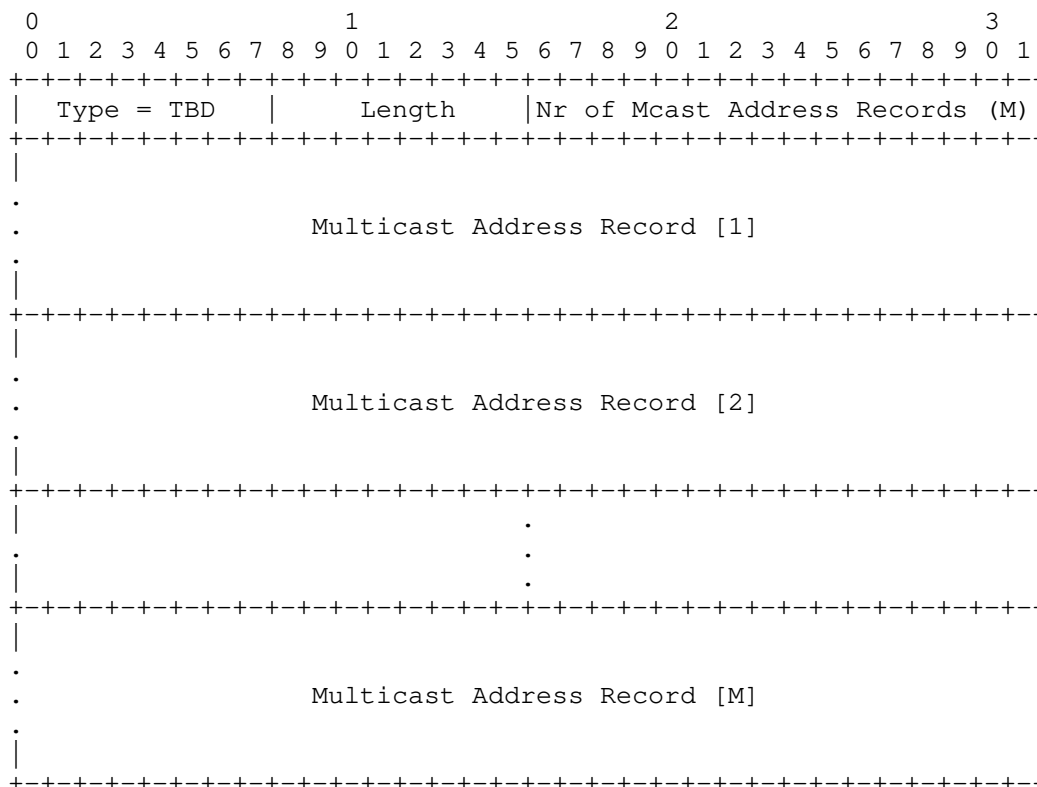


Figure 8: Multicast channel information

Each Multicast Address Record has the following internal format, where the Record Type MUST be always "1" (i.e., MODE_IS_INCLUDE).

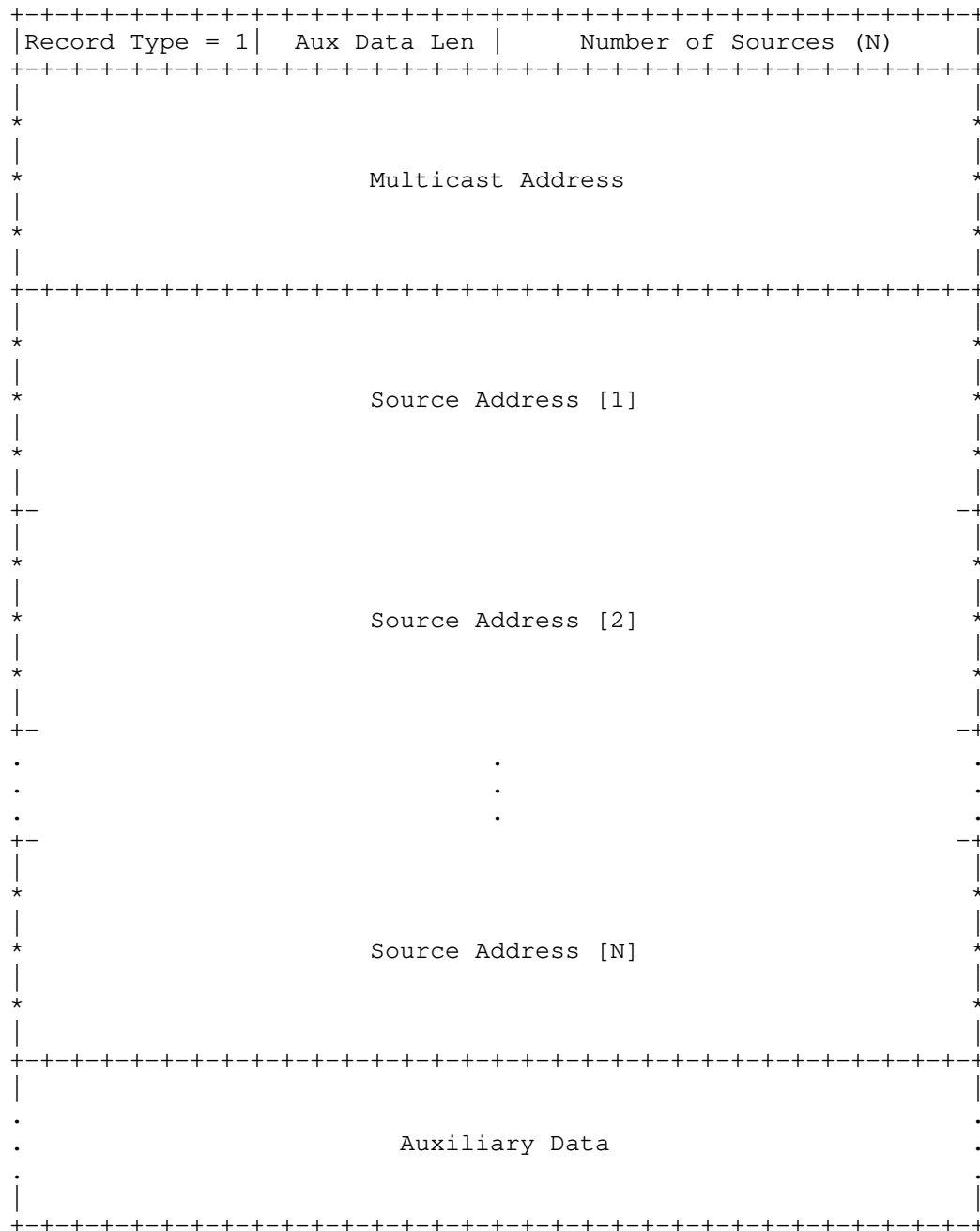


Figure 9: Multicast Address Record format

9.2. Proxy Binding Acknowledgement Message with Multicast Extension

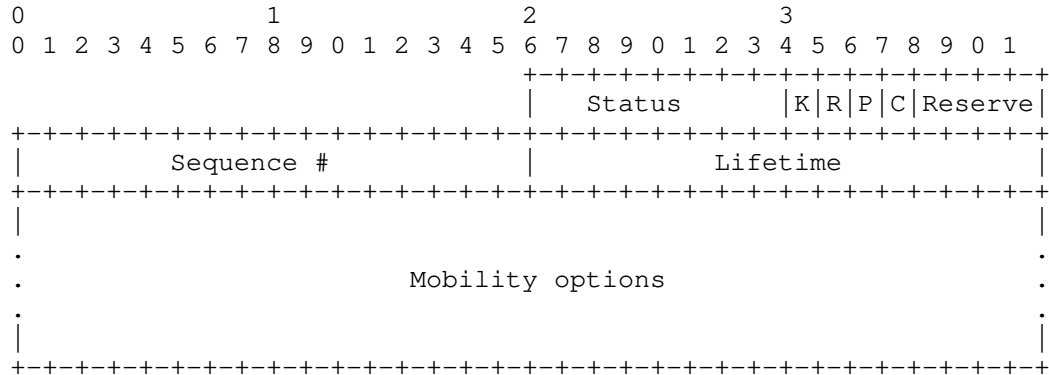


Figure 10: PBA with Multicast Extension

A "Proxy Binding Acknowledgement" message is sent from LMA to MAG in response to a Proxy Binding Update message. A new flag (C) is included in the Proxy Binding Acknowledgement message with Multicast extension (PBA-M). The rest of the Binding Acknowledgement message format remains the same as defined in [10] and with the additional (R) flag, as specified in [11] and [2], respectively.

Multicast Channel Subscription Flag

A new flag (C) is included in the Binding Acknowledgement message to indicate to MAG that the Binding Acknowledgement message is a multicast channel subscription.

When (C) flag is specified in PBA-M message, the mobility options field includes "multicast channel information", which is the same information of MLDv2 Report message [4] as described in Section 9.1.

10. IANA Considerations

This document creates a new registry for the flags in the Binding Update message called the "Binding Update Flags".

The following flags are reserved:

- (A) 0x8000 [RFC3775]
- (H) 0x4000 [RFC3775]
- (L) 0x2000 [RFC3775]
- (K) 0x1000 [RFC3775]
- (M) 0x0800 [RFC4140]
- (R) 0x0400 [RFC3963]
- (P) 0x0200 [RFC5213]

This document reserves a new flag (C) for "Proxy Binding Update with Multicast Extension" as described in Section 9.1 as follows:

- (C) 0x0100

The rest of the values in the 16-bit field are reserved. New values can be assigned by Standards Action or IESG approval.

This document also creates a new registry for the flags in the Binding Acknowledgment message called the "Binding Acknowledgment Flags".

The following flags are reserved:

- (K) 0x80 [RFC3775]
- (R) 0x40 [RFC3963]
- (P) 0x20 [RFC5213]

This document reserves a new flag (C) for "Proxy Binding Acknowledgement with Multicast Extension" as described in Section 9.2 as follows:

- (C) 0x010

The rest of the values in the 8-bit field are reserved. New values

can be assigned by Standards Action or IESG approval.

The IANA should also allocate the value of the type field of "multicast channel information" described in Section 9.1 for the Mobility options field upon publication of the first RFC.

11. Security Considerations

TBD.

12. Acknowledgements

Many of the specifications described in this document are discussed and provided by the multimob mailing-list.

13. References

13.1. Normative References

- [1] Bradner, S., "Key words for use in RFCs to indicate requirement levels", RFC 2119, March 1997.
- [2] Gundavelli, S, Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [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] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.
- [5] 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.
- [6] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.
- [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] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.

13.2. Informative References

- [9] Schmidt, T., Waehlich, M., and S. Krishnan, "Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains", RFC 6224, April 2011.
- [10] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [11] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.
- [12] Soliman, H., Castelluccia, C., El Malki, K., and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)",

RFC 4140, August 2005.

- [13] Loughney, Ed., J., Nakhjiri, M., Perkins, C., and R. Koodli, "Context Transfer Protocol (CXTP)", RFC 4067, July 2005.
- [14] Yokota, H., Chowdhury, K., Koodli, R., Patil, B., and F. Xia, "Fast Handovers for Proxy Mobile IPv6", RFC 5949, September 2010.
- [15] Asaeda, H., Liu, H., and Q. Wu, "Tuning the Behavior of IGMP and MLD for Routers in Mobile and Wireless Networks", draft-ietf-multimob-igmp-mld-tuning-02.txt (work in progress), October 2011.
- [16] 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.

Authors' Addresses

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

Email: pierrick.seite@orange-ftgroup.com

Jinwei Xia
Huawei Technologies Co., Ltd.
Huihong Mansion, No.91 Baixia Rd.
Nanjing, Jiangsu 21001
China

Email: xiajinwei@huawei.com

MULTIMOB Working Group
INTERNET-DRAFT
Intended Status: Experimental
Expires: May 3, 2012

Luis M. Contreras
Telefonica I+D
Carlos J. Bernardos
Universidad Carlos III de Madrid
Ignacio Soto
Universidad Politecnica de Madrid
October 31, 2011

Rapid acquisition of the MN multicast subscription after handover
<draft-contreras-multimob-rams-03.txt>

Abstract

A new proposal is presented for speeding up the acquisition by the MAG of the MN's active multicast subscription information, in order to accelerate the multicast delivery to the MN after a handover. To do that, an extension to the current PMIPv6 protocol is proposed. The solution described in this memo is not only applicable to the base solution for multicast support in PMIPv6, but also it can be applied to other solutions envisioned as possible architectural evolutions of it. Furthermore, it is also independent of the role played by the MAG within the multicast network (either acting as MLD proxy or multicast router).

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) 2011 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	Conventions and Terminology	5
2	Overview	6
3	PMIPv6 extensions	7
3.1	New "Active Multicast Subscription" mobility option	7
3.1.1	Option application rules	7
3.1.2	Option format	7
3.2	New "multicast Signaling" flag on PBU/PBA message headers	8
3.2.1	Flag application rules	8
3.2.1.1	Registration process	8
3.2.1.2	De-registration process	9
3.2.2	New format of conventional PBU/PBA messages	9
3.2.2.1	Proxy Binding Update Message	9
3.2.2.2	Proxy Binding Acknowledgement Message	10
3.3.1	Flag application rules	10
3.4	New messages for active multicast subscription interrogation	11
3.4.1	Subscription Query message	11
3.4.1.1	Message application rules	11
3.4.1.2	Message format	11
3.4.2	Subscription Response message	12
3.4.2.1	Message application rules	12
3.4.2.2	Message format	13
3.5	New messages for active multicast subscription indication	14
3.5.1	Multicast Activity Indication message	14
3.5.1.1	Message application rules	14
3.5.1.2	Message format	14
3.5.2	Multicast Activity Indication Acknowledge message	15
3.5.2.1	Message application rules	15
3.5.2.2	Message format	15
3.6	New "PBA timer" in the LMA	16
4	Signaling process description	17

4.1	Handover of proactive type	17
4.1.1	Rationale	17
4.1.2	Message flow description	17
4.2	Handover of reactive type	19
4.2.1	Rationale	19
4.2.2	Message flow description	20
4.2.3	Further considerations for the reactive handover signaling	25
5	Co-existence with PMIPv6 multicast architectural evolutions . .	29
6	Benefits of layer-2 triggers for fast handover	29
7	Security Considerations	30
8	IANA Considerations	30
9	References	30
9.1	Normative References	30
9.2	Informative References	30
10	Acknowledgments	31
	Author's Addresses	31

1 Introduction

Recently, a base solution has been adopted for continuous multicast service delivery in PMIPv6 domains [4]. This solution specifies the basic functionality needed in the PMIPv6 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 MN. Thus, once the MN attaches to a new MAG, the MN is interrogated by the MAG through an MLD General Query, which is sent just after any new link is set up, to get knowledge of any existing subscription, as specified in [2].

However, as highlighted by [5], the base solution must be improved to cover some performance requirements, especially those referred to the user perceived service quality, seriously affected by the disruption of multicast content forwarding to the MN during handovers.

One MN with an active multicast subscription, moving from one point-of attachment to another within a PMIPv6 domain, will experience a certain delay in receiving again the multicast content that it was previously receiving at the previous location. Such delay will cause a gap on the content reception. Two measures can help to mitigate such reception gap. One of them is to buffer at the previous MAG the traffic with destination the MN and forwarding it at the new MAG, in order to properly deliver that traffic to the MN. The other possible measure is to reduce the time needed by the new MAG to get knowledge of the active multicast subscription maintained by the MN, in order to subscribe to the multicast group on behalf of the MN as soon as possible.

While the first measure can be accomplished by using [7] or some evolution of it (despite being only applicable in the case the underlying radio access technology supports layer-2 triggers), there is no a generic standard solution for the rapid acquisition of the on-going multicast subscription of the MN.

The method used in the base solution to get knowledge of an existing multicast subscription relies on the behaviour of the IGMP/MLD protocols. Both protocols send multicast membership interrogation messages when a new link is up. The answer to that request will report any existing multicast subscription by the MN.

Due to this behavior, despite of being a straightforward method, the MAG can incur in a huge delay in receiving the corresponding MLD Report message caused by either the MLD query processing time or the radio transfer delays associated with this procedure.

The new approach proposed here consists on extending the PMIPv6

signaling protocol defined in [1] by including a new multicast information option to update PMIPv6 entities during registration and de-registration processes, and new messages to trigger the transfer of such multicast information. No extension is required for any of the multicast-related protocols (IGMP/MLD or PIM protocols).

This proposal intends to provide a signaling method internal to the network to speed up the subscription information acquisition by the MAG, in order to accelerate the multicast delivery to the MN. By doing so, the knowledge by the MAG of the currently active multicast subscription becomes independent of the underlying radio technology dynamics and relaxes the requirement of a rapid response from the MN in processing MLD control messages. Issues like radio framing, radio access contention, channel reliability, IGMP/MLD timers optimisation for wireless environments, etc, are not relevant any more to determine multicast performance after handovers.

The solution described in this memo is not only applicable to the base solution defined in [4], but also it can be applied to other solutions envisioned as possible architectural evolutions of it, as those stated in [6]. Furthermore, it is also independent of the role played by the MAG within the multicast network (either acting as MLD proxy or multicast router).

1.1 Conventions and Terminology

This document uses the terminology referring to PMIPv6 components as defined in [1]. 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 LMA receives the MN de-registration from the pMAG previously to receive the MN registration from the nMAG.

2 Overview

The LMA is a key element within the PMIPv6 infrastructure. It traces the MN reachability along the PMIPv6 domain, therefore the LMA is the best element to store and forward the multicast subscription information to the rest of entities within the PMIPv6, that is, to the MAGs, as the MN moves.

The LMA only requires to know the detailed subscription information (in terms of the IP addresses of both the multicast group subscribed, G, and the source delivering it, S) during the handover event. Apart from the handover event, it is not worthy to continuously inform the LMA about it. Such procedure would significantly increase the signaling load within the PMIPv6 domain without a clear benefit. The subscription information (S,G) is only critical during handover, 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.

To do that, it will be necessary to extend the PMIPv6 protocol in several ways. First of all, a new mobility option is needed to pack the IP addresses of the current multicast subscription. Furthermore, additional messages are required 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.

Unicast IP address of the node which injects the multicast content in the network.

Multicast Group IP address

Multicast IP address identifying the content which the MN subscribes to.

3.2 New "multicast Signaling" flag on PBU/PBA message headers

3.2.1 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 subject of 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.

3.2.1.1 Registration process

These rules 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 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, without any further meaning.

* If S=1 in the corresponding PBU message, two sub-cases can happen

- o S=1 in the PBA message if the multicast subscription information is provided in this message for the MN. When S=1, if the MN maintains an active multicast session, the PBA

message will include the "Active Multicast Subscription" mobility option with the IP addresses of the subscribed group and the source providing it.

o S=0 in the PBA message if the multicast subscription information is not provided in this message for the MN. The PBA message will include the "Active Multicast Subscription" mobility option with the IP addresses of the group and the source set to 0. This case is useful to decouple unicast and multicast signaling for a MN being registered at nMAG. A way for obtaining later active multicast-subscription information is described later in this document.

3.2.1.2 De-registration process

These rules apply for the Binding De-registration process

o PBU message

* S=0, it indicates that the MN has no active multicast session.

* S=1, it indicates that the MN has an active multicast session, and the IP addresses of the subscribed group and the source providing it are transported in the "Active Multicast Subscription" mobility option.

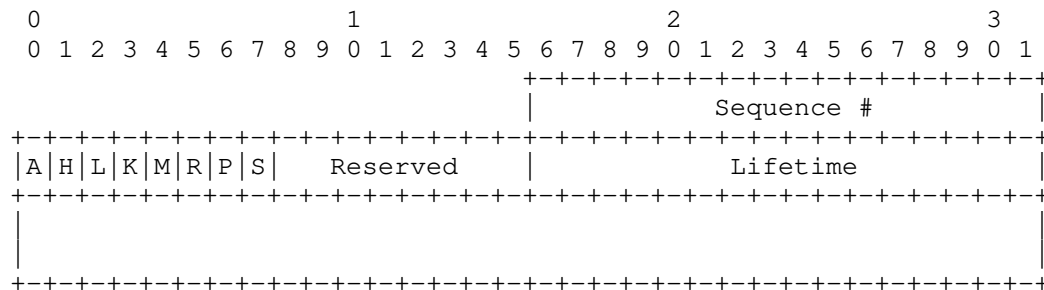
o PBA message

The value of the flag in the PBA message should be a copy of the value received in the PBU message, without any further meaning.

3.2.2 New format of conventional PBU/PBA messages

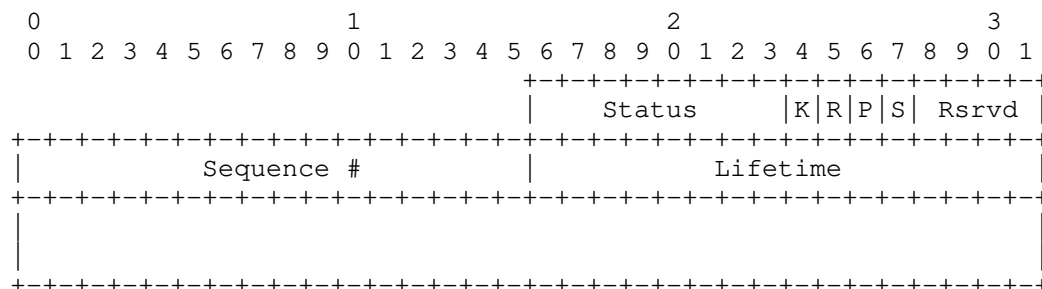
3.2.2.1 Proxy Binding Update Message

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



3.2.2.2 Proxy Binding Acknowledgement Message

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



3.3 New "multicast Active" flag on LMA Binding Cache (and optionally on the MN's policy store)

3.3.1 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 interrogation 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 interrogate or not the pMAG (after receiving a PBU message from the nMAG) is as follows:

- 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 interrogate the pMAG, and registers the MN as attached to the nMAG as usual.
- 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 that multicast signaling is not supported by the nMAG for that MN, the LMA does not interrogate the pMAG, and registers the MN as attached to the nMAG as usual.
- 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 interrogate the pMAG, and registers the MN as attached to the nMAG as usual.

- 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 interrogates the pMAG to obtain the multicast subscription details in the form of (S,G) 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.

3.4 New messages for active multicast subscription interrogation

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 [3].

3.4.1 Subscription Query message

3.4.1.1 Message application rules

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

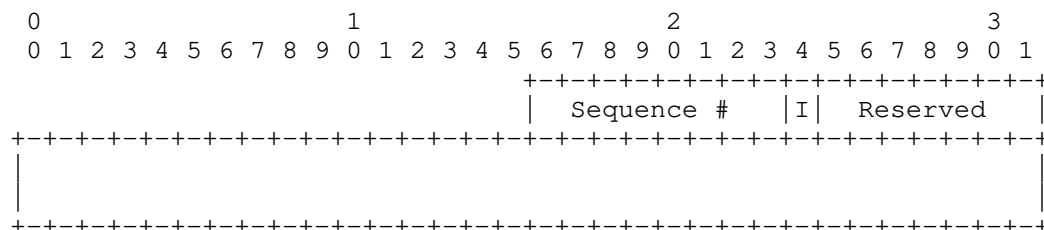
Additionally, this message is sent by the nMAG towards the LMA to interrogate it about the existing multicast subscription of the MN when the LMA acknowledges the PBU sent by the nMAG but the multicast information is not provided (in detail, when the PBU messages has set the flag S to 1, and the PBA message has set the flag S to 0).

3.4.1.2 Message format

The Subscription Query message has the following format.

3.4.2.2 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)

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.

3.5.2 Multicast Activity Indication Acknowledge message

3.5.2.1 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.

3.5.2.2 Message format

The Multicast Activity Indication message has the following format.

4 Signaling process description

As the MN moves from one access gateway (named previous-MAG, pMAG) to another (named new-MAG, nMAG), 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 should 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.

4.1 Handover of proactive type

4.1.1 Rationale

In the proactive case, the LMA receives the MN de-registration from the pMAG previously to receive the MN registration from the nMAG.

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 IP addresses of the multicast subscription(s) active in 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 addresses of the group(s) subscribed by the MN, and the source(s) delivering it(them), 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.

4.1.2 Message flow description

The figure 1 summarizes this process.

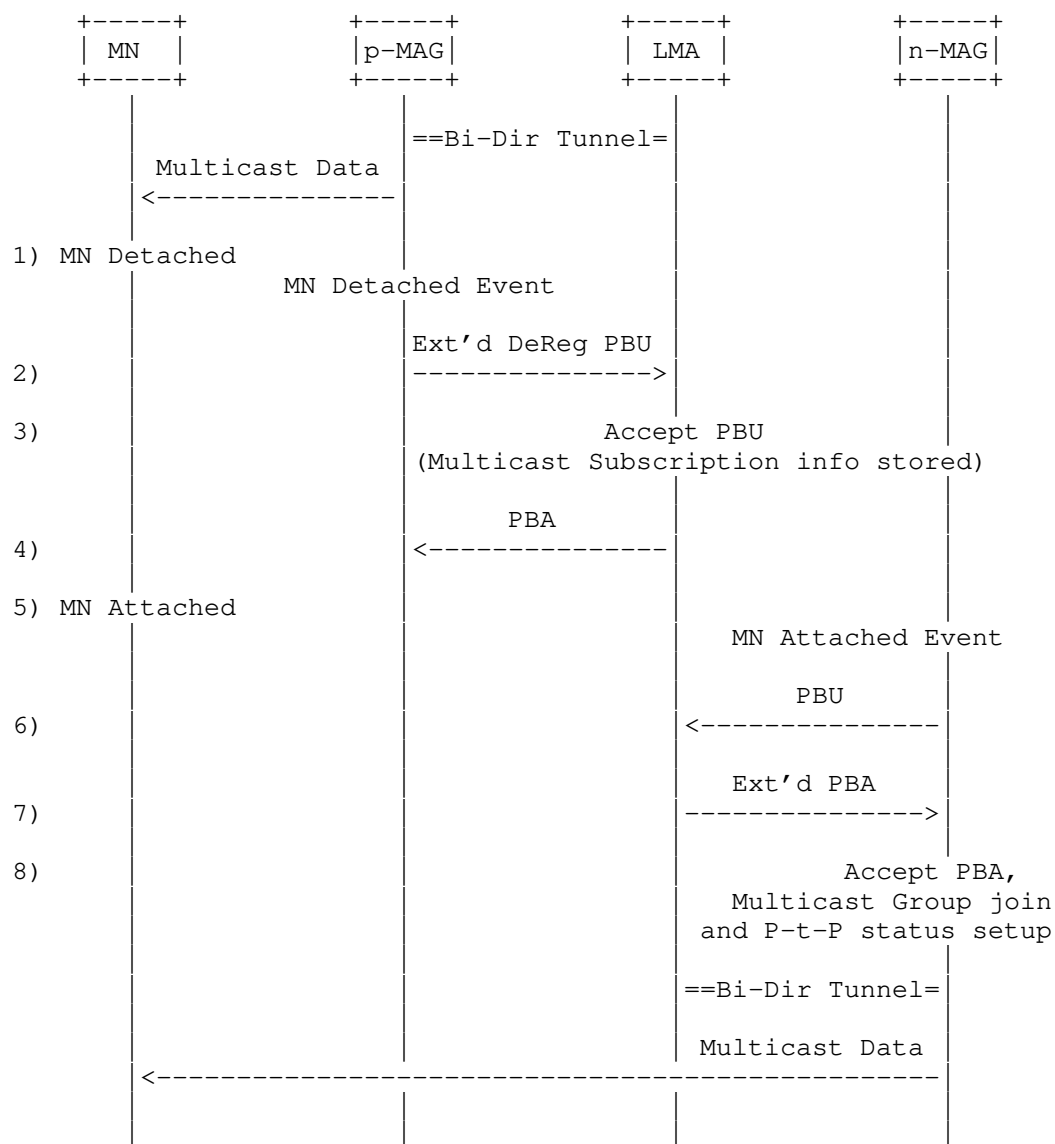


Figure 1. Proactive handover

The sequence of messages is the following:

- 1) A registered MN is receiving a multicast content which has been previously subscribed by sending an 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 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 IP addresses of the (S,G) pairs 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 when the handover has been 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 [1].

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 IP addresses of the (S,G) pairs of the active multicast subscriptions in the moment of handover.

8) The nMAG processes the PBA message, following all the standard procedures described in [1]. 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 present MN attached to it. From that instant, the multicast content is served to the MN.

4.2 Handover of reactive type

4.2.1 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.

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.

4.2.2 Message flow description

The set of figures 2a to 2d summarize this process.

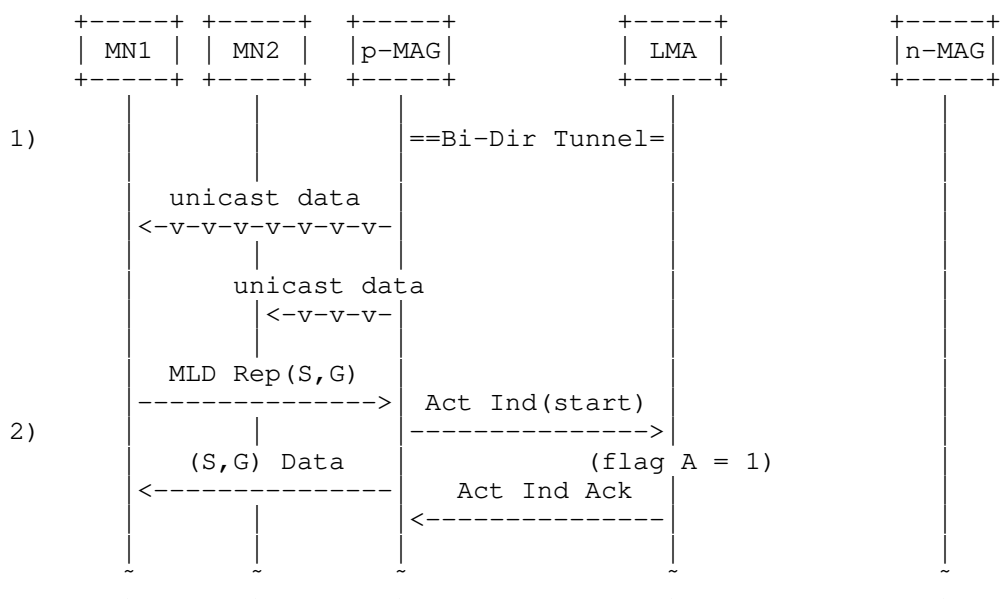


Figure 2a. Reactive handover (steps 1 to 2)

The sequence of messages is the following:

1) A pair of MNs, named MN1 and MN2, are attached to the pMAG. Both MNs are multicast-enabled nodes, and both MNs are only receiving unicast traffic as usual in PMIPv6 domains, with no multicast subscription yet. At some point in time, the MN1 request to the pMAG

to be subscribed to the content identified by the IP addresses (S,G), by sending an standard MLD report from the MN to the pMAG. The pMAG will keep the multicast status state of the point-to-point link with the MN. The multicast flow (S,G) is then forwarded by the pMAG to the MN1.

2) Due to this initial multicast subscription for the MN1, the pMAG 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 pMAG to acknowledge the previous indication.

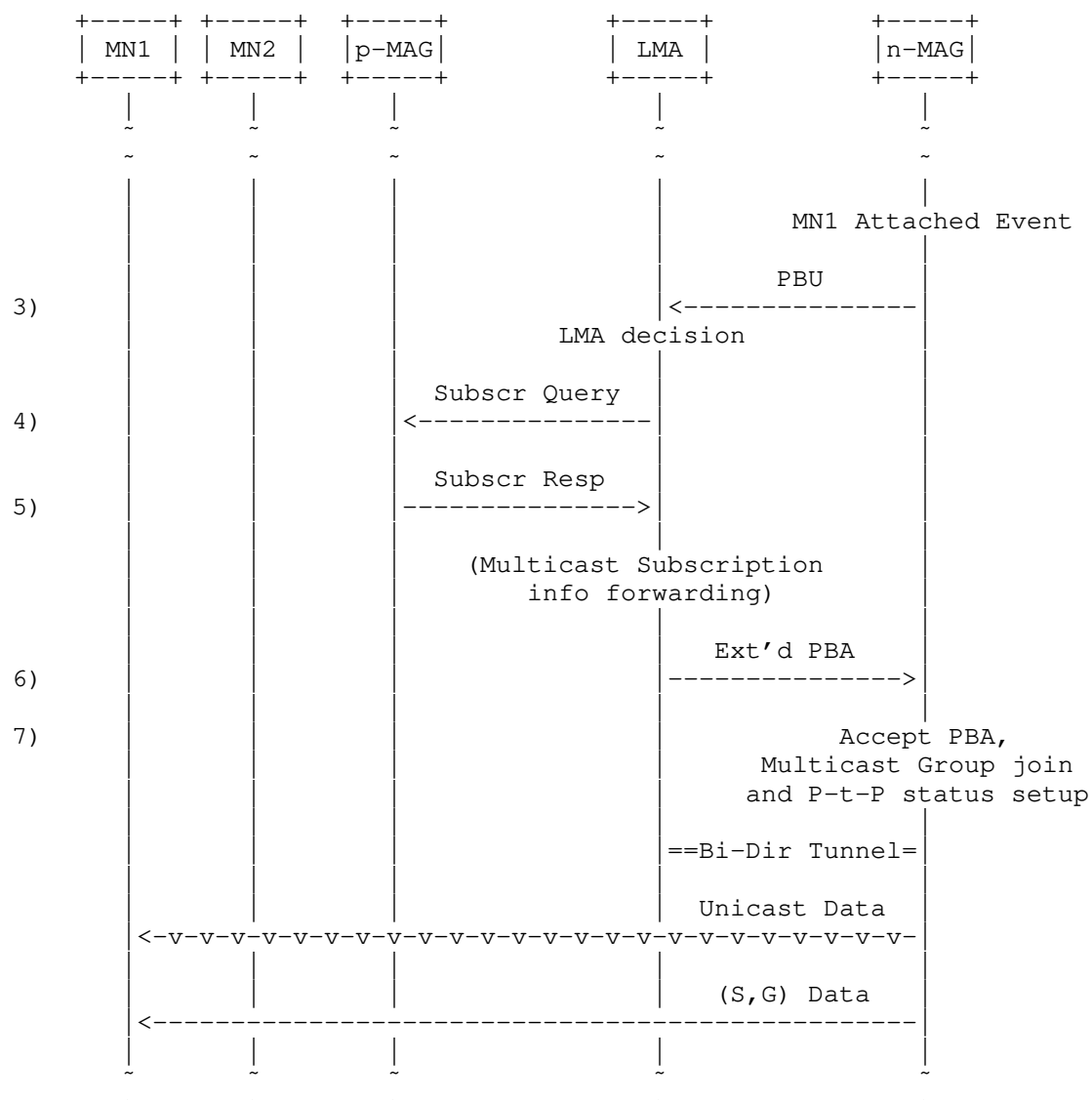


Figure 2b. Reactive handover (steps 3 to 7)

3) Some time later, 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.

4) 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 interrogates the pMAG about if there is any active multicast subscription for the MN1, by sending a Subscription Query message.

5) The pMAG answers the LMA with a Subscription Response message including the IP addresses of the existing subscriptions (the pair (S,G) in this case).

6) After processing the pMAG answer, the LMA acknowledges the PBU message, including the multicast subscription information within the new TLV-encoded option "Active Multicast Subscription". The nMAG then process the extended PBA message.

7) 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.

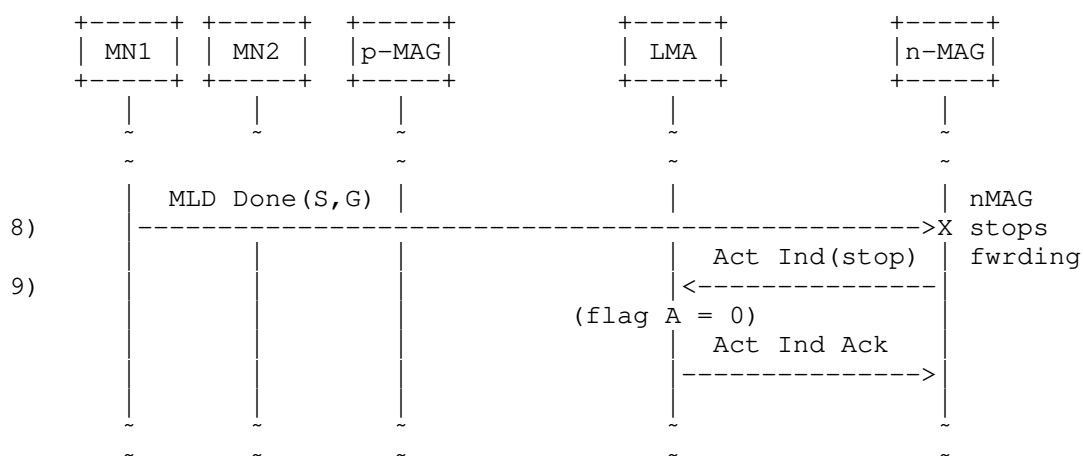


Figure 2c. Reactive handover (steps 8 to 9)

8) Some time later, the MN1 decides to totally stop all the active multicast subscriptions that it maintains. The MN1 will send an MLD Done message to nMAG to request the cease of the multicast traffic delivery. As consequence, the nMAG will stop all the multicast

traffic forwarding to the MN1.

9) After removing the active subscriptions for the MN1, the nMAG 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 nMAG to acknowledge the previous indication.

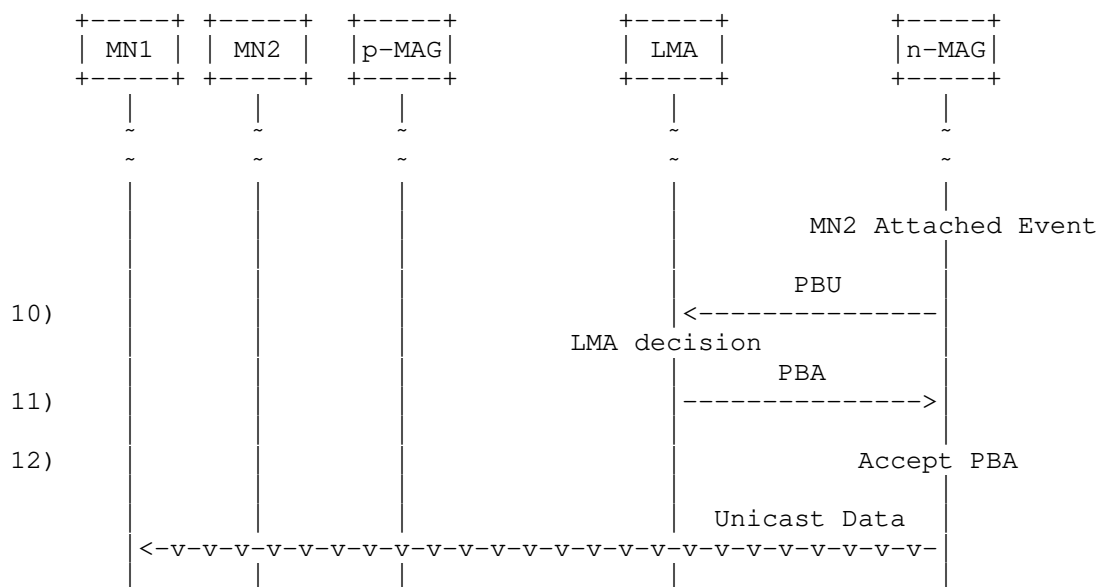


Figure 2d. Reactive handover(steps 10 to 12)

10) 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 neither 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.

11) 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 interrogate the pMAG, and acknowledges the PBU message. The nMAG then process the extended PBA message.

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

4.2.3 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.

4.2.4 Prevention of large delays of the binding acknowledgement for unicast traffic

Attending to the message sequences detailed above for reactive handovers, in case the LMA has to request the multicast subscription information to 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 to the LMA towards the MN, a mechanism should be implemented to decouple multicast from unicast traffic reception by the MN.

The figures 3a and 3b show this mechanism:

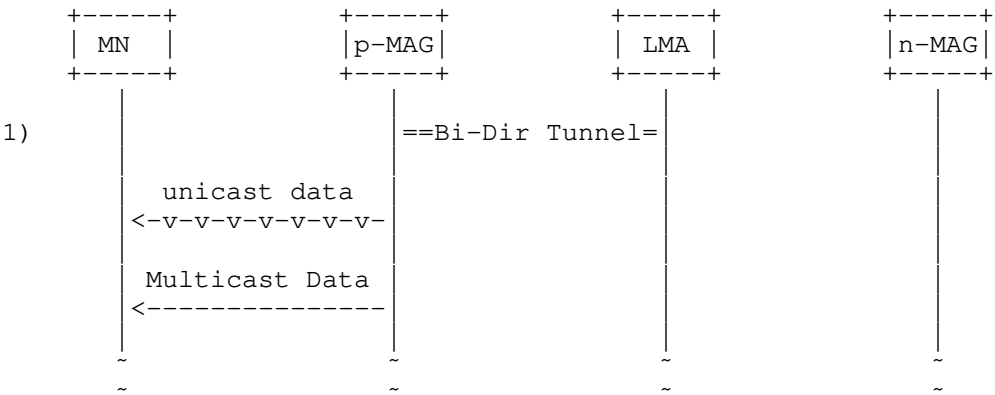


Figure 3a. Decoupling of unicast and multicast signaling (step 1)

The sequence of messages is the following:

- 1) An MN, named MN1, is attached to the pMAG. The MN is a multicast-enabled node, and it is receiving both unicast and multicast traffic simultaneously.

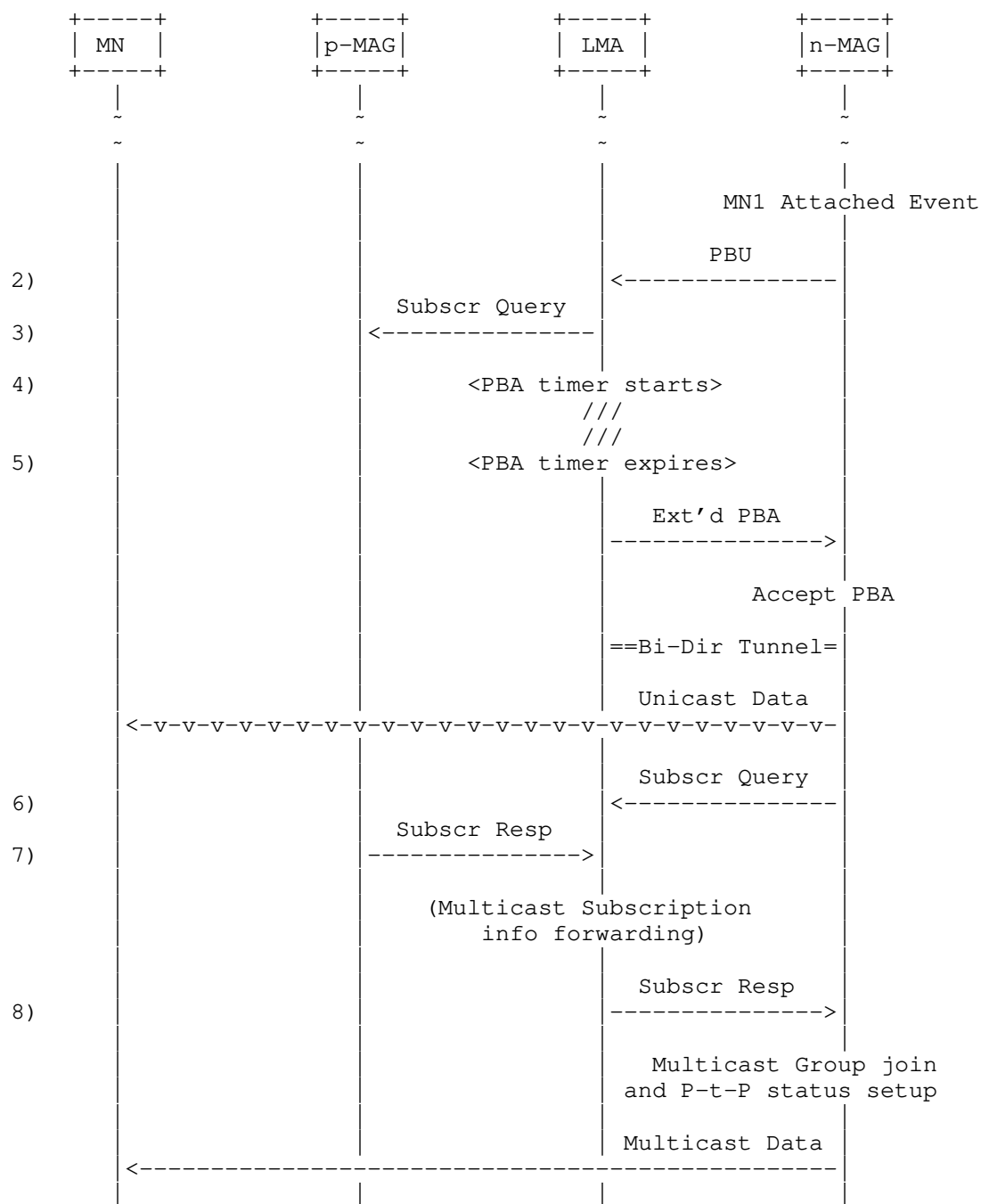


Figure 3b. Decoupling of unicast and multicast signaling (steps 2 to 8)

- 2) Some time later, the MN1 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 interrogate the pMAG about if there is any active multicast subscription for the MN1, 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 duration 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=0. 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 by another MN connection).
- 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 IP addresses of the existing subscriptions (the pair (S,G) in this case).
- 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 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 also be served to the MN.

5 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 [4]. However, the solution described in this memo is not only applicable to the base solution, but also it can be applied to other solutions envisioned as possible architectural evolutions to solve the tunnel convergence problem affecting the base solution, as those stated in [6].

The Multicast Tree Mobility Anchor (MTMA) solution in [6] 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.

In case of 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 IP addresses of the source and the content), 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 memo.

6 Benefits of layer-2 triggers for fast handover

As stated before, the global performance of the multicast handover can be improved in the case that layer-2 triggers are supported by the underlying radio technology. In [7], a procedure which allows to buffer at the pMAG and forward to the nMAG the traffic with destination the MN during the handover duration is defined. This forwarding can be beneficial for either strict real-time services or for networks with long handover duration. By forwarding the traffic to the MN, the disruption of the multicast traffic reception is minimized.

The solution in [7] avoids packet loss during the handover. Even so, the proposal in this memo is still useful, because reducing the time required to set up multicast traffic delivery in the nMAG minimizes the buffering needed at the pMAG.

In any case, because the feature in [7] is dependent on the capabilities of the underlying radio technology, and that not all the multicast applications could take benefit of it, that functionality can be seen as optional for multicast handover optimization.

7 Security Considerations

TBD.

8 IANA Considerations

This document defines the new following elements which values should be allocated:

- 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.
- o Flags: the multicast Signaling (S), the multicast Information (I), and the multicast Active (A) flags.

9 References

9.1 Normative References

- [1] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [2] S. Deering, W. Fenner, B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.
- [3] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

9.2 Informative References

- [4] T.C. Schmidt, M. Waehlis, and S. Krishnan, "A Minimal Deployment Option for Multicast Listeners in PMIPv6 Domains", RFC6224, April 2011.
- [5] D. von Hugo, H. Asaeda, B. Sarikaya, 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.
- [6] J.C. Zuniga, L.M. Contreras, C.J. Bernardos, S. Jeon, and Y. Kim, "Mobile Multicast Routing Optimizations", draft-zuniga-

multimob-pmipv6-ropt-01, (work in progress), October 2011.

- [7] H. Yokota, Chowdhury, K., Koodli, R., Patil, B., and F. Xia, "Fast Handovers for Proxy Mobile IPv6", RFC 5949, September 2010

10 Acknowledgments

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 also has received funding from the Spanish MICINN through the I-MOVING project (TEC2010-18907).

Author's Addresses

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

Carlos J. Bernardos
Universidad Carlos III de Madrid
Email: cjb@it.uc3m.es

Ignacio Soto
Universidad Politecnica de Madrid
Email: isoto@dit.upm.es

MULTIMOB Working Group
Internet-Draft
Expires: January 12, 2012

H. Asaeda
Keio University
H. Liu
Q. Wu
Huawei Technologies
July 11, 2011

Tuning the Behavior of IGMP and MLD for Routers in Mobile and Wireless
Networks
draft-ietf-multimob-igmp-ml-d-tuning-01

Abstract

IGMP and MLD are the protocols used by hosts and multicast routers to exchange their IP multicast group memberships with each other. This document describes the ways of IGMPv3 and MLDv2 protocol optimization for mobility, and aims to become a guideline for query and other timers and values tuning.

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 12, 2012.

Copyright Notice

Copyright (c) 2011 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. Terminology	4
3. Explicit Tracking of Membership Status	5
4. Tuning IGMP/MLD Timers and Values	6
4.1. Tuning IGMP/MLD General Query Interval	6
4.2. Tuning IGMP/MLD Query Response Interval	7
4.3. Tuning Last Member Query Timer (LMQT) and Last Listener Query Timer (LLQT)	7
4.4. Tuning Startup Query Interval	8
4.5. Tuning Robustness Variable	8
4.6. Tuning Scenarios for Various Mobile IP Networks	9
5. Destination Address of Specific Query	11
6. Interoperability	12
7. Security Considerations	13
8. Acknowledgements	14
9. References	15
9.1. Normative References	15
9.2. Informative References	15
Appendix A. Unicasting General Query	17
Authors' Addresses	18

1. Introduction

The Internet Group Management Protocol (IGMP) [2] for IPv4 and the Multicast Listener Discovery Protocol (MLD) [3] for IPv6 are the standard protocols for hosts to initiate joining or leaving multicast sessions. These protocols must be also supported by multicast routers or IGMP/MLD proxies [10] that maintain multicast membership information on their downstream interfaces. Conceptually, IGMP and MLD work on both wireless and mobile networks. However, wireless access technologies operate on a shared medium or a point-to-point link with limited frequency and bandwidth. In many wireless regimes, it is desirable to minimize multicast-related signaling to preserve the limited resources of battery powered mobile devices and the constrained transmission capacities of the networks. A mobile host may cause disruption of a multicast service initiation and termination in the new or previous network upon its movement. Slow multicast service activation following a join may incur additional delay in receiving multicast packets and degrade reception quality. Slow service termination triggered by IGMP/MLD querying or by a rapid departure of the mobile host without leaving the group in the previous network may waste network resources.

When IGMP and MLD are used with mobile IP protocols, the proximity of network entities should be considered. For example, when bi-directional tunnel is used with the mobility entities described in [14][11] in place, the mobile host experiences additional latency, because the round-trip time using bi-directional tunnel between mobility entities is larger comparing to the case that a host and an upstream router attach to a LAN.

To create the optimal multicast membership management condition, IGMP and MLD protocols could be tuned to "ease a mobile host's processing cost or battery power consumption by IGMP/MLD Query transmission timing coordination by routers" and "realize fast state convergence by successive monitoring whether downstream members exist or not".

This document describes the ways of tuning the IGMPv3 and MLDv2 protocol behavior on the router side for wireless and mobile networks, including query and other timers tuning. The selective optimization that provides tangible benefits to the mobile hosts and routers is given by keeping track of downstream hosts' membership status and varying IGMP/MLD Query types and values to tune the number of responses. The proposed behavior interoperates with the IGMPv3 and MLDv2 protocols.

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 [1].

3. Explicit Tracking of Membership Status

Mobile hosts use IGMP and MLD to request to join or leave multicast sessions. When an adjacent upstream router receives the IGMP/MLD Report messages, it recognizes the membership status on the link. To update the membership status reliably, the router sends IGMP/MLD Query messages periodically, and sends Group-Specific and/or Group-and-Source Specific Queries when a member host reports its leave. Then the other member hosts reply IGMP/MLD Report messages to notify their memberships. IGMP/MLD Query is therefore necessary to obtain the up-to-date membership information, but a large number of the reply messages sent from all member hosts may cause network congestion or consume network bandwidth consumption.

The "explicit tracking function" [9] is the possible approach to reduce the transmitted number of IGMP/MLD messages and contribute to the efficiency of mobile communications. It enables the router to keep track of the membership status of the downstream IGMPv3 or MLDv2 member hosts. That is, if a router enables the explicit tracking function, it does not always need to ask Current-State Report message transmission from the receiver hosts since the router implicitly recognizes the (potential) last member host when it receives the State-Change Report. The router can therefore send IGMP/MLD Group-Specific and Group-and-Source Specific Queries LMQC/LLQC times (see Section 4.3 for LMQC/LLQC) only when it recognizes the last member has left from the network. This reduces the transmitted number of Current-State Report messages.

Enabling the explicit tracking function is advantageous for mobile multicast, but the function requires additional processing capability and a possibly large memory for routers to keep all membership status. Especially when a router needs to maintain a large number of receiver hosts, this resource requirement is potentially impacted. Therefore, in this document, we propose that adjacent upstream multicast routers SHOULD enable the explicit tracking function for IP multicast communications on wireless networks, if they have enough resources. If operators think that their routers do not have enough resources, they MAY decide to disable this function on their routers. Note that whether routers enable the explicit tracking function or not, they need to maintain downstream membership status by sending IGMPv3/MLDv2 General Query messages as some IGMPv3/MLDv2 messages may be lost during transmission.

4. Tuning IGMP/MLD Timers and Values

4.1. Tuning IGMP/MLD General Query Interval

IGMP and MLD are non-reliable protocols; to cover the possibility of a State-Change Report being missed by one or more multicast routers, "hosts retransmit the same State-Change Report messages [Robustness Variable] - 1 more times", at intervals chosen at random from the range (0, [Unsolicited Report Interval]) [2][3]. Although this behavior increases the protocol robustness, it does not guarantee that the State-Change Report reaches the routers. Therefore, routers still need to refresh the downstream membership information by receiving Current-State Report periodically solicited by IGMP/MLD General Query sent in the [Query Interval] period, in order to enhance robustness of the host in case of link failures and packet loss. It also supports the situation that mobile hosts turn off or move from a network to other network managed by a different router without any notification (e.g., leave request).

The [Query Interval] is the interval between General Queries sent by the regular IGMPv3/MLDv2 querier, and the default value is 125 seconds [2][3]. By varying the [Query Interval], multicast routers can tune the number of IGMP/MLD messages on the network; larger values cause IGMP/MLD Queries to be sent less often.

This document proposes 150 seconds for the [Query Interval] value by changing the Querier's Query Interval Code (QQIC) field specified in the IGMP/MLD Query message, for the case that a router enabling the explicit tracking function sends General Query and potentially operates a large number of member hosts such as more than 200 hosts on the wireless link. This longer interval value contributes to minimizing traffic of Report messages and battery power consumption for mobile hosts.

On the other hand, this document also proposes 60 to 90 seconds for the [Query Interval] value for the case that a router enabling the explicit tracking function attaches to a wireless link having higher capacity of the resource. This shorter interval contributes to quick synchronization of the membership information tracked by the router but may consume battery power of mobile hosts.

If a router does not enable the explicit tracking function, the [Query Interval] value would be its default value, 125 seconds.

In situations where Mobile IPv6 [14] is used, when the home agent implements multicast router functionality and multicast data packets are tunneled to and from the home agent, the home agent may want to slow down Query periodicity, especially when network congestion is

detected. This can be done by the home agent starting forwarding queries with the default [Query Interval] value and increasing it in a gradual manner until it exceeds the mobile host's lifetime.

4.2. Tuning IGMP/MLD Query Response Interval

The [Query Response Interval] is the Max Response Time (or Max Response Delay) used to calculate the Max Resp Code inserted into the periodic General Queries. Its default value is 10 seconds expressed by "Max Resp Code=100" for IGMPv3 [2] and "Maximum Response Code=10000" for MLDv2 [3]. By varying the [Query Response Interval], multicast routers can tune the burstiness of IGMP/MLD messages on the network; larger values make the traffic less bursty as host responses are spread out over a larger interval, but will increase join latency when State-Change Report is missing.

According to our experimental analysis, this document proposes two tuning scenarios for tuning the [Query Response Interval] value in different wireless link conditions; one scenario is for a wireless link with a lower capacity of network resource or a lossy link, and the other scenario is for a wireless link with enough capacity or reliable condition for IGMP/MLD message transmission.

Regarding the first scenario, for instance, when a multicast router attaches to a bursty IEEE 802.11b link, the router configures the longer [Query Response Interval] value, such as 10 to 20 (sec). This configuration will reduce congestion of the Current-State Report messages on a link but may increase join latency and leave latency when the unsolicited messages (State-Change Record) are lost on the router.

The second scenario may happen for a multicast router attaching to a wireless link having higher capacity of the resource or a point-to-(multi-)point link such as an IEEE 802.16e link, because IGMP/MLD messages do not seriously affect the link condition. The router can seek Current-State Report messages with the shorter [Query Response Interval] value, such as 5 to 10 (sec). This configuration will contribute to quickly (at some level) discovering non-tracked member hosts and synchronizing the membership information.

4.3. Tuning Last Member Query Timer (LMQT) and Last Listener Query Timer (LLQT)

Shortening the Last Member Query Timer (LMQT) for IGMPv3 and the Last Listener Query Timer (LLQT) for MLDv2 contributes to minimizing leave latency. LMQT is represented by the Last Member Query Interval (LMQI), multiplied by the Last Member Query Count (LMQC), and LLQT is represented by the Last Listener Query Interval (LLQI), multiplied by

the Last Listener Query Count (LLQC).

While LMQUI and LLQI are changeable, it is reasonable to use the default values (i.e., 1 second) for LMQUI and LLQI in a wireless network. LMQC and LLQC, whose default value is the [Robustness Variable] value, are also tunable. Therefore, LMQC and LLQC MAY be set to "1" for routers enabling the explicit tracking function, and then LMQT and LLQT are set to 1 second. However, setting LMQC and LLQC to 1 increases the risk of missing the last member; LMQC and LLQC SHOULD be set to 1 only when network operators think that their wireless link is stable enough.

On the other hand, if network operators think that their wireless link is lossy (e.g., due to a large number of attached hosts or limited resources), they MAY set LMQC and LLQC to "2" for their routers enabling the explicit tracking function. Although bigger LMQC and LLQC values may cause longer leave latency, the risk of missing the last member will be reduced.

4.4. Tuning Startup Query Interval

The [Startup Query Interval] is the interval between General Queries sent by a Querier on startup. The default value is 1/4 of [Query Interval]; however, this document recommends the use of its shortened value such as 1 second since the shorter value would contribute to shortening handover delay for mobile hosts in, e.g., the base solution with PMIPv6 [12]. Note that the [Startup Query Interval] is a static value and cannot be changed by any external signal. Therefore operators who maintain routers and wireless links must properly configure this value.

4.5. Tuning Robustness Variable

To cover the possibility of unsolicited reports being missed by multicast routers, unsolicited reports are retransmitted [Robustness Variable] - 1 more times, at intervals chosen at random from the defined range [2][3]. The QRV (Querier's Robustness Variable) field in IGMP/MLD Query contains the [Robustness Variable] value used by the querier. The default [Robustness Variable] value defined in IGMPv3 [2] and MLDv2 [3] is "2".

This document proposes "2" for the [Robustness Variable] value for mobility, when a router attaches to a wireless link having lower capacity of the resource or a large number of hosts. For a router that attaches to a wireless link having higher capacity of the resource or reliable condition, it is not required to retransmit the same State-Change Report message; hence the router sets the [Robustness Variable] to "1". Note that whether the explicit

tracking function is enabled or not, the [Robustness Variable] value SHOULD NOT be bigger than "2".

4.6. Tuning Scenarios for Various Mobile IP Networks

In mobile IP networks, IGMP and MLD are used either with three deployment scenarios; (1) running directly between host and access router on a wireless network, (2) running between host and home router through a tunnel link, and (3) running between home router and foreign router through a tunnel link.

When a receiver host connects directly through a wireless link to a foreign access router or a home router, the tuning of the IGMP/MLD protocol parameters should be the same as suggested in the previous sections. The example of this scenario occurs when route optimization is adopted in MIPv6 [14] or Mobile IP [15], or when in Proxy Mobile IPv6 (PMIPv6) [11], the mobile access gateway, whose role is similar to the one of a foreign router, acts as a multicast router as proposed in [13].

The second scenario occurs when bi-directional tunnel established between host and home router is used to exchange IGMP/MLD messages such as [14][15]. There are difficulties in tuning the parameters in this situation, because the tunnel link condition is diverse and changeable. When a host is far away from the home router, the transmission delay between the two entities may be longer and the packet delivery may be more unreliable. Thus the effects of the IGMP/MLD message transmission through a tunnel link should be considered during the parameter setting. For example, the [Query Interval] and [Query Response Interval] could be set shorter to compensate the transmission delay, and the [Robustness Variable] could be increased for possible packet loss.

The third scenario occurs in [12], in which the mobile access gateway (i.e., foreign router) acts as the IGMP/MLD Proxy [10] in PMIPv6 [11]. Through the bi-directional tunnel established with the local mobility anchor (i.e., home router), the mobile access gateway sends summary reports of its downstream member hosts to the local mobility anchor. Apart from the distance factor that influences the parameter setting, the [Query Response Interval] on the local mobility anchor could be set to the smaller value since the number of foreign router is much smaller compared to the that of the host and the chances of packet burst is low for the same reason.

Ideally, the IGMP/MLD querier router adjusts its parameter setting according to the actual mobile IP network conditions to benefit service performance and resource utilization. It would be desirable that a home router determines aforementioned timers and values

according to the delay between the initiating IGMP/MLD Query and the responding IGMP/MLD Report, while describing such mechanism dynamically adjusting these timers and values is out of scope of this document.

5. Destination Address of Specific Query

IGMP/MLD Group-Specific and Group-and-Source Specific Queries defined in [2][3] are sent to verify whether there are hosts that desire reception of the specified group or a set of sources or to rebuild the desired reception state for a particular group or a set of sources. These specific Queries build and refresh multicast membership state of hosts on an attached network. These specific Queries should be sent to all desired hosts with specific multicast address (not the all-hosts/all-nodes multicast address) as their IP destination addresses, because hosts that do not join the multicast session do not pay attention to these specific Queries, and only active member hosts that have been receiving multicast contents with the specified address reply IGMP/MLD reports.

6. Interoperability

IGMPv3 [2] and MLDv2 [3] provide the ability for hosts to report source-specific subscriptions. With IGMPv3/MLDv2, a mobile host can specify a channel of interest, using multicast group and source addresses in its join request. Upon its reception, the upstream router that supports IGMPv3/MLDv2 establishes the shortest path tree toward the source without coordinating a shared tree. This function is called the source filtering function and is required to support Source-Specific Multicast (SSM) [8].

Recently, the Lightweight-IGMPv3 (LW-IGMPv3) and Lightweight-MLDv2 (LW-MLDv2) [4] protocols have been defined as the proposed standard protocols in the IETF. These protocols provide protocol simplicity for mobile hosts and routers, as they eliminate a complex state machine from the full versions of IGMPv3 and MLDv2, and promote the opportunity to implement SSM in mobile communications.

This document assumes that both multicast routers and mobile hosts MUST be IGMPv3/MLDv2 capable, regardless whether the protocols are the full or lightweight version. And this document does not consider interoperability with older version protocols. The main reason not being interoperable with older IGMP/MLD protocols is that the explicit tracking function does not work properly with older IGMP/MLD protocols.

7. Security Considerations

This document neither provides new functions or modifies the standard functions defined in [2][3][4]. Therefore there is no additional security consideration provided.

8. Acknowledgements

Marshall Eubanks, Gorrry Fairhurst, Dirk von Hugo, Imed Romdhani, Behcet Sarikaya, Yogo Uchida, Stig Venaas, Jinwei Xia, and others provided many constructive and insightful comments.

9. References

9.1. Normative References

- [1] Bradner, S., "Key words for use in RFCs to indicate requirement levels", RFC 2119, March 1997.
- [2] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.
- [3] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.
- [4] 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.
- [5] Deering, S., "Host Extensions for IP Multicasting", RFC 1112, August 1989.
- [6] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, July 1997.
- [7] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.
- [8] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.
- [9] Asaeda, H. and Y. Uchida, "IGMP/MLD-Based Explicit Membership Tracking Function for Multicast Routers", draft-asaeda-mboned-explicit-tracking-02.txt (work in progress), March 2011.

9.2. Informative References

- [10] 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.
- [11] Gundavelli, S, Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [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 Multicast", draft-asaeda-multimob-pmip6-extension-06 (work in progress), July 2011.
- [14] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [15] Perkins, Ed., C., "IP Mobility Support for IPv4, Revised", RFC 5944, November 2010.

Appendix A. Unicasting General Query

IGMPv3 and MLDv2 specifications [2][3] describe that a host **MUST** accept and process any Query whose IP Destination Address field contains any of the addresses (unicast or multicast) assigned to the interface on which the Query arrives. In general, the all-hosts multicast address (224.0.0.1) or link-scope all-nodes multicast address (FF02::1) is used as the IP destination address of IGMP/MLD General Query. On the other hand, according to [2][3], a router **MAY** be able to unicast General Query to tracked member hosts in [Query Interval], if the router keeps track of membership information (Section 3).

Unicasting IGMP/MLD General Query would reduce the drain on battery power of mobile hosts as only the active hosts that have been receiving multicast contents respond the unicast IGMP/MLD General Query messages and non-active hosts do not need to pay attention to the IGMP/MLD messages. This also allows the upstream router to proceed fast leaves (or shorten leave latency) by setting LMQC/LLQC smaller, because the router can immediately converge and update the membership information, ideally.

However, there is a concern in unicast General Query. If a multicast router sends General Query "only" by unicast, it cannot discover potential member hosts whose join requests were lost. Since the hosts do not retransmit the same join requests (i.e., unsolicited Report messages), they lose the chance to join the channels unless the upstream router asks the membership information by sending General Query by multicast. It will be solved by using both unicast and multicast General Queries and configuring the [Query Interval] timer value for multicast General Query and the [Unicast Query Interval] timer value for unicast General Query. However, using two different timers for General Queries would require the protocol extension this document does not focus on. If a router does not distinguish the multicast and unicast General Query Intervals, the router should only use and enable multicast General Query.

Also, unicasting General Query does not remove multicasting General Query. Multicast General Query is necessary to update membership information if it is not correctly synchronized due to missing Reports. Therefore, enabling unicast General Query **SHOULD NOT** be used for the implementation that does not allow to configure different query interval timers as [Query Interval] and [Unicast Query Interval] (See Appendix A for the detail). If a router does not distinguish these multicast and unicast General Query Intervals, the router **SHOULD** only use and enable multicast General Query.

Authors' Addresses

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/>

Hui Liu
Huawei Technologies Co., Ltd.
Huawei Bld., No.3 Xinxu Rd.
Shang-Di Information Industry Base
Hai-Dian District, Beijing 100085
China

Email: helen.liu@huawei.com

Qin Wu
Huawei Technologies Co., Ltd.
Site B, Floor 12F, Huihong Mansion
No.91 Baixia Rd.
Nanjing, Jiangsu 21001
China

Email: bill.wu@huawei.com

MULTIMOB Working Group
Internet-Draft
Expires: May 3, 2012

H. Asaeda
Keio University
H. Liu
Q. Wu
Huawei Technologies
October 31, 2011

Tuning the Behavior of IGMP and MLD for Routers in Mobile and Wireless
Networks
draft-ietf-multimob-igmp-ml-d-tuning-02

Abstract

IGMP and MLD are the protocols used by hosts and multicast routers to exchange their IP multicast group memberships with each other. This document describes the ways of IGMPv3 and MLDv2 protocol optimization for mobility, and aims to become a guideline for query and other timers and values tuning.

Status of this Memo

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

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

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

This Internet-Draft will expire on May 3, 2012.

Copyright Notice

Copyright (c) 2011 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. Terminology	4
3. Explicit Tracking of Membership Status	5
4. Tuning IGMP/MLD Timers and Values	6
4.1. Tuning IGMP/MLD General Query Interval	6
4.2. Tuning IGMP/MLD Query Response Interval	7
4.3. Tuning Last Member Query Timer (LMQT) and Last Listener Query Timer (LLQT)	7
4.4. Tuning Startup Query Interval	8
4.5. Tuning Robustness Variable	8
4.6. Tuning Scenarios for Various Mobile IP Networks	9
5. Destination Address of Specific Query	11
6. Interoperability	12
7. Security Considerations	13
8. Acknowledgements	14
9. References	15
9.1. Normative References	15
9.2. Informative References	15
Appendix A. Unicasting General Query	17
Authors' Addresses	18

1. Introduction

The Internet Group Management Protocol (IGMP) [2] for IPv4 and the Multicast Listener Discovery Protocol (MLD) [3] for IPv6 are the standard protocols for hosts to initiate joining or leaving multicast sessions. These protocols must be also supported by multicast routers or IGMP/MLD proxies [10] that maintain multicast membership information on their downstream interfaces. Conceptually, IGMP and MLD work on both wireless and mobile networks. However, wireless access technologies operate on a shared medium or a point-to-point link with limited spectrum and bandwidth. In many wireless regimes, it is desirable to minimize multicast-related signaling to preserve the limited resources of battery powered mobile devices and the constrained transmission capacities of the networks. A mobile host may cause disruption of a multicast service initiation and termination in the new or previous network upon its movement. Slow multicast service activation following a join may incur additional delay in receiving multicast packets and degrade reception quality. Slow service termination triggered by IGMP/MLD querying or by a rapid departure of the mobile host without leaving the group in the previous network may waste network resources.

When IGMP and MLD are used with mobile IP protocols, the proximity of network entities should be considered. For example, when bi-directional tunnel is used with the mobility entities described in [11][14] in place, the mobile host experiences additional latency, because the round-trip time using bi-directional tunnel between mobility entities is larger comparing to the case that a host and an upstream router attach to a LAN.

This document describes the ways of tuning the IGMPv3 and MLDv2 protocol behavior on multicast router and proxy side for wireless and mobile networks, including query and other timers tuning. The selective optimization that provides tangible benefits to the mobile hosts and routers is given by keeping track of downstream hosts' membership status and varying IGMP/MLD Query types and values to tune the number of responses. The proposed behavior interoperates with the IGMPv3 and MLDv2 protocols.

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 [1].

In this document, "router" means both multicast router and IGMP/MLD proxy.

3. Explicit Tracking of Membership Status

Mobile hosts use IGMP and MLD to request to join or leave multicast sessions. When an adjacent upstream router receives the IGMP/MLD Report messages, it recognizes the membership status on the link. To update the membership status reliably, the router sends IGMP/MLD Query messages periodically, and sends Group-Specific and/or Group-and-Source Specific Queries when a member host reports its leave. Then the other member hosts reply IGMP/MLD Report messages to notify their memberships. IGMP/MLD Query is therefore necessary to obtain the up-to-date membership information, but a large number of the reply messages sent from all member hosts may cause network congestion or consume network bandwidth consumption.

The "explicit tracking function" [9] is the possible approach to reduce the transmitted number of IGMP/MLD messages and contribute to the efficiency of mobile communications. It enables the router to keep track of the membership status of the downstream IGMPv3 or MLDv2 member hosts. That is, if a router enables the explicit tracking function, it does not always need to ask Current-State Report message transmission from the receiver hosts since the router implicitly recognizes the (potential) last member host when it receives the State-Change Report. The router can therefore send IGMP/MLD Group-Specific and Group-and-Source Specific Queries LMQC/LLQC times (see Section 4.3 for LMQC/LLQC) only when it recognizes the last member has left from the network. This reduces the transmitted number of Current-State Report messages.

Enabling the explicit tracking function is advantageous for mobile multicast, but the function requires additional processing capability and a possibly large memory for routers to keep all membership status. Especially when a router needs to maintain a large number of receiver hosts, this resource requirement is potentially impacted. Therefore, this document recommends that adjacent upstream multicast routers enables the explicit tracking function for IP multicast communications on wireless and mobile networks, if they have enough resources. If operators think that their routers do not have enough resources, they may disable this function on their routers. Note that whether routers enable the explicit tracking function or not, they need to maintain downstream membership status by sending IGMPv3/MLDv2 General Query messages as some IGMPv3/MLDv2 messages may be lost during transmission.

4. Tuning IGMP/MLD Timers and Values

4.1. Tuning IGMP/MLD General Query Interval

IGMP and MLD are non-reliable protocols; to cover the possibility of a State-Change Report being missed by one or more multicast routers, "hosts retransmit the same State-Change Report messages [Robustness Variable] - 1 more times", at intervals chosen at random from the range (0, [Unsolicited Report Interval]) [2][3]. Although this behavior increases the protocol robustness, it does not guarantee that the State-Change Report reaches the routers. Therefore, routers still need to refresh the downstream membership information by receiving Current-State Report periodically solicited by IGMP/MLD General Query sent in the [Query Interval] period, in order to enhance robustness of the host in case of link failures and packet loss. It also supports the situation that mobile hosts turn off or move from a network to other network managed by a different router without any notification (e.g., leave request).

The [Query Interval] is the interval between General Queries sent by the regular IGMPv3/MLDv2 querier, and the default value is 125 seconds [2][3]. By varying the [Query Interval], multicast routers can tune the number of IGMP/MLD messages on the network; larger values cause IGMP/MLD Queries to be sent less often.

This document proposes 150 seconds for the [Query Interval] value by changing the Querier's Query Interval Code (QQIC) field specified in the IGMP/MLD Query message, for the case that a router enabling the explicit tracking function sends General Query and potentially operates a large number of member hosts such as more than 200 hosts on the wireless link. This longer interval value contributes to minimizing traffic of Report messages and battery power consumption for mobile hosts.

On the other hand, this document also proposes 60 to 90 seconds for the [Query Interval] value for the case that a router enabling the explicit tracking function attaches to a wireless link having higher capacity of the resource. This shorter interval contributes to quick synchronization of the membership information tracked by the router but may consume battery power of mobile hosts.

If a router does not enable the explicit tracking function, the [Query Interval] value would be its default value, 125 seconds.

In situations where Mobile IPv6 [14] is used, when the home agent implements multicast router functionality and multicast data packets are tunneled to and from the home agent, the home agent may want to slow down Query periodicity, especially when network congestion is

detected. This can be done by the home agent starting forwarding queries with the default [Query Interval] value and increasing it in a gradual manner until it exceeds the mobile host's lifetime.

4.2. Tuning IGMP/MLD Query Response Interval

The [Query Response Interval] is the Max Response Time (or Max Response Delay) used to calculate the Max Resp Code inserted into the periodic General Queries. Its default value is 10 seconds expressed by "Max Resp Code=100" for IGMPv3 [2] and "Maximum Response Code=10000" for MLDv2 [3]. By varying the [Query Response Interval], multicast routers can tune the burstiness of IGMP/MLD messages on the network; larger values make the traffic less bursty as host responses are spread out over a larger interval, but will increase join latency when State-Change Report is missing.

According to our experimental analysis, this document proposes two tuning scenarios for tuning the [Query Response Interval] value in different wireless link conditions; one scenario is for a wireless link with a lower capacity of network resource or a lossy link, and the other scenario is for a wireless link with enough capacity or reliable condition for IGMP/MLD message transmission.

Regarding the first scenario, for instance, when a multicast router attaches to a bursty IEEE 802.11b link, the router configures the longer [Query Response Interval] value, such as 10 to 20 (sec). This configuration will reduce congestion of the Current-State Report messages on a link but may increase join latency and leave latency when the unsolicited messages (State-Change Record) are lost on the router.

The second scenario may happen for a multicast router attaching to a wireless link having higher capacity of the resource or a point-to-(multi-)point link such as an IEEE 802.16e link, because IGMP/MLD messages do not seriously affect the link condition. The router can seek Current-State Report messages with the shorter [Query Response Interval] value, such as 5 to 10 (sec). This configuration will contribute to quickly (at some level) discovering non-tracked member hosts and synchronizing the membership information.

4.3. Tuning Last Member Query Timer (LMQT) and Last Listener Query Timer (LLQT)

Shortening the Last Member Query Timer (LMQT) for IGMPv3 and the Last Listener Query Timer (LLQT) for MLDv2 contributes to minimizing leave latency. LMQT is represented by the Last Member Query Interval (LMQI), multiplied by the Last Member Query Count (LMQC), and LLQT is represented by the Last Listener Query Interval (LLQI), multiplied by

the Last Listener Query Count (LLQC).

While LMQUI and LLQI are changeable, it is reasonable to use the default values (i.e., 1 second) for LMQUI and LLQI in a wireless network. LMQC and LLQC, whose default value is the [Robustness Variable] value, are also tunable. Therefore, LMQC and LLQC MAY be set to "1" for routers enabling the explicit tracking function, and then LMQT and LLQT are set to 1 second. However, setting LMQC and LLQC to 1 increases the risk of missing the last member; LMQC and LLQC SHOULD be set to 1 only when network operators think that their wireless link is stable enough.

On the other hand, if network operators think that their wireless link is lossy (e.g., due to a large number of attached hosts or limited resources), they MAY set LMQC and LLQC to "2" for their routers enabling the explicit tracking function. Although bigger LMQC and LLQC values may cause longer leave latency, the risk of missing the last member will be reduced.

4.4. Tuning Startup Query Interval

The [Startup Query Interval] is the interval between General Queries sent by a Querier on startup. The default value is 1/4 of [Query Interval]; however, this document recommends the use of its shortened value such as 1 second since the shorter value would contribute to shortening handover delay for mobile hosts in, e.g., the base solution with PMIPv6 [12]. Note that the [Startup Query Interval] is a static value and cannot be changed by any external signal. Therefore operators who maintain routers and wireless links must properly configure this value.

4.5. Tuning Robustness Variable

To cover the possibility of unsolicited reports being missed by multicast routers, unsolicited reports are retransmitted [Robustness Variable] - 1 more times, at intervals chosen at random from the defined range [2][3]. The QRV (Querier's Robustness Variable) field in IGMP/MLD Query contains the [Robustness Variable] value used by the querier. The default [Robustness Variable] value defined in IGMPv3 [2] and MLDv2 [3] is "2".

This document proposes "2" for the [Robustness Variable] value for mobility, when a router attaches to a wireless link having lower capacity of the resource or a large number of hosts. For a router that attaches to a wireless link having higher capacity of the resource or reliable condition, it is not required to retransmit the same State-Change Report message; hence the router sets the [Robustness Variable] to "1". Note that whether the explicit

tracking function is enabled or not, the [Robustness Variable] value SHOULD NOT be bigger than "2".

4.6. Tuning Scenarios for Various Mobile IP Networks

In mobile IP networks, IGMP and MLD are used either with three deployment scenarios; (1) running directly between host and access router on a wireless network, (2) running between host and home router through a tunnel link, and (3) running between home router and foreign router through a tunnel link.

When a receiver host connects directly through a wireless link to a foreign access router or a home router, the tuning of the IGMP/MLD protocol parameters should be the same as suggested in the previous sections. The example of this scenario occurs when route optimization is adopted in MIPv6 [14] or Mobile IP [15], or when in Proxy Mobile IPv6 (PMIPv6) [11], the mobile access gateway, whose role is similar to the one of a foreign router, acts as a multicast router as proposed in [13].

The second scenario occurs when bi-directional tunnel established between host and home router is used to exchange IGMP/MLD messages such as [14][15]. There are difficulties in tuning the parameters in this situation, because the tunnel link condition is diverse and changeable. When a host is far away from the home router, the transmission delay between the two entities may be longer and the packet delivery may be more unreliable. Thus the effects of the IGMP/MLD message transmission through a tunnel link should be considered during the parameter setting. For example, the [Query Interval] and [Query Response Interval] could be set shorter to compensate the transmission delay, and the [Robustness Variable] could be increased for possible packet loss.

The third scenario occurs in [12], in which the mobile access gateway (i.e., foreign router) acts as the IGMP/MLD Proxy [10] in PMIPv6 [11]. Through the bi-directional tunnel established with the local mobility anchor (i.e., home router), the mobile access gateway sends summary reports of its downstream member hosts to the local mobility anchor. Apart from the distance factor that influences the parameter setting, the [Query Response Interval] on the local mobility anchor could be set to the smaller value since the number of foreign router is much smaller compared to the that of the host and the chances of packet burst is low for the same reason.

Ideally, the IGMP/MLD querier router adjusts its parameter setting according to the actual mobile IP network conditions to benefit service performance and resource utilization. It would be desirable that a home router determines aforementioned timers and values

according to the delay between the initiating IGMP/MLD Query and the responding IGMP/MLD Report, while describing such mechanism dynamically adjusting these timers and values is out of scope of this document.

5. Destination Address of Specific Query

IGMP/MLD Group-Specific and Group-and-Source Specific Queries defined in [2][3] are sent to verify whether there are hosts that desire reception of the specified group or a set of sources or to rebuild the desired reception state for a particular group or a set of sources. These specific Queries build and refresh multicast membership state of hosts on an attached network. These specific Queries should be sent to all desired hosts with specific multicast address (not the all-hosts/all-nodes multicast address) as their IP destination addresses, because hosts that do not join the multicast session do not pay attention to these specific Queries, and only active member hosts that have been receiving multicast contents with the specified address reply IGMP/MLD reports.

6. Interoperability

IGMPv3 [2] and MLDv2 [3] provide the ability for hosts to report source-specific subscriptions. With IGMPv3/MLDv2, a mobile host can specify a channel of interest, using multicast group and source addresses in its join request. Upon its reception, the upstream router that supports IGMPv3/MLDv2 establishes the shortest path tree toward the source without coordinating a shared tree. This function is called the source filtering function and is required to support Source-Specific Multicast (SSM) [8].

Recently, the Lightweight-IGMPv3 (LW-IGMPv3) and Lightweight-MLDv2 (LW-MLDv2) [4] protocols have been defined as the proposed standard protocols in the IETF. These protocols provide protocol simplicity for mobile hosts and routers, as they eliminate a complex state machine from the full versions of IGMPv3 and MLDv2, and promote the opportunity to implement SSM in mobile communications.

This document assumes that both multicast routers and mobile hosts MUST be IGMPv3/MLDv2 capable, regardless whether the protocols are the full or lightweight version. And this document does not consider interoperability with older version protocols. The main reason not being interoperable with older IGMP/MLD protocols is that the explicit tracking function does not work properly with older IGMP/MLD protocols.

7. Security Considerations

This document neither provides new functions or modifies the standard functions defined in [2][3][4]. Therefore there is no additional security consideration provided.

8. Acknowledgements

Luis M. Contreras, Marshall Eubanks, Gorrry Fairhurst, Dirk von Hugo, Imed Romdhani, Behcet Sarikaya, Yogo Uchida, Stig Venaas, Jinwei Xia, and others provided many constructive and insightful comments.

9. References

9.1. Normative References

- [1] Bradner, S., "Key words for use in RFCs to indicate requirement levels", RFC 2119, March 1997.
- [2] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.
- [3] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.
- [4] 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.
- [5] Deering, S., "Host Extensions for IP Multicasting", RFC 1112, August 1989.
- [6] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, July 1997.
- [7] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.
- [8] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.

9.2. Informative References

- [9] 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.
- [10] 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.
- [11] Gundavelli, S, Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [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 Multicast", draft-asaeda-multimob-pmip6-extension-07 (work in progress), October 2011.
- [14] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [15] Perkins, Ed., C., "IP Mobility Support for IPv4, Revised", RFC 5944, November 2010.

Appendix A. Unicasting General Query

IGMPv3 and MLDv2 specifications [2][3] describe that a host **MUST** accept and process any Query whose IP Destination Address field contains any of the addresses (unicast or multicast) assigned to the interface on which the Query arrives. In general, the all-hosts multicast address (224.0.0.1) or link-scope all-nodes multicast address (FF02::1) is used as the IP destination address of IGMP/MLD General Query. On the other hand, according to [2][3], a router **MAY** be able to unicast General Query to tracked member hosts in [Query Interval], if the router keeps track of membership information (Section 3).

Unicasting IGMP/MLD General Query would reduce the drain on battery power of mobile hosts as only the active hosts that have been receiving multicast contents respond the unicast IGMP/MLD General Query messages and non-active hosts do not need to pay attention to the IGMP/MLD messages. This also allows the upstream router to proceed fast leaves (or shorten leave latency) by setting LMQC/LLQC smaller, because the router can immediately converge and update the membership information, ideally.

However, there is a concern in unicast General Query. If a multicast router sends General Query "only" by unicast, it cannot discover potential member hosts whose join requests were lost. Since the hosts do not retransmit the same join requests (i.e., unsolicited Report messages), they lose the chance to join the channels unless the upstream router asks the membership information by sending General Query by multicast. It will be solved by using both unicast and multicast General Queries and configuring the [Query Interval] timer value for multicast General Query and the [Unicast Query Interval] timer value for unicast General Query. However, using two different timers for General Queries would require the protocol extension this document does not focus on. If a router does not distinguish the multicast and unicast General Query Intervals, the router should only use and enable multicast General Query.

Also, unicasting General Query does not remove multicasting General Query. Multicast General Query is necessary to update membership information if it is not correctly synchronized due to missing Reports. Therefore, enabling unicast General Query **SHOULD NOT** be used for the implementation that does not allow to configure different query interval timers as [Query Interval] and [Unicast Query Interval]. If a router does not distinguish these multicast and unicast General Query Intervals, the router **SHOULD** only use and enable multicast General Query.

Authors' Addresses

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/>

Hui Liu
Huawei Technologies Co., Ltd.
Huawei Bld., No.3 Xinxu Rd.
Shang-Di Information Industry Base
Hai-Dian District, Beijing 100085
China

Email: helen.liu@huawei.com

Qin Wu
Huawei Technologies Co., Ltd.
Site B, Floor 12F, Huihong Mansion
No.91 Baixia Rd.
Nanjing, Jiangsu 21001
China

Email: bill.wu@huawei.com

MULTIMOB Group
Internet-Draft
Intended status: Standards Track
Expires: May 16, 2012

T C. Schmidt
HAW Hamburg
M. Waehlich
link-lab & FU Berlin
R. Koodli
Cisco Systems
G. Fairhurst
University of Aberdeen
November 13, 2011

Multicast Listener Extensions for MIPv6 and PMIPv6 Fast Handovers
draft-schmidt-multimob-fmipv6-pfmipv6-multicast-05

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 May 16, 2012.

Copyright Notice

Copyright (c) 2011 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 PFMIPv6 - 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.

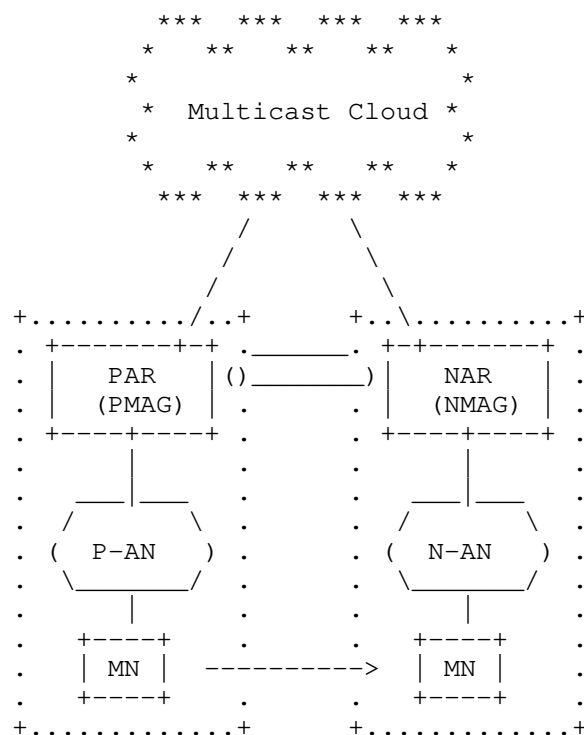


Figure 1: Reference Network for Fast Handover

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.

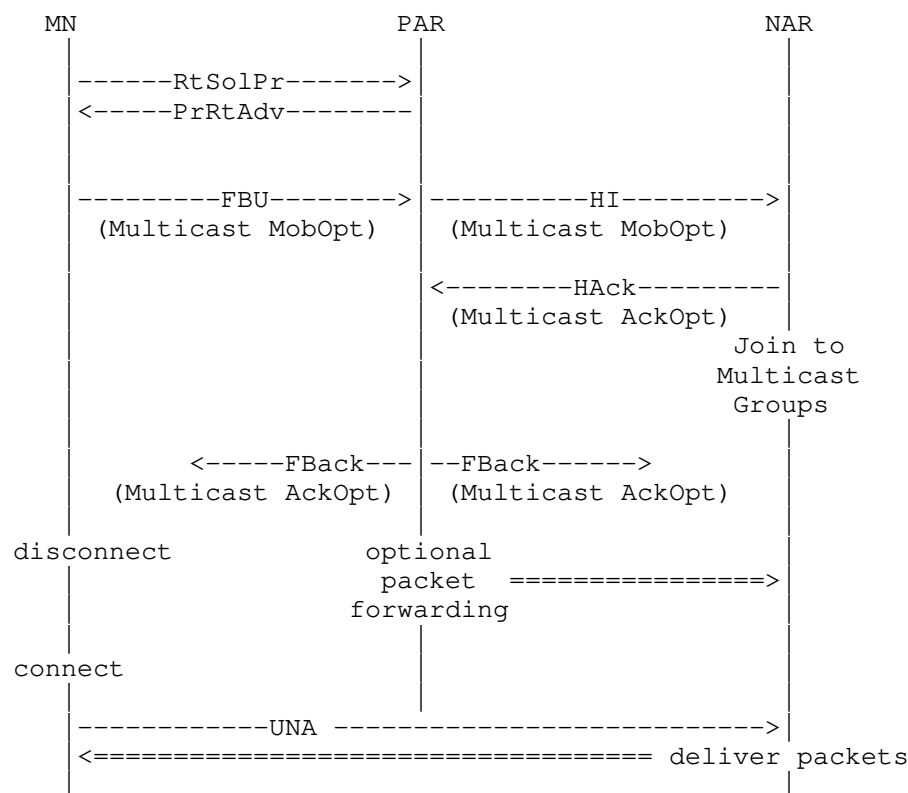


Figure 2: Predictive Multicast Handover for FMIPv6

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.

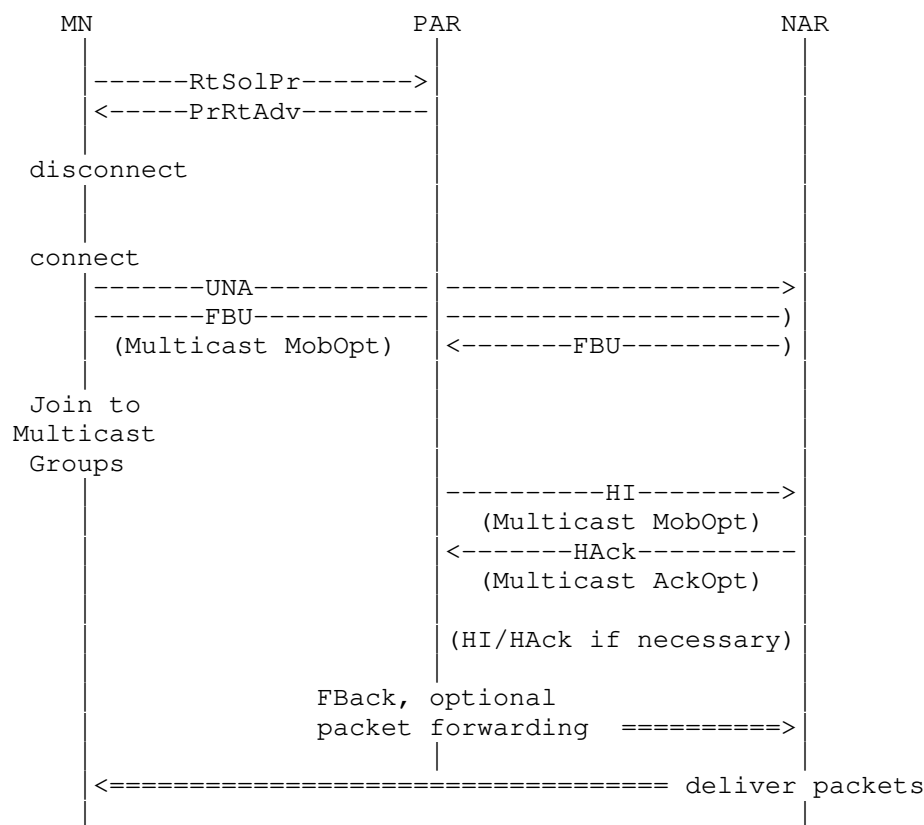


Figure 3: Reactive Multicast Handover for FMIPv6

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.

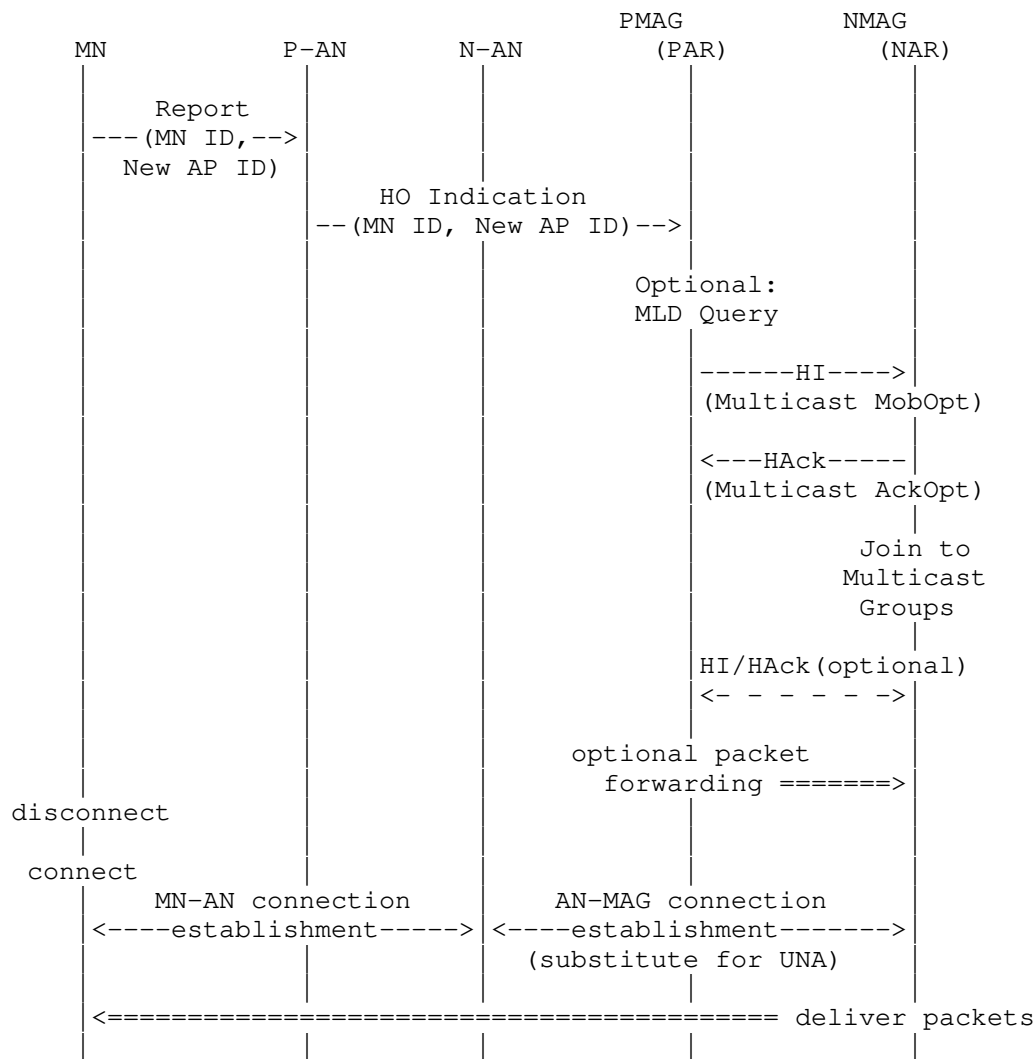


Figure 4: Predictive Multicast Handover for PFMIPv6

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.

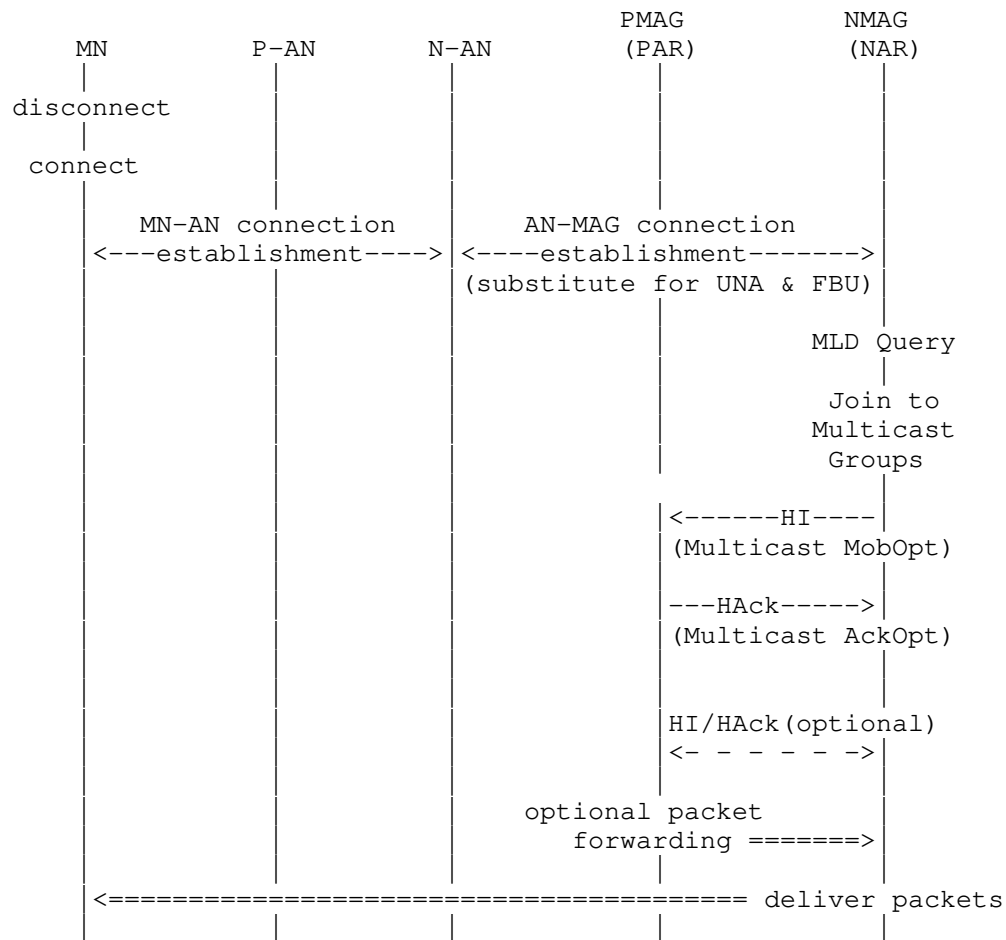


Figure 5: Reactive Multicast Handover for PFMIPv6

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.

4.1.2. 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 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 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.

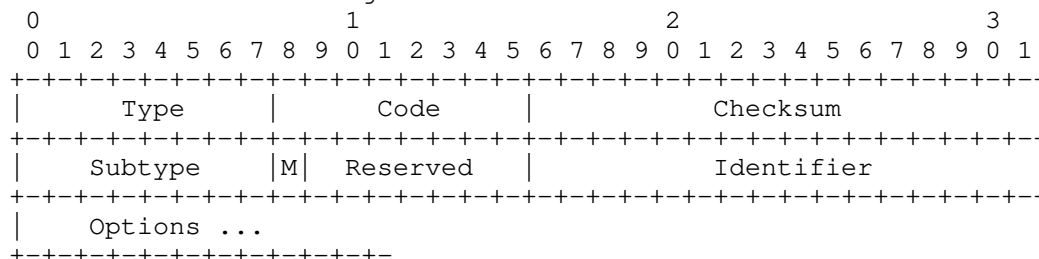


Figure 6: Multicast Indicator Bit for Proxy Router Advertisement (PrRtAdv) Message

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.

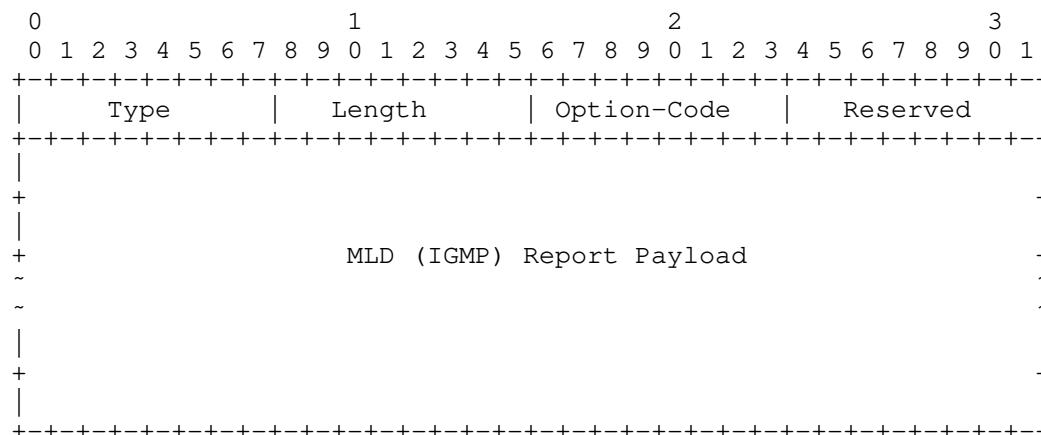


Figure 7: Mobility Header Multicast Option

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).

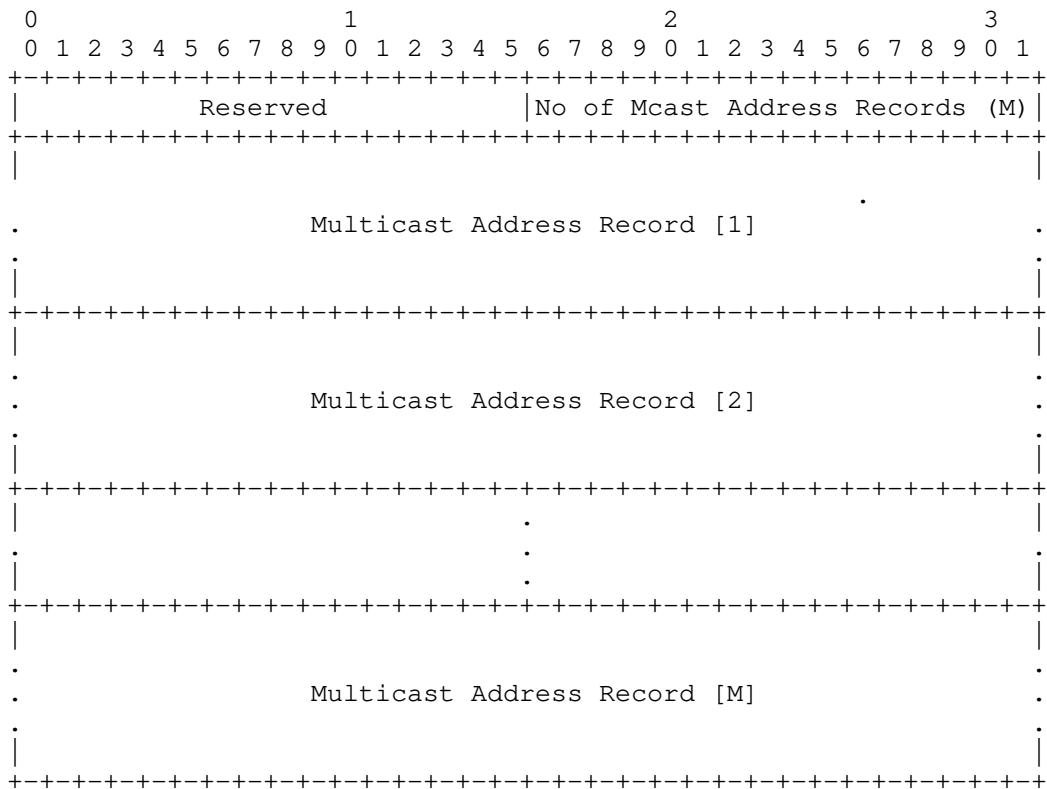


Figure 8: MLDv2 Report Payload

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.

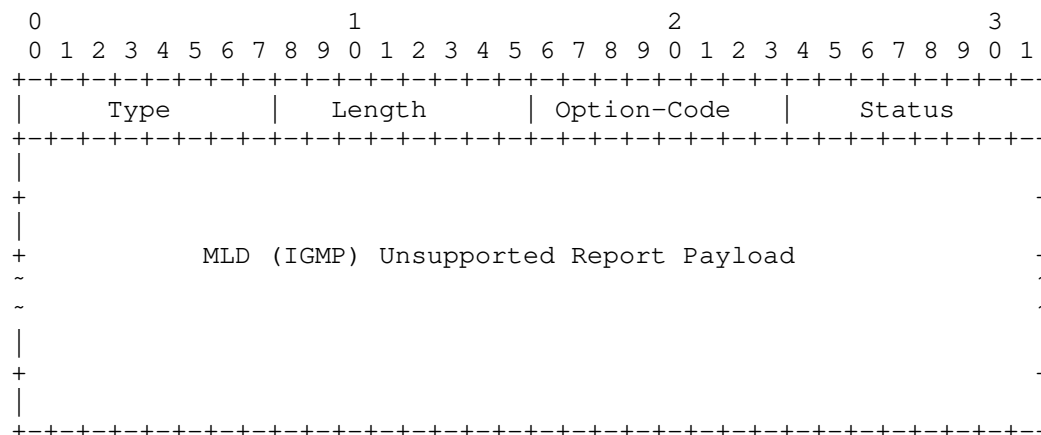


Figure 9: Mobility Header Multicast Acknowledgement Option

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., 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-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

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-smspmip]). 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.

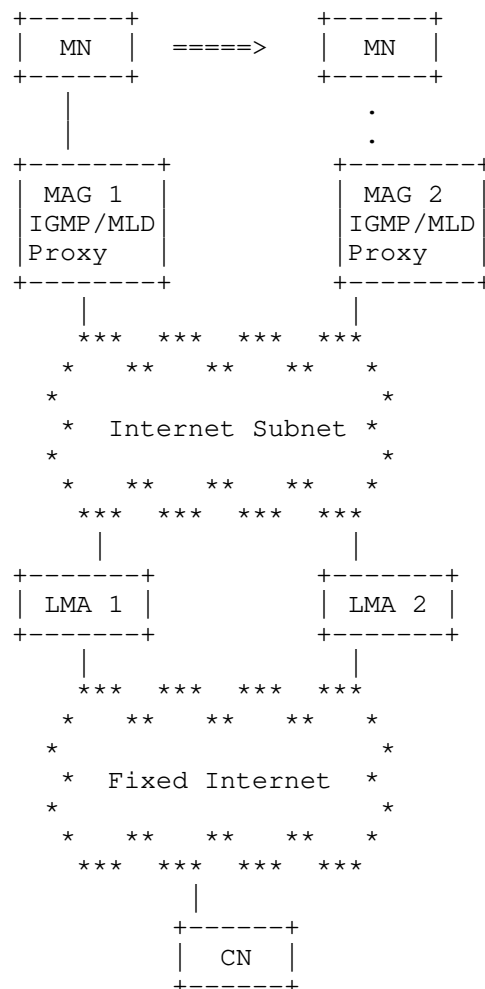


Figure 1: MultiMob Scenario for chartered PMIP6 issue

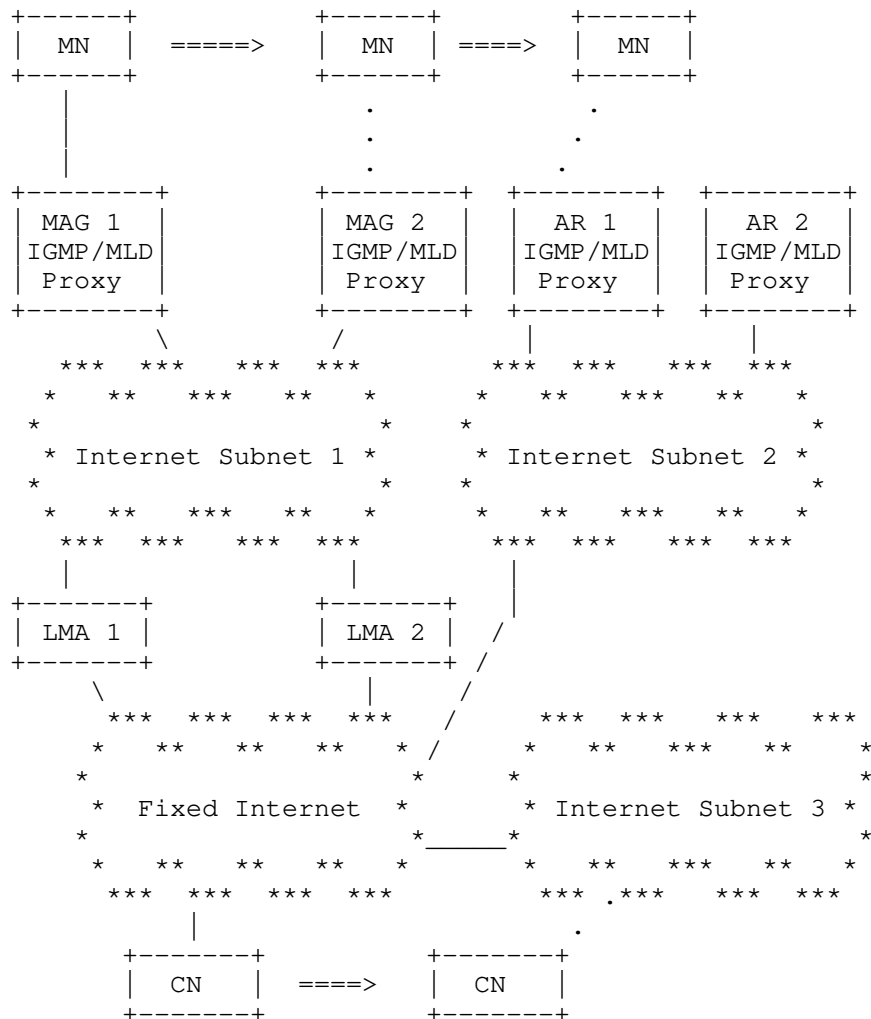


Figure 2: MultiMob scenario for extended MultiMob issues

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 be 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

Hitoshi Asaeda
Keio University
Graduate School of Media and Governance
5322 Endo
Fujisawa, Kanagawa 252-8520
Japan

Email: 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

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

Email: pierrick.seite@orange-ftgroup.com

MULTIMOB Group
Internet-Draft
Expires: January 5, 2012

D. von Hugo
Deutsche Telekom Laboratories
H. Asaeda
Keio University
July 4, 2011

Context Transfer Protocol Extension for Multicast
draft-vonhugo-multimob-cxtp-extension-00

Abstract

This document describes an extension of the Context Transfer Protocol (CXTP) to support seamless IP multicast services with Proxy Mobile IPv6 (PMIPv6).

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 5, 2012.

Copyright Notice

Copyright (c) 2011 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	4
3. Handover Process	5
3.1. Multicast Context Transfer Data Format	5
3.2. Multicast Context Transfer with MLD Proxy	6
3.3. Multicast Context Transfer with PIM-SM	9
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 extension of the Context Transfer Protocol (CXTTP) [10] to provide seamless handover for multicast communications operated with Proxy Mobile IPv6 (PMIPv6) [2]. When a mobile node receiving multicast data detaches from the current MAG and attaches to a new MAG, the node should be able to continuously receive the multicast data through the new MAG just after the node completed handover 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.

The Context Transfer Protocol (CXTTP) specification [10] describes the mechanism that allows better support for minimizing service disruption during handover. In this document, CXTTP is extended for the multicast context transfer protocol in PMIPv6. "Multicast-Context Transfer Data (M-CTD)" is defined for transferring multicast membership state from a previously attached MAG (p-MAG) to a newly attached MAG (n-MAG) for PMIPv6. The context transfer is either started from the n-MAG on its own after attachment of the mobile node or initiated by the p-MAG after being informed by the access network of the planned handover.

An approach to apply CXTTP to multicast for client-based mobile IPv6 had been proposed in [14].

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 the Proxy Mobile IPv6 specification [2]; 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. Handover Process

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. MAG tracks the mobile node's movements to and from the access link and performs signaling of the status to the mobile node's LMA. In PMIPv6, it SHOULD NOT be required for mobile nodes to initiate re-subscription to multicast channels, and MAG SHOULD keep multicast membership state for mobile nodes even if they attach a different MAG in PMIPv6-Domain.

For multicast context transfer, an IGMP/MLD-based explicit membership tracking function [12] MUST be enabled on MAG (whether the MAG 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-MAG extracts the mobile node's multicast membership state from complete multicast membership state the p-MAG has maintained and transmits it to the n-MAG.

3.1. Multicast Context Transfer Data Format

Multicast Context Transfer Data (M-CTD) is a message used with CXTF to transfer multicast membership state from p-MAG to n-MAG. 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 [4].
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 MAG.

The following information included in a reply to M-CTD (similar to the CTDR message defined in [10]) is used to request the old MAG to store still incoming multicast data, to forward them to the new MAG, and finally to leave the multicast group after successful handover from n-MAG to p-MAG.

1. Receiver address - indicates the address of the MN sending the Current-State Report.
2. Flag indicating the p-MAG 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 succesful handover, or to leave (L) the multicast groups unless there are still other active subscriptions for the corresponding groups on the p-MAG.
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 succesful reception of context data at the new MAG.

The explicit tracking function [12] does not maintain information of an (S,G) join request with EXCLUDE filter mode. Therefore, when the "Filter mode" for a multicast session is EXCLUDE, "Source address" for the session MUST be set "Null".

3.2. Multicast Context Transfer with MLD Proxy

This section describes the case that MAG operates as an MLD proxy, as defined in [6] and specified in the base MultiMob solution [11].

The MLD listener handover with CXTP and MLD proxy shown in Figure 1 is defined as follows.

1. After attaching a new MAG, a mobile node sends a Router Solicitation (RS) as specified in [7]. As the MN shall remain unaware of any change in connectivity the n-MAG has to identify the p-MAG address during proxy binding registration process with the mobile node's LMA. n-MAG then sends a request for context transfer (CT-Req) to the p-MAG as defined in [10]. Since the MN cannot initiate the related Context Transfer Activate Request (CTAR) message that may be sent by the LMA. In case the mobile node has the capability and the chance to signal to the p-MAG the link status and the potential new MAG address (e.g. as is specified in terms of Event Services by [9]) the p-MAG will send a CTAR message to n-MAG on behalf of the mobile node. Alternatively the p-MAG or the n-MAG may have information on potential MAGs in their vicinity to which such a CTAR or CT-Req message may be multicast.

2. p-MAG provides together with the other feature data the multicast states corresponding to the moving MN-Identifier to n-MAG. p-MAG utilizes a context transfer protocol to deliver MN's Policy Profile to n-MAG, and sends Multicast Context Transfer Data (M-CTD) (defined in Section 3.1) to n-MAG.
3. If there are multicast channels the MN has subscribed but the n-MAG has not yet subscribed, n-MAG subscribes via sending (potentially aggregated) MLD [4][5] Membership Report messages (i.e. Join) to the corresponding LMA.
4. n-MAG requests from p-MAG to store still incoming multicast data for transfer to MN after successful handover completion. For this purpose a newly defined B-flag in the Multicast Context Transfer Response message is sent from n-MAG to p-MAG, denoted as M-CTDR(B).
5. After successful completion of MN attachment to n-MAG the forwarding of the stored Multicast data from p-MAG to n-MAG is initiated via sending a Multicast Context Transfer Response message with a newly defined F-flag from n-MAG to p-MAG, denoted as M-CTDR(F).
6. LMA forwards requested multicast data to the n-MAG which subsequently delivers them to MN.
7. n-MAG may request from p-MAG to leave those multicast groups it had subscribed to on behalf of the MN where MN had been the last member. This is done via sending a Multicast Context Transfer Response message from n-MAG to p-MAG with a newly defined L-flag set, denoted as M-CTDR(L).

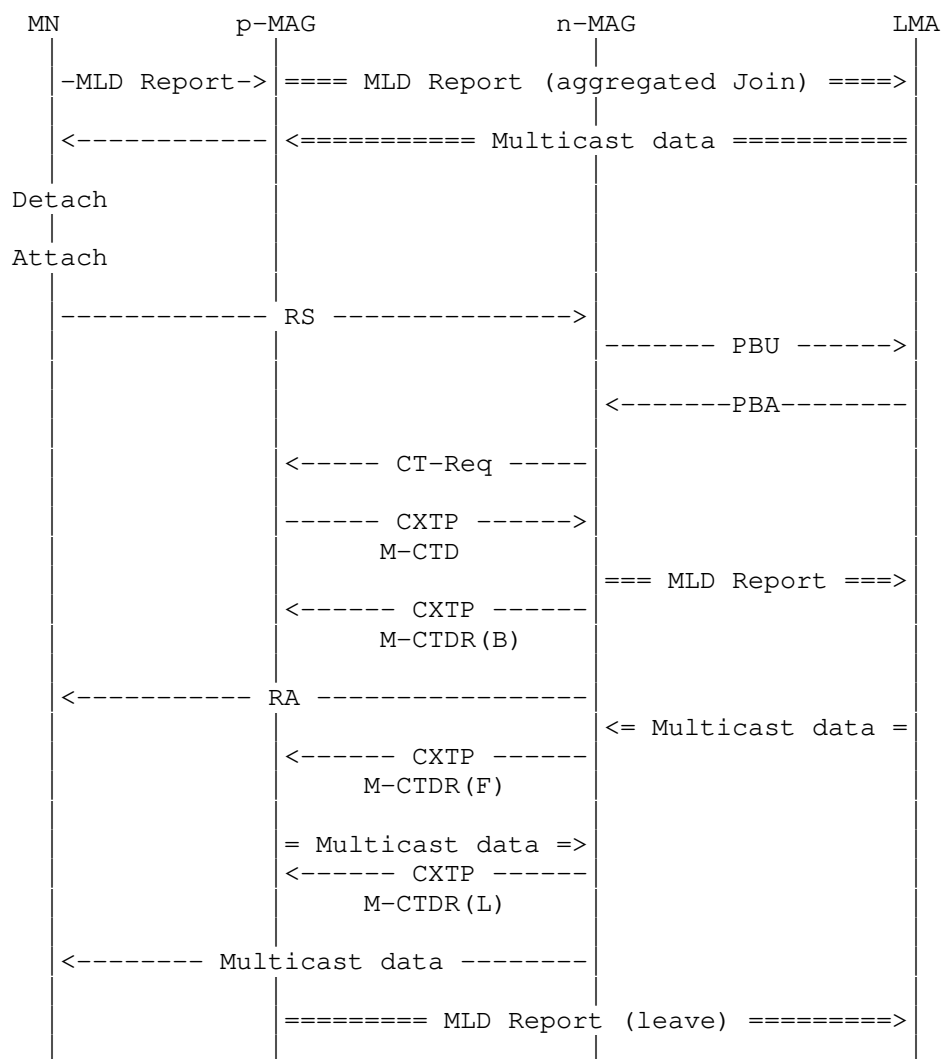


Figure 1: MLD listener handover with CXTP and MLD proxy

After MN attaches to n-MAG, the forwarded multicast data from p-MAG will be delivered to the MN immediately. Afterwards the current multicast data are delivered as received from LMA and the MN's multicast membership state at the p-MAG is cancelled.

3.3. Multicast Context Transfer with PIM-SM

This section describes the case that MAG operates as a PIM-SM [3] router, as described in a proposed solution [13].

The MLD listener handover with CXTTP and PIM-SM shown in Figure 2 is defined as follows.

1. The first and second procedures are the same ones as described in Section 3.2.
2. If there are multicast channels the MN has subscribed but the n-MAG has not yet subscribed, n-MAG joins the multicast tree via sending PIM Join messages to the upstream router (Figure 2 shows the example that the upstream router is the corresponding LMA).
3. The remaining steps for completion of the context transfer are the same ones as described in Section 3.2 with the only exception being that p-MAG sends a PIM Prune message to LMA instead of a MLD Report (leave) message if there are no attached mobile nodes listening the multicast channels.

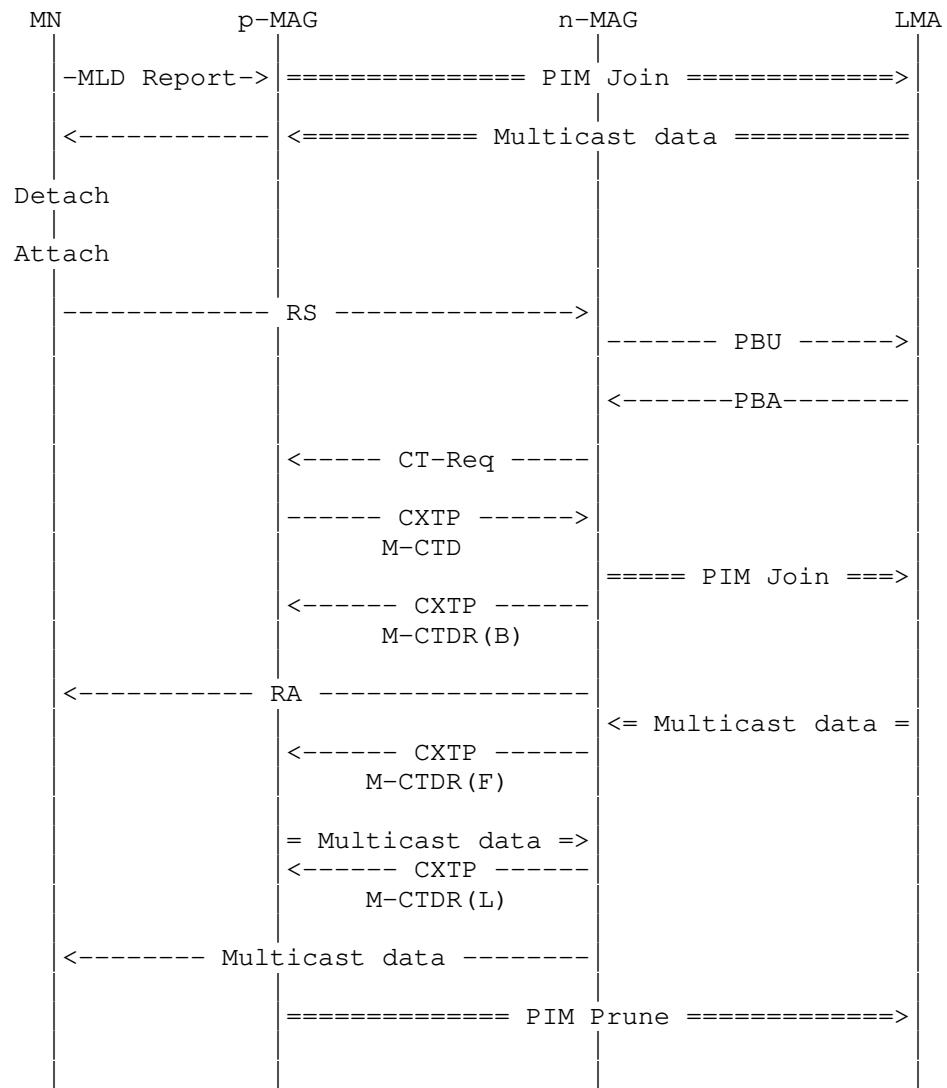


Figure 2: MLD listener handover with CXTP and PIM-SM

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.

7. References

7.1. Normative References

- [1] Bradner, S., "Key words for use in RFCs to indicate requirement levels", RFC 2119, March 1997.
- [2] Gundavelli, S, Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [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] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.
- [5] Liu, H., Cao, W., and H. Asaeda, "Lightweight IGMPv3 and MLDv2 Protocols", RFC 5790, February 2010.
- [6] 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.
- [7] Singh, H., Beebee, W., and E. Nordmark, "IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes", RFC 5942, July 2010.
- [8] Yokota, H., Chowdhury, K., Koodli, R., Patil, B., and F. Xia, "Fast Handovers for Proxy Mobile IPv6", RFC 5949, September 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 (CXTP)", RFC 4067, July 2005.
- [11] Schmidt, T., Waehlis, M., and S. Krishnan, "Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains", RFC 6224, April 2011.
- [12] Asaeda, H. and Y. Uchida, "IGMP/MLD-Based Explicit Membership Tracking Function for Multicast Routers",

draft-asaeda-mboned-explicit-tracking-02.txt (work in progress), March 2011.

- [13] Asaeda, H., Seite, P., and J. Xia, "PMIPv6 Extensions for Multicast",
draft-asaeda-multimob-pmipv6-extensions-05.txt (work in progress), February 2011.
- [14] Miloucheva, I. and K. Jonas, "Multicast Context Transfer in mobile IPv6", draft-miloucheva-mldv2-mipv6-00.txt (work in progress), June 2005.

Authors' Addresses

Dirk von Hugo
Deutsche Telekom AG Laboratories
Deutsche-Telekom-Allee 7
D-64295 Darmstadt
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/>

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:

- Point To Point (PTP) link model
- Point To Multipoint (PTMP) link model
- 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:

- 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.
- 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.
- By eliminating multicast listener report suppression, hosts have fewer messages to process; this leads to a simpler state machine implementation.
- 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 Interval], 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

MULTIMOB Working Group
Internet Draft
Expires: January 2012

Hong-Ke Zhang
Zhi-Wei Yan
Shuai Gao
Li-Li Wang
Beijing Jiaotong University
Qian Wu
He-Wu Li
Tsinghua University
July 22, 2011

Multicast Source Mobility Support in PMIPv6 Network
draft-zhang-multimob-msm-03.txt

Abstract

Proxy Mobile IPv6 (PMIPv6), specified in RFC 5213 [1], is a network-based mobility management protocol. It uses a Mobile Access Gateway (MAG) and a Local Mobility Anchor (LMA) to allow hosts to move around within a domain while keeping their address or address prefix stable. Although the issues of mobile multicast in the PMIPv6 network are being discussed in the Multimob WG, how to provide the service connectivity when the multicast source is moving is still a problem for the PMIPv6. This document proposes and analyzes the potential solutions of the multicast source mobility in PMIPv6.

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 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>

This Internet-Draft will expire on January, 2012.

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 Simplified BSD License.

Table of Contents

1. Introduction.....	3
2. Problem statement.....	3
3. Multicast source mobility scheme in PMIPv6.....	4
3.1. Data transmission through tunneling.....	4
3.2. Data transmission after tunneling.....	8
4. Extensions of PMIPv6.....	9
4.1. MAG.....	10
4.2. LMA.....	10
5. Format of signaling messages.....	10
5.1. PBU.....	10
5.2. PBA.....	11
5.3. Multicast address option.....	11
6. Security Considerations.....	12
7. References.....	12
Authors' Addresses.....	14
Acknowledgment.....	14

Different from Mobile IPv6 (MIPv6) [2], PMIPv6 was proposed to support the network-based mobility management. The entities in the PMIPv6 have the responsibilities to track the Mobile Node (MN), update the location of the MN and redirect the packets to and from the MN. However, the basic PMIPv6 protocol only solves the mobility management for the MN which is involved in the unicast communication. In order to deploy the multicast service in the PMIPv6 network, many schemes have been proposed [3-6]. However, all of these schemes aim to support the multicast service for the mobile receiver. How to support the multicast source mobility in the PMIPv6 network is a newly planned work in the Multimob WG. Without doubt, the multicast source mobility is also a very important issue for the deployment of the multicast service. For example, there is an advanced concept based on the Intelligent Transport Systems (ITS) service. In this concept, all the vehicles on the same route are identified by using a GPS or a car-navigation system. The vehicles multicast real-time video information about the transportation through the communication infrastructure like 3G, WiFi to the other vehicles interested in it. This advance information is called as 'future vision' [7]. The multicast source mobility is one of the core supporting schemes to realize the above functions.

In this document, the potential solutions of the multicast source mobility in PMIPv6 are proposed and analyzed.

2. Problem statement

In PMIPv6 base solution, the LMA and the MAG are two most important functional entities. The LMA is the home agent for the MN in a PMIPv6 domain. It is the topological anchor point for the MN's home network prefix(es) and is the entity that manages the MN's binding state. The MAG is a function on an access router that manages the mobility-related signaling for an MN that is attached to its access link. It is responsible for tracking the MN's movements to and from the access link and for signaling the MN's LMA. Therefore, the topological location of the MN is not equal to the actual location in the PMIPv6 networks, which brings some problems for the multicast packet transmission.

And according to the statements in the Section 6.10.5 in RFC5213, when the MAG receives a packet from an MN connected to its access link, to a destination that is not directly connected, the packet MUST be forwarded to the LMA through the bi-directional tunnel established between the MAG and the MN's LMA. And in Section 6.3 in RFC5213 it is assumed that the link between the MN and the MAG have

multicast capability. However, there is no related description on the transmission of the multicast data in RFC5213, that is, there is no scheme about the multicast data forwarding. Thus, the MAG does not explicitly support the multicast communication. When the multicast traffic flows arrive at the MAG, for there is no Multicast Forwarding Information Base (MFIB) on the MAG, it will not be forwarded or transmitted through the bi-directional tunnel between the MAG and the LMA and then these packets would be simply discarded by the MAG.

And even though the multicast packets can be transmitted to the LMA by some special processing, whether the LMA could carry out the functionality of the Designated Router (DR) can not be guaranteed. That is, whether the LMA can execute the source registration to the Rendezvous Point (RP) in the Any Source Multicast (ASM) scenario is not sure. And similarly in the Source-Specific Multicast (SSM) case, whether the LMA could forward the packets received from the tunnel interface to the other multicast router according to the related MFIB is also not sure. It is possibly because that the LMA is not directly connected to the source and the network prefix of the LMA's interface address is different from the Home Network Prefix (HNP) of the MN.

In Section 3, the above mentioned problems of multicast source mobility in PMIPv6 will be discussed and also some possible solutions are proposed.

3. Multicast source mobility scheme in PMIPv6

In this section, according to the problem statement in Section 2 and the path of the multicast packet transmission, it is divided into two parts to describe the scheme of the multicast source mobility in PMIPv6.

3.1. Data transmission through tunneling

Because the MAG does not explicitly support the multicast communication, in order to make the multicast data be forwarded or transmitted through the bi-directional tunnel between the MAG and the LMA based on the PMIPv6 protocol, two possible solutions for that are given as follows.

Solution I: some extensions on the PMIPv6 are required for the transmission of the multicast data. By establishing multicast forwarding states on the MAG based on the PMIPv6, the multicast data sent by the mobile source can be forwarded through the LMA-MAG tunnel to the LMA after receiving this packet on the MAG. That is, after the MAG builds the PMIPv6 tunnel and adds route for the anycast packets originated from or destined to the MN, it should also update the

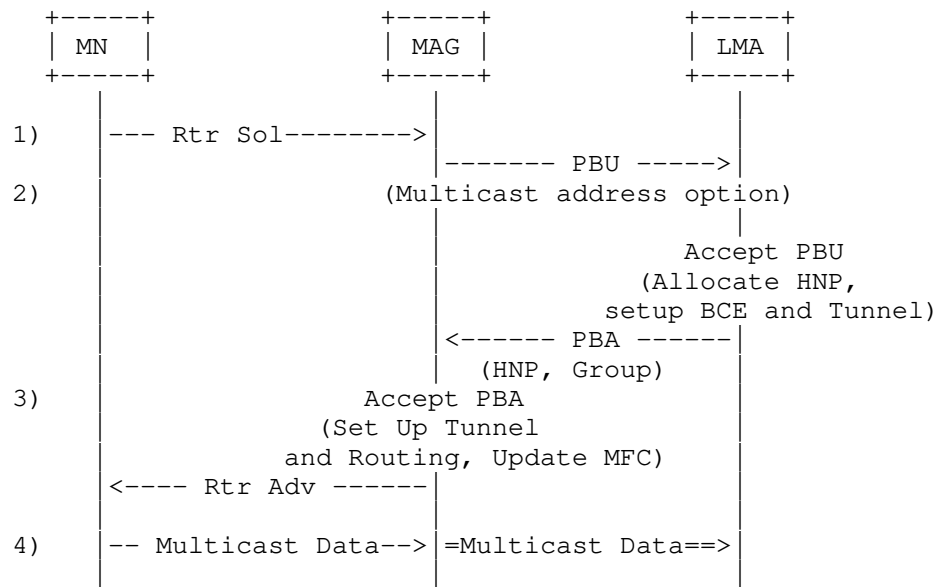


Figure 1: Procedure of extending the PMIPv6

The detailed descriptions are as follows:

- 1) The MN connects to the MAG initially and sends Router Solicitation (RS) message to the MAG;
- 2) When the attachment of MN is detected by the MAG, it obtains the group address as well as LMAA and MN_ID from the profile. Then an extended Proxy Binding Update (PBU) message is sent to the LMA. Because the LMA finds the Multicast address option contained in the PBU message, the LMA decide whether the MN is authorized to send multicast data to the group address. And then the LMA sends back an extended Proxy Binding Acknowledgement (PBA) message to the MAG. Afterwards, the tunnel is established in the LMA;
- 3) The MAG on receiving the PBA message sets up its endpoint of the bi-directional tunnel to the LMA and then sets up the forwarding for the MN's unicast traffic. At the same time, in order to support multicast source mobility, the MAG should also update the MFC in the kernel. And then it sends Router Advertisement (RA)

- 4) The same as the specification in RFC5213, when the MAG receives a multicast packet from an MN connected to its access link, to a multicast destination that has been authorized by the LMA, the MAG will forward this packet to the LMA through the bi-directional tunnel established between itself and the LMA.

And the format of the tunnel multicast packets is shown below.

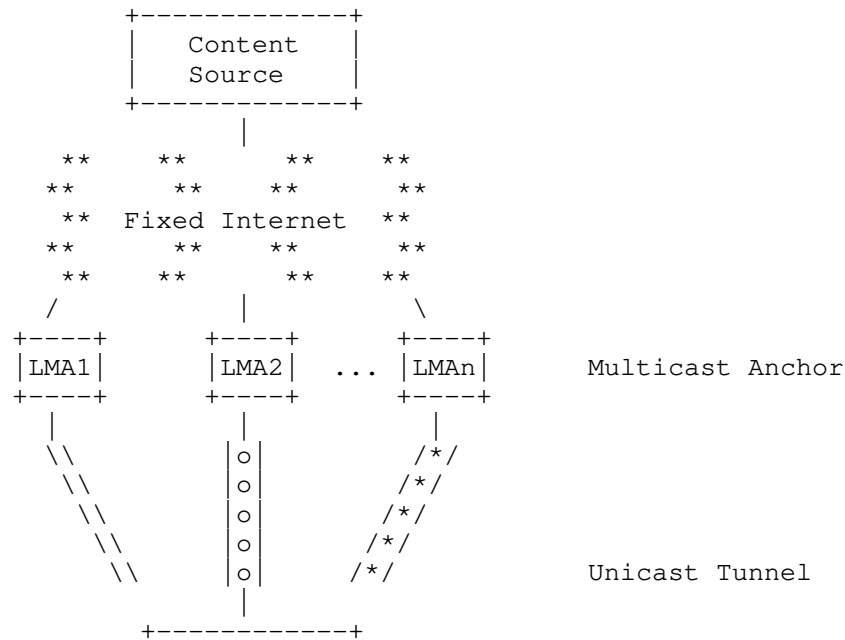
```
IPv6 header (src= Proxy-CoA, dst= LMAA)   /*Tunnel Header*/  
  IPv6 header (src= MN-HoA, dst= GRPA)   /*Packet Header*/  
    Upper layer protocols                   /*Packet Content*/
```

Solution II: some extra functions, such as MLD Proxy as discussed in RFC 4605 [8] and [draft-schmidt-multimob-pmipv6-base-source] [9], could be used to transmit the multicast data through the tunnel of the PMIPv6. The MLD proxy functions are deployed at the MAG as described in RFC 6224 [10] and the MLD proxy instance serving a mobile multicast source configures its upstream interface at the tunnel towards the MN's corresponding LMA. For each LMA, there will be a separate instance of an MLD proxy.

Although multicast communication can be enabled in PMIPv6 domains by deploying MLD Proxy functions at MAG, some disadvantages still exist. Firstly, for a proxy device performing IGMP/MLD-based forwarding has a single upstream interface and one or more downstream interfaces as described in RFC4605, there should be many MLD Proxy functions deployed at one MAG, which is complicated and then is difficult for implementation and management. And then when the multicast packets arrive at the MAG running multiple parallel MLD proxy functions, there may be confusions for the data if there is no extra processing or filtering scheme at the MAG. In addition, the route optimization issue is still up in the air, that is, for a mobile receiver and a source on the same MAG using 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.

Therefore, the MLD Proxy function should be extended to accommodate the PMIPv6 protocol. As same as the document [9] and [10], the MLD proxy functions are deployed at the MAG, while only one MLD Proxy function is required to run at the MAG and multiple upstream interfaces can be set for the MLD Proxy instance, which is called Multi-Upstream Interfaces MLD Proxy (MUIMP). Figure 2 shows the

architecture of the MUIMP deploying in PMIPv6 for the multicast source mobility. As shown in Figure 2, the paths among the MAGs and the LMA represented by "||", "|o|" and "/*/" indicate the tunnels in base PMIPv6 for the MN1, MN2, and MNn, respectively. In this way, when the multicast data sent by the mobile source gets to the MAG from the downstream interface of an MLD proxy, the MAG forwards this data to the corresponding upstream interface according to the Binding Update List Entry (BULE) for example at this MAG and to all but the incoming downstream interfaces with appropriate forwarding states for this group. And the specific scheme for the choice of the corresponding upstream interface is outside of this document. Therefore, multicast packets originating from an MN/mobile source will arrive at the corresponding LMA and directly at all mobile receivers co-located at the same MAG. Figure 3 shows the signaling call flow of the MN attachment in this scheme. And when the MN leaves, after the deregistration of the PMIPv6 for MNs, the MUIMP deletes the corresponding upstream tunnel interface for each MN which leaves. When the MN hands over, it is the same course as the MN attached. And this scheme can not only solve the route optimization issue as mentioned in the document [9], but also can be easily to deploy, implement and manage.



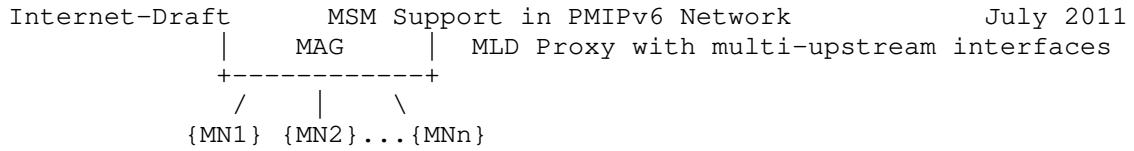


Figure 2: Architecture of the MUIMP deploying in PMIPv6

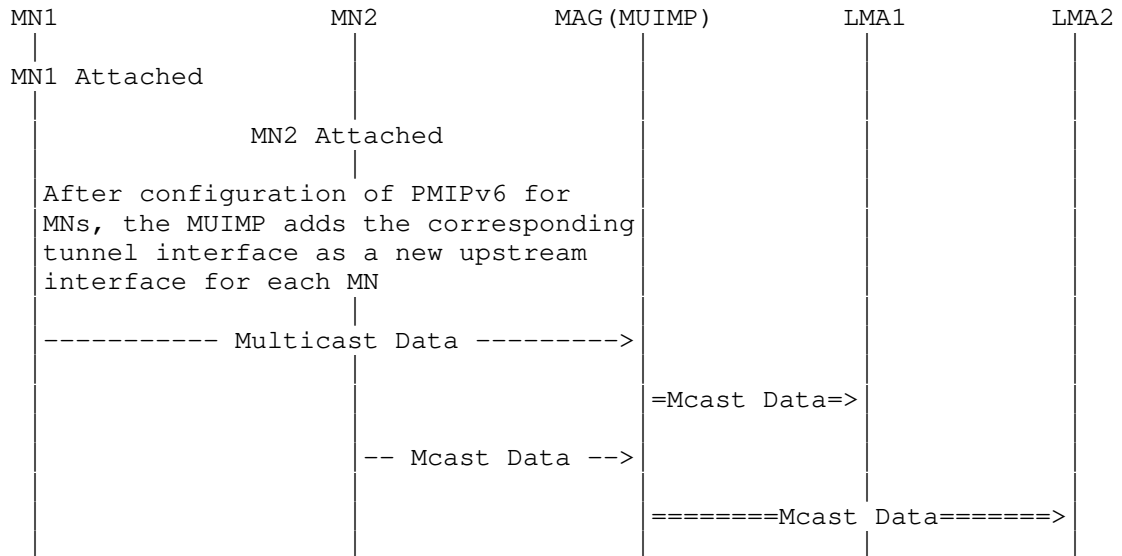


Figure 3: Mobile Node Attachment (MUIMP) - Signaling Call Flow

3.2. Data transmission after tunneling

After the processing in Section 3.1, the multicast data arrives at the LMA through the PMIPv6 tunnel and the subsequent data transmission is illustrated in detail as follows.

When the LMA can conduct the DR function, the data transmission procedures are described as follows.

In the scenario of ASM, the multicast receivers send the (*,G) join message to the RP to establish the RPT from the RP to the receivers. In this case, the LMA allows a mobile source to continuously send data to the group through the LMA-MAG tunnel firstly. And then the packets are transmitted from the LMA to the RP through the source

registration and then delivered to the receivers according to the multicast routing protocols. When the MN hands over from one MAG to another, only the PMIPv6 tunnel is updated and the movement of source is transparent to the receivers.

When the data traffic of the multicast source exceeds a certain value of data rate, the RP sends a (HoA,G) 'connection' message to the DR/LMA to establish the SPT from the specific source to the RP. Then the LMA parses this message and establishes the related multicast state. And when the handover from the Rendezvous Point Tree (RPT) to the Shortest Path Tree (SPT) happens, the receivers send the join message (HoA,G) to join the SPT of the source, and then the LMA receives this message and establishes the related multicast state. In this way, the LMA-based SPT is established successfully and the subsequent multicast data flow will be transmitted through the LMA-based SPT. However, the path between the LMA and the MN is still used for the multicast packets transmission. Although the SPT handover finishes, the practical path is not the topological shortest path tree due to the existence of the PMIPv6 tunnel.

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, this message is delivered to the LMA firstly and then the LMA-based multicast SPT from the LMA to the receivers can be established. Accordingly, the SSM scenario with the LMA-based scheme is similar to the SPT handover in the ASM scenario with the LMA-based scheme. And the current SPT path is also not the topological shortest path tree due to the existence of PMIPv6 tunnel.

As described in RFC 4601 [11], 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 also the iif is identical to the Reverse Path Forwarding (RPF) interface. However, because the network prefix of the LMA's interfaces is not same with the HNP allocated to the mobile source, the check of the source's direct connection will not be successful and then the LMA may not perform the function of the DR for the source. And when the LMA can not conduct the DR function, some extensions on the LMA should be needed, which will be our future work for the multicast source mobility in PMIPv6.

4. Extensions of PMIPv6

The signaling messages and the related processing of basic PMIPv6 should be extended in order to notify the multicast source-related information from the MAG to the LMA.

In order to provide the multicast service during the MN's movement, the MAG must recognize that the attached MN is a multicast source and the corresponding multicast address must also be learned. These information can be learned by the MAG during the authentication phase for example. The particular procedure is out of this document.

When the MAG finds that the attached MN is a multicast source, it should send the extended PBU message to the LMA. In the extended PBU message, a one bit "S" flag is added and set to "1", which means the MN is a multicast source. The multicast address is contained in the Multicast address option when the "S" is set to "1".

4.2. LMA

When receiving the extended PBU message and finding the "S" flag is set to "1", the LMA should send back an extended PBA message with the "S" flag set to "1" to the MAG. And then the LMA establishes a tunnel to the MAG as specified in PMIPv6.

5. Format of signaling messages

5.1. PBU

The format of the PBU message is shown in Figure 4.

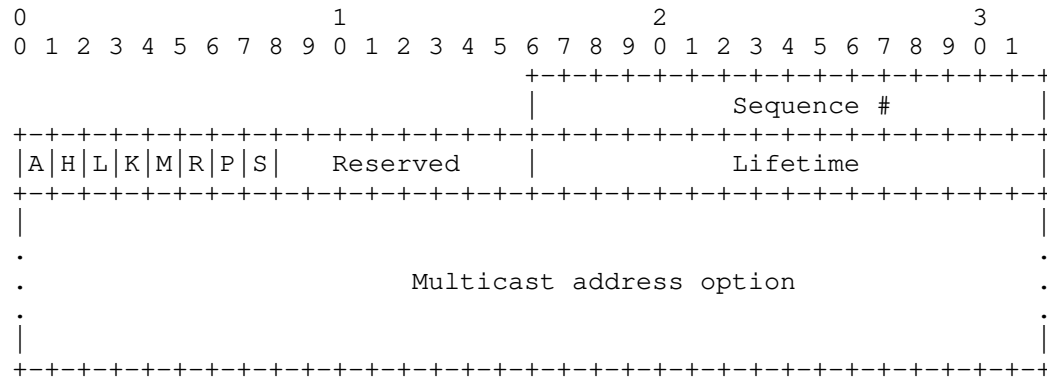


Figure 4: PBU Message Format

S flag and Multicast address option

Internet-Draft MSM Support in PMIPv6 Network July 2011
 1-bit "Multicast source identification" flag is used to identify whether this MN is a mobile multicast source. When this flag is set to "1", the related multicast address is attached in the Multicast address option.

5.2. PBA

The format of the PBA message is shown in Figure 5.

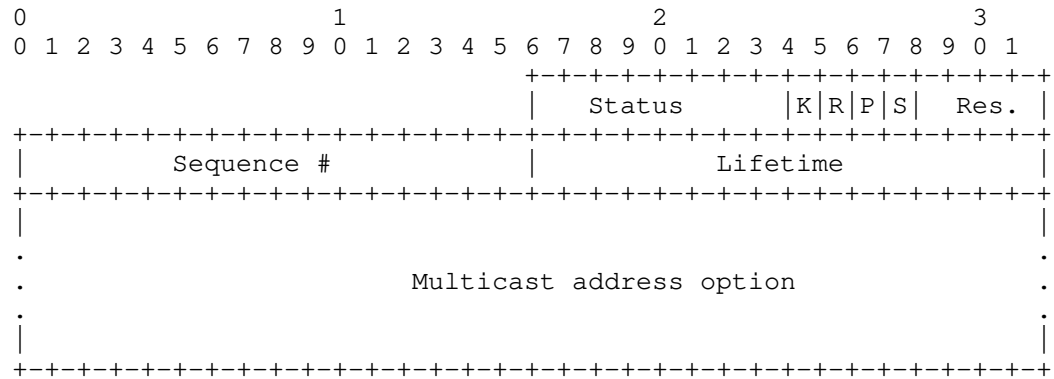


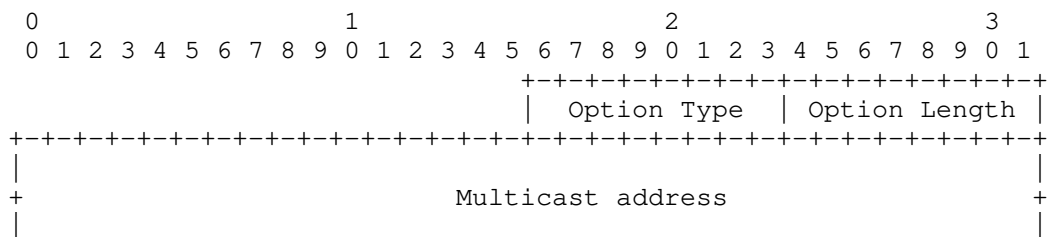
Figure 5: PBA Message Format

S flag and Multicast address option

1-bit "Multicast source identification" flag is used to identify whether this MN is a mobile multicast source. The flag is set to "1" only if the corresponding PBU had the S flag set to "1". And when this flag is set to "1", the related multicast address is attached in the Multicast address option.

5.3. Multicast address option

The format of Multicast address option is illustrated in Figure 6.



[illegible]

Figure 6: Multicast Address Option

Option Type

TBD

Option Length

8-bit unsigned integer indicating the length of the option in octets, excluding the option type and option length fields. This field can be set to 16 and 4 for the IPv6 and IPv4 multicast addresses, respectively.

Multicast address

The multicast address related to the multicast session provided by the MN.

6. Security Considerations

This document does not introduce any security considerations.

7. References

- [1] Gundavelli, et al.. "Proxy Mobile Ipv6", RFC5213, August 2008.
- [2] David B. Johnson, Charles E. Perkins and Jari Arkko. "Mobility Support in IPv6", RFC 3775, June 2004.
- [3] T C. Schmidt, M. Waehlich and S. Krishnan. "Base Deployment for Multicast Listener Support in PMIPv6 Domains", draft-ietf-multimob-pmipv6-base-solution-07, December 29, 2010.
- [4] H. Asaeda, P. Seite and J. Xia. "PMIPv6 Extensions for Multicast", draft-asaeda-multimob-pmip6-extension-04, September 9, 2010.
- [5] Seil Jeon and Younghwan Kim. "Mobile Multicasting Support in Proxy Mobile IPv6", draft-sijeon-multimob-mms-pmip6-02, March 4, 2010.

- [6] T C. Schmidt, M. Waehlisich, R. Koodli and G. Fairhurst. "Multicast Listener Extensions for MIPv6 and PMIPv6 Fast Handovers", draft-schmidt-multimob-fmipv6-pfmipv6-multicast-03, November 08, 2010.
- [7] K. Sato, M. Katsumoto, T. Miki. "Future vision distribution system and network", This paper appears in: IEEE International Symposium on Communications and Information Technology, 2004. ISCIT 2004, vol.1, pp: 274 - 279, October 2004.
- [8] 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.
- [9] T C. Schmidt, M. Waehlisich and M. Farooq. "Mobile Multicast Sender Support in PMIPv6 Domains with Base Multicast Deployment", draft-schmidt-multimob-pmipv6-base-source-00, March 28, 2011.
- [10] T. Schmidt, M. Waehlisich and S. Krishnan. "Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains", RFC 6224, April 2011.
- [11] B. Fenner, M. Handley, H. Holbrook and I. Kouvelas. "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.

Hong-Ke Zhang, Zhi-Wei Yan, Shuai-Gao, Li-Li Wang
National Engineering Lab for NGI Interconnection Devices
Beijing Jiaotong University, China

Phone: +861051684274
Email: hkzhang@bjtu.edu.cn
 06120232@bjtu.edu.cn
 shgao@bjtu.edu.cn
 liliwang@bjtu.edu.cn

Qian Wu, He-Wu Li
Network Research Center
Tsinghua University, China

Phone: +861062772375
Email: wuqian@cernet.edu.cn
 lihewu@cernet.edu.cn

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

MULTIMOB Group
INTERNET-DRAFT
Intended Status: Standards Track
Expires: May 2, 2012

J. C. Zuniga
(InterDigital Communications, LLC)
L. M. Contreras
(Telefonica I+D)
C. J. Bernardos
(Universidad Carlos III de Madrid)
S. Jeon
Y. Kim
(Soongsil University)
October 30, 2011

Multicast Mobility Routing Optimizations for Proxy Mobile IPv6
<draft-zuniga-multimob-pmipv6-ropt-01.txt>

Abstract

The MULTIMOB group has specified a base solution to support IP multicasting in a PMIPv6 domain [RFC6224]. In this document, some enhancements are proposed to the base solution. 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 deployments scenarios.

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) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

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

Table of Contents

1	Introduction	4
2	Conventions and Terminology	4
3	Multicast Tree Mobility Anchor (MTMA)	5
3.1	Architecture	6
3.2	Deployment Scenarios	7
3.2.1	PMIPv6 domain with ratio 1:1	8
3.2.2	PMIPv6 domain with ratio N:1	8
3.2.3	PMIPv6 domain with ratio 1:N	10
3.2.4	PMIPv6 domain with H-LMA	11
3.3	Multicast Establishment	14
3.4	Multicast Mobility	15
3.5	PMIPv6 enhancements	16
3.5.1	New Binding Update List in MAG	16
3.5.2	Policy Profile Information with Multicast Parameters	17
3.5.3	MAG to MTMA attach requirements	17
3.5.4	Data structure stored by MTMA	17
3.6	Advantages	17
4	Direct routing	21
4.1	MAG as MLD proxy	22
4.1.1	Local subscription when the MAG implements MLD proxy functionality	22
4.1.1.1	Local subscription architecture	22
4.1.1.2	Handover procedure for local routing	23
4.1.2	Remote subscription when the MAG implements MLD proxy functionality	24
4.2	MAG as multicast router	25
4.2.1	Local subscription when the MAG implements a multicast routing protocol	25
4.2.2	Remote subscription when the MAG implements a multicast routing protocol	25
5	Dynamic selection of local versus remote multicast subscription	25
5.1	Any source multicast scenario	26
5.2	Source specific multicast scenario	26
6	Security Considerations	27
7	IANA Considerations	27
8	Contributors	27
9	References	27
9.1	Normative References	27
9.2	Informative References	28
	Author's Addresses	29

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 does 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.

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 [RFC4605] allows an intermediate (edge) node to appear as a multicast router to downstream hosts, and as a host to upstream multicast routers. IGMP and MLD related protocols 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 a multiple of PMIPv6 tunnels with LMAs. Hence, when IP multicasting is applied into PMIPv6, it leads to redundant traffic at a MAG called "Tunnel Convergence problem". To address this issue, two enhancements are proposed in this document; multicast anchor and direct routing. The former uses a multicast tree mobility anchor (MTMA) as the topological anchor point for delivering multicast traffic, while the latter uses direct routing, allowing a MAG to connect directly to a multicast router for simple access to local content. Both schemes have no impact on the MN to support multicast listener mobility.

The MTMA architecture and solution are described in section 3. Section 4 describes the direct routing solution and the enhancements details. Section 5 describes the details about the selection at the MAG between direct routing (e.g. for local access) and MTMA (e.g. for remote access).

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 [RFC2119].

This document uses the terminology defined in [RFC5213], [RFC3775], 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 in such a way that an MN using that service is not aware of mobility as it moves from one MAG to another associated to that LMA regarding its 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.

- Direct routing: it uses native multicast infrastructure for retrieving multicast data. For the operator having its own local content, this technique also includes the case that content source is directly connected to a MAG.

This means 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 exclusively.

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

3 Multicast Tree Mobility Anchor (MTMA)

A PMIPv6 domain may handle data from both unicast and multicast sources. This document addresses optimizations to the base solution

specified for multicast support in PMIPv6 domains [RFC6224] by firstly introducing a complementary network entity, named multicast tree mobility anchor (MTMA), and defining the architecture and protocol flows derived from it; and secondly by defining a direct routing option where a MAG can directly receive packets from a multicast router.

An MTMA can be used to serve as the mobility anchor for multicast traffic. 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.

This section describes how the MTMA works in scenarios of MN attachment and multicast mobility. We first concentrate on the case of both LMA and MTMA defining a unique PMIPv6 domain, and then different deployment scenarios are presented.

3.1 Architecture

Figure 1 shows an example of a PMIPv6 domain supporting multicast mobility. LMA1 is dedicated to unicast traffic, and MTMA1 is dedicated to multicast traffic. The tree mobility anchor MTMA1 can be considered to be a form of upstream multicast router with tunnel interfaces allowing remote subscription for the MNs. Note that there can be multiple LMAs for unicast traffic (not shown in Figure 1) in a given PMIPv6 domain. Similarly, more than one MTMA can be deployed by the operator (not shown in Figure 1).

Also in this architecture, all MAGs that are connected to the MTMA must support the MLD proxy [RFC4605] function. Specifically in Figure 1, each of the MAG1-MTMA1 and MAG2-MTMA1 tunnel interfaces defines an MLD proxy domain. The MNs are considered to be on the downstream interface of the MLD proxy (in the MAG), and MTMA1 is considered to be on the upstream interface (of the MAG) as per [RFC4605]. Note that 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.

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, despite of that, this draft considers that every MN demanding multicast-only services is previously registered in a PMIPv6 unicast domain to get a unicast IP address. This registration can be required also for several purposes

such as remote management, billing, etc.

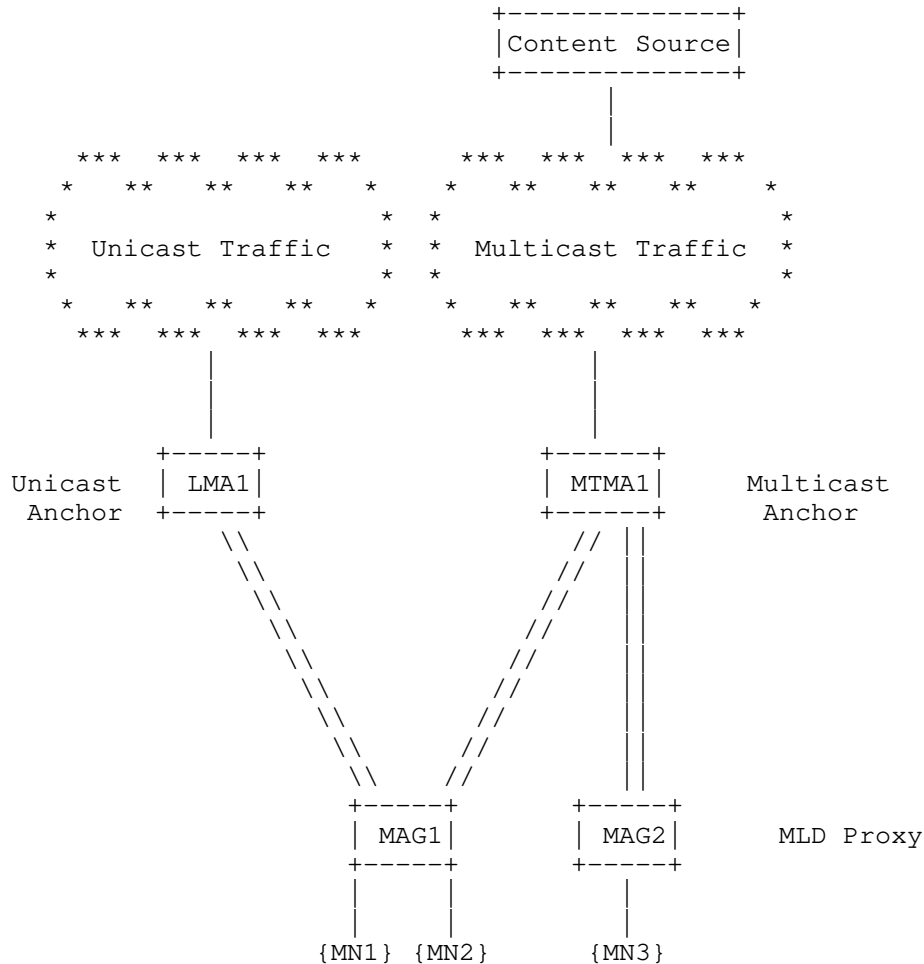


Figure 1. Architecture of Multicast Tree Mobility Anchor (MTMA)

3.2 Deployment Scenarios

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:

- 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).
- 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).
- 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.

3.2.1 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.

3.2.2 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 2 shows the scenario here described.

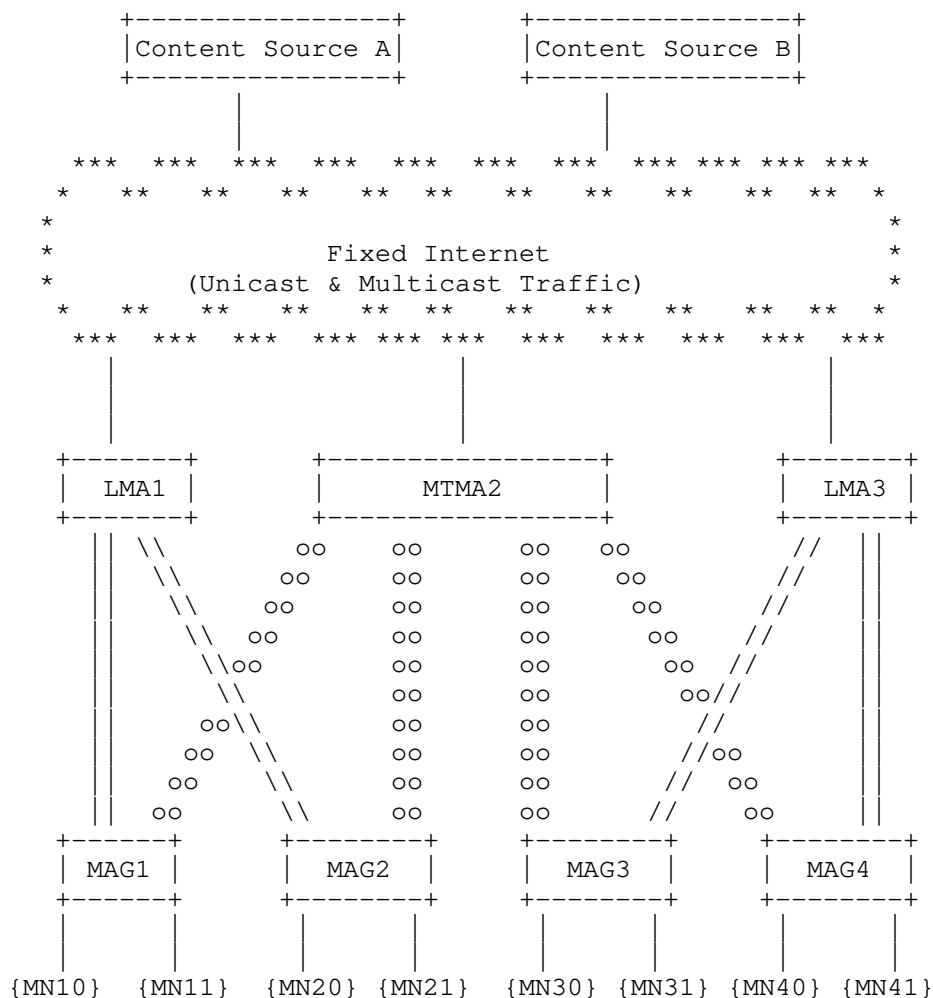


Figure 2. PMIPv6 domain with ratio N:1

The figure 2 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 ("ooo") 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.

3.2.3 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. Each particular MN association with the LMA and MTMAs (unicast and multicast respectively) remains always the same as it moves in the PMIPv6 domain.

Figure 3 shows the scenario here described.

The figure 3 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) or not. 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 each MN and the corresponding LMA and MTMA is permanently maintained.

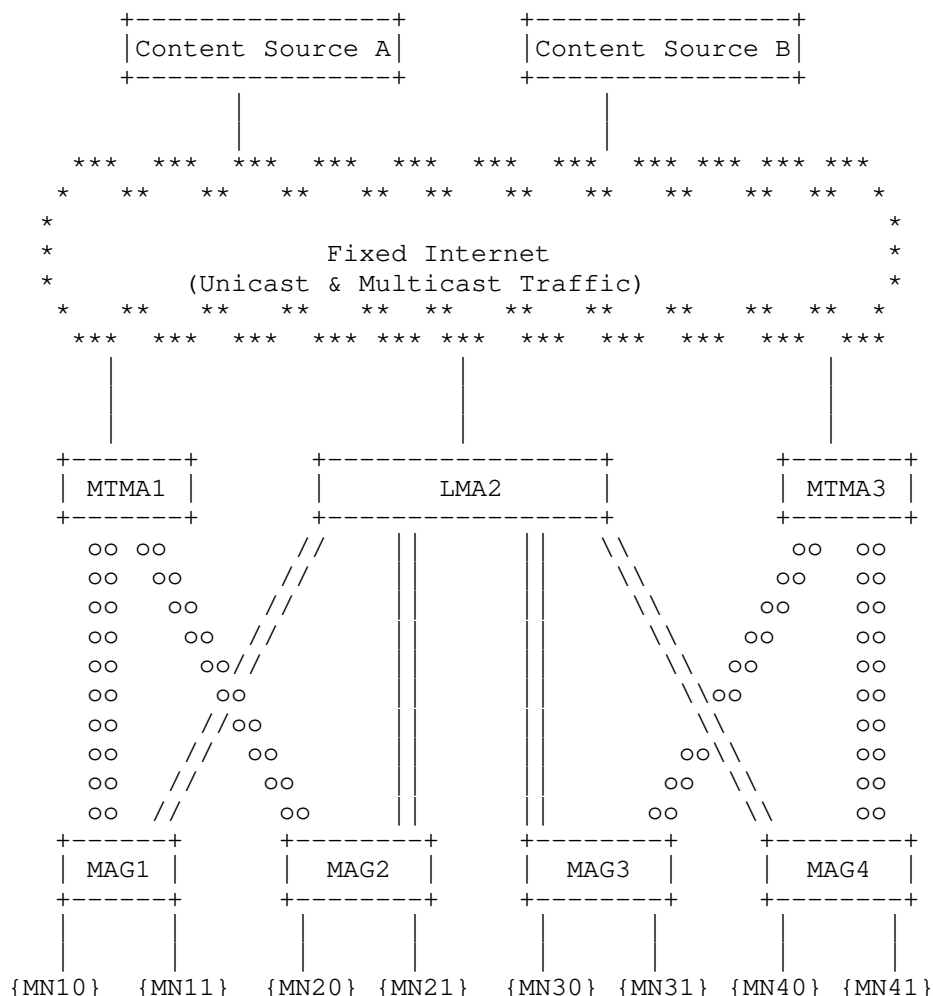


Figure 3. PMIPv6 domain with ratio 1:N

3.2.4 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 4 adapts the PMIPv6 domain with ratio N:1 scenario of figure 2 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 4 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.

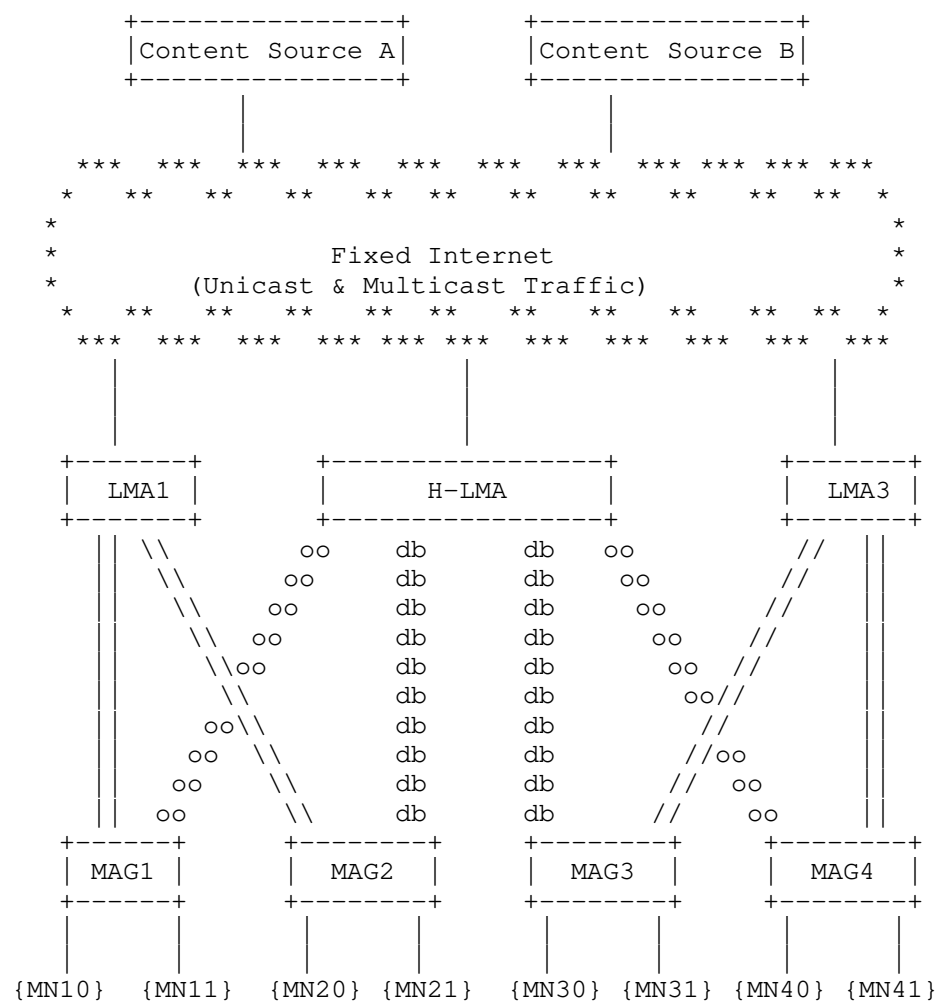


Figure 4. PMIPv6 domain with H-LMA

3.3 Multicast Establishment

Figure 5 shows the procedure when MN1 attaches to MAG1, and establishes associations with LMA (unicast) and MTMA (multicast).

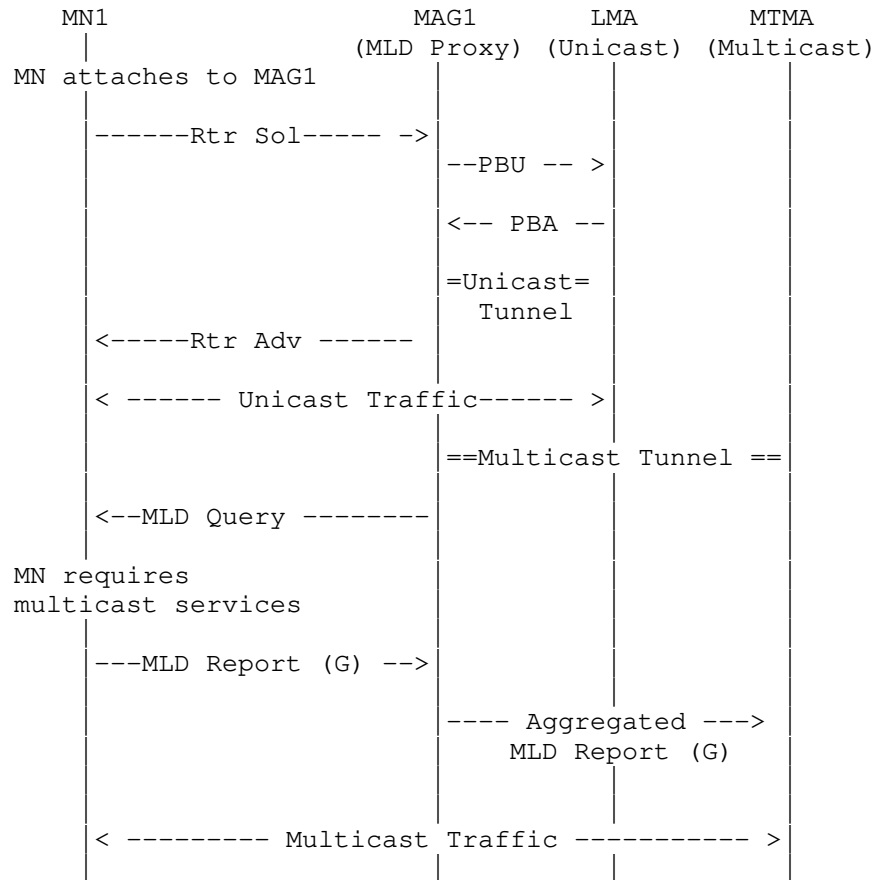


Figure 5. MN Attachment and Multicast Service Establishment

In Figure 5, MAG1 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 MAG1 and MTMA. Or the multicast tunnel 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 MAG1. MAG1 acting as a MLD Proxy as defined in [RFC4605] will then send an Aggregated MLD Report to the multicast anchor, MTMA (assuming that this is a new multicast group which MAG1 had not previously subscribed to). Multicast traffic will then flow from MTMA towards MN1.

3.4 Multicast Mobility

Figure 6 illustrates the mobility scenario for multicast traffic. Specifically, MN2 with ongoing multicast subscription moves from MAG1 to MAG2. Note that, for simplicity, in this scenario we only consider the tunnel of MAG2 with MTMA (for multicast traffic) and we assume that MN2 does not receive unicast traffic. Of course, if it was desired to support unicast traffic, this is served by a tunnel between MAG2 and LMA to transfer unicast traffic.

According to baseline solution signaling method described in [RFC6224], after MN2 mobility, MAG2 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 MN2 requests membership of a new multicast group (from MAG2's point of view), this will then result in an Aggregated MLD Report being sent to MTMA from MAG2. This message will be sent through a pre-established (or dynamically established) multicast tunnel between MAG2 and MTMA.

When MN2 detaches, MAG1 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, MAG1 may decide to keep the multicast tunnel for potential future use.

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

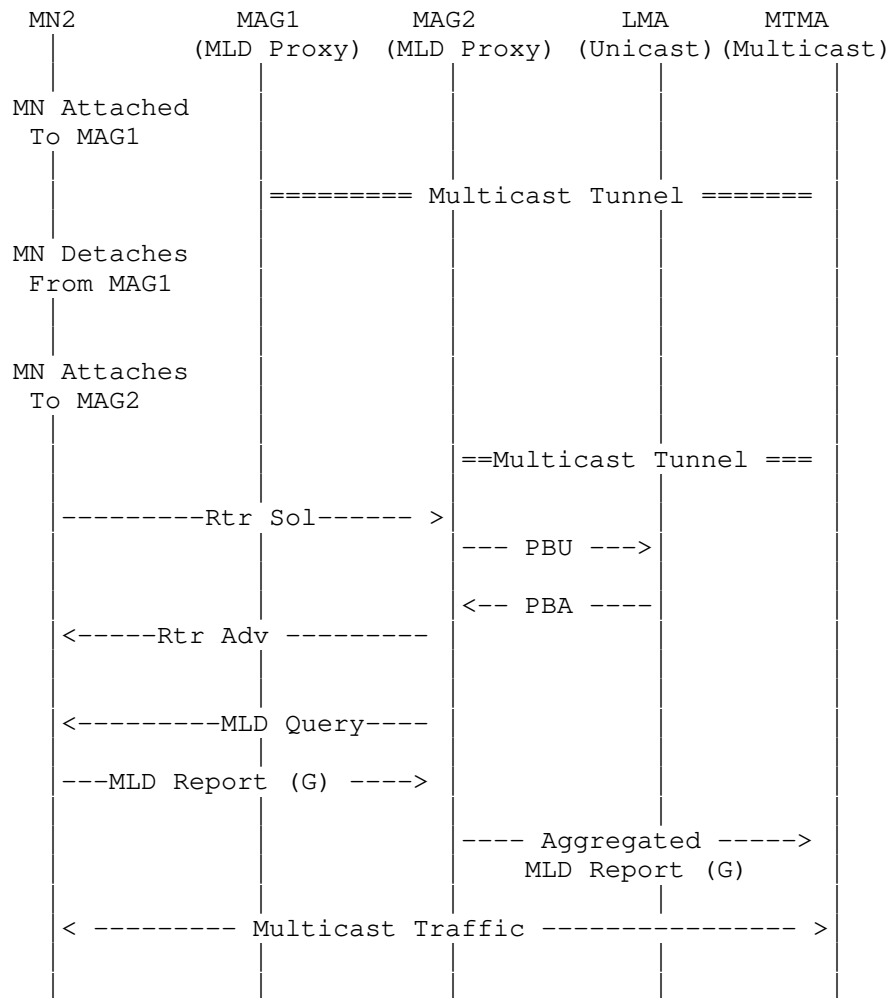


Figure 6. Multicast Mobility Signaling

3.5 PMIPv6 enhancements

This section describes the enhancements to the Proxy Mobile IPv6 [RFC5213] protocol required to support the MTMA architecture.

3.5.1 New Binding Update List in MAG

The Binding Update List 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.

3.5.2 Policy Profile Information with Multicast Parameters

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.

3.5.3 MAG to MTMA attach requirements

The MAG procedures must be updated to be able to handle simultaneous attach for a given mobile node to both the LMA and MTMA. For example, packets coming from a given mobile node must be screened to determine if it should be sent to the LMA or to the MTMA.

3.5.4. Data structure stored by MTMA

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 (as 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.

3.6 Advantages

An advantage of the proposed MTMA architecture is that it allows a PMIPv6 domain to closely follow a simple multicast tree topology for Proxy MLD forwarding (cf., sections 1.1 and 1.2 of [RFC4605]). In contrast, the combined unicast/multicast LMA as proposed in [RFC6224] will be a more complex set of trees.

Another advantage of the proposed dedicated multicast solution is that it allows a gradual network upgrade of a PMIPv6 domain to support multicast functionality. This is because the operator does not have to upgrade all the LMAs in the network to support multicast functionality. Only certain nodes (MTMAs), dedicated to multicast support, will have to be upgraded to support the new multicast functionality. Also, multiple deployment scenarios are supported as required by the operator for expected traffic distributions.

A final advantage is that a specific multicast elements minimize the replication of multicast packets (the Tunnel Convergence problem), in certain scenarios, compared to [RFC6224]. Figures 7 and 8 illustrate this point visually. For this simple scenario, it can be observed that the multicast MTMA topology (Figure 7) generates 6 packets for one input multicast packet. In comparison, the combined unicast/multicast LMA topology (Figure 8) generates 8 packets for one input multicast packet.

In general, it can be seen that the extra multiplication of packets in the combined unicast/multicast LMA topology will be proportional to the number of LMAs, and the number of MNs (in a given MAG) associated to different LMAs, for a given multicast group. The packet multiplication problem aggravates as more MNs associated to different LMAs receive the same multicast traffic when attached to the same MAG. Hence, the MTMA architecture significantly decreases the network capacity requirements in this scenario.

(Note that in Figure 7, it is assumed that MN1 and MN2 are associated with MAG1-LMA1, and MN3 is associated with MAG2-MTMA2 for multicast traffic. In Figure 8, it is assumed that MN1 is associated with MAG1-LMA1, MN2 is associated with MAG1-LMA2, and MN3 is associated with MAG2-LMA2 for multicast traffic. In both Figures 7 and 8, it is assumed that the packets are transmitted point to point on the last hop wireless link.)

Additional results can be found in [ERCIM], where both solutions are compared by simulation under realistic traffic conditions. It can be shown that, for multicast traffic, the number of channels that a node (LMA in the base solution, MTMA in the proposed multicast architecture) has to serve does not decrease linearly with the reduction of the number of MNs associated to that node. The key factor is the set of channels subscribed by the MNs. In fact, as the number of MNs increases in the PMIPv6 domain, we have less advantage for having several nodes serving multicast, as each of them will probably manage all the multicast channels (or at least the popular ones) anyway.

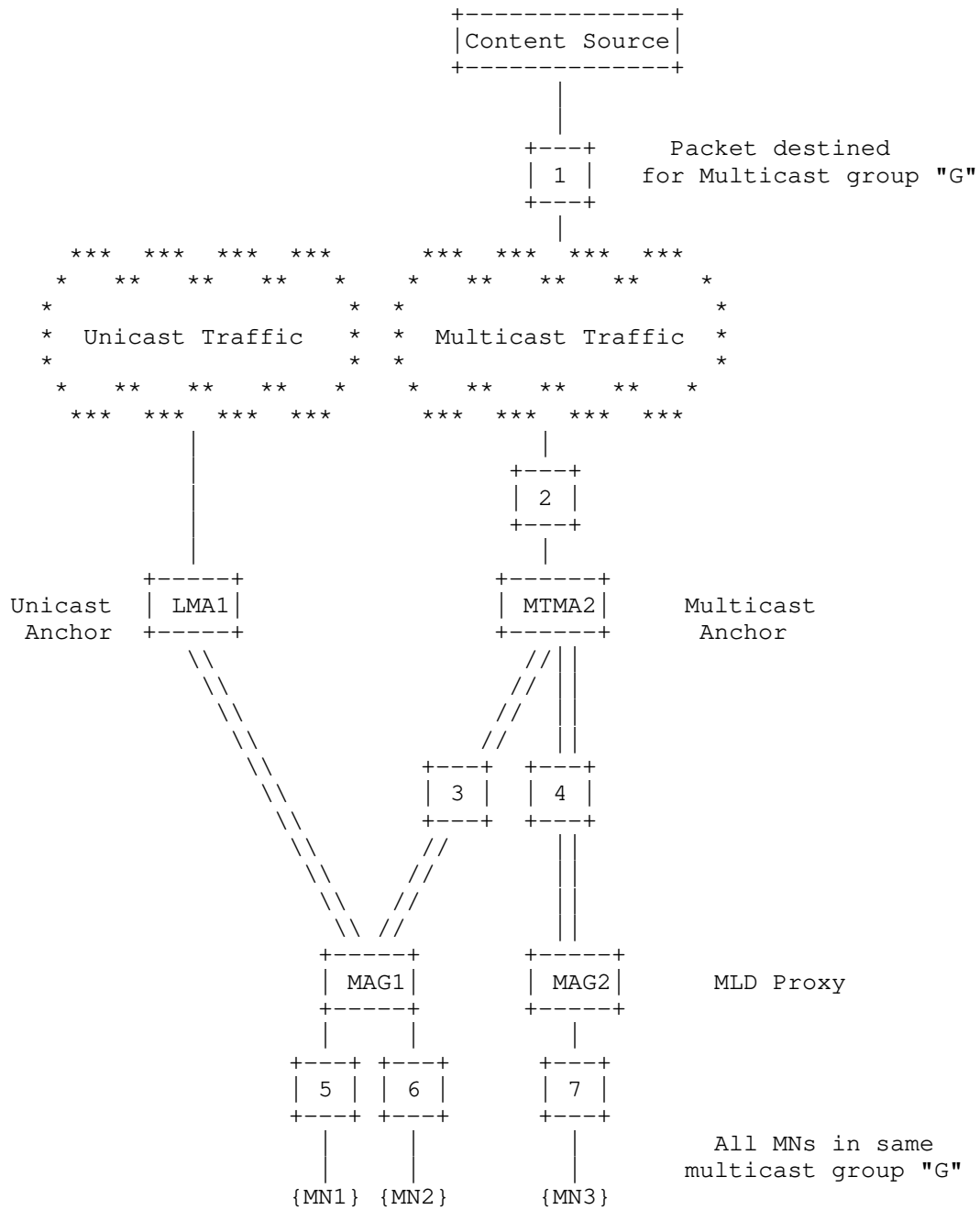


Figure 7. Packet Flow in the MTMA architecture

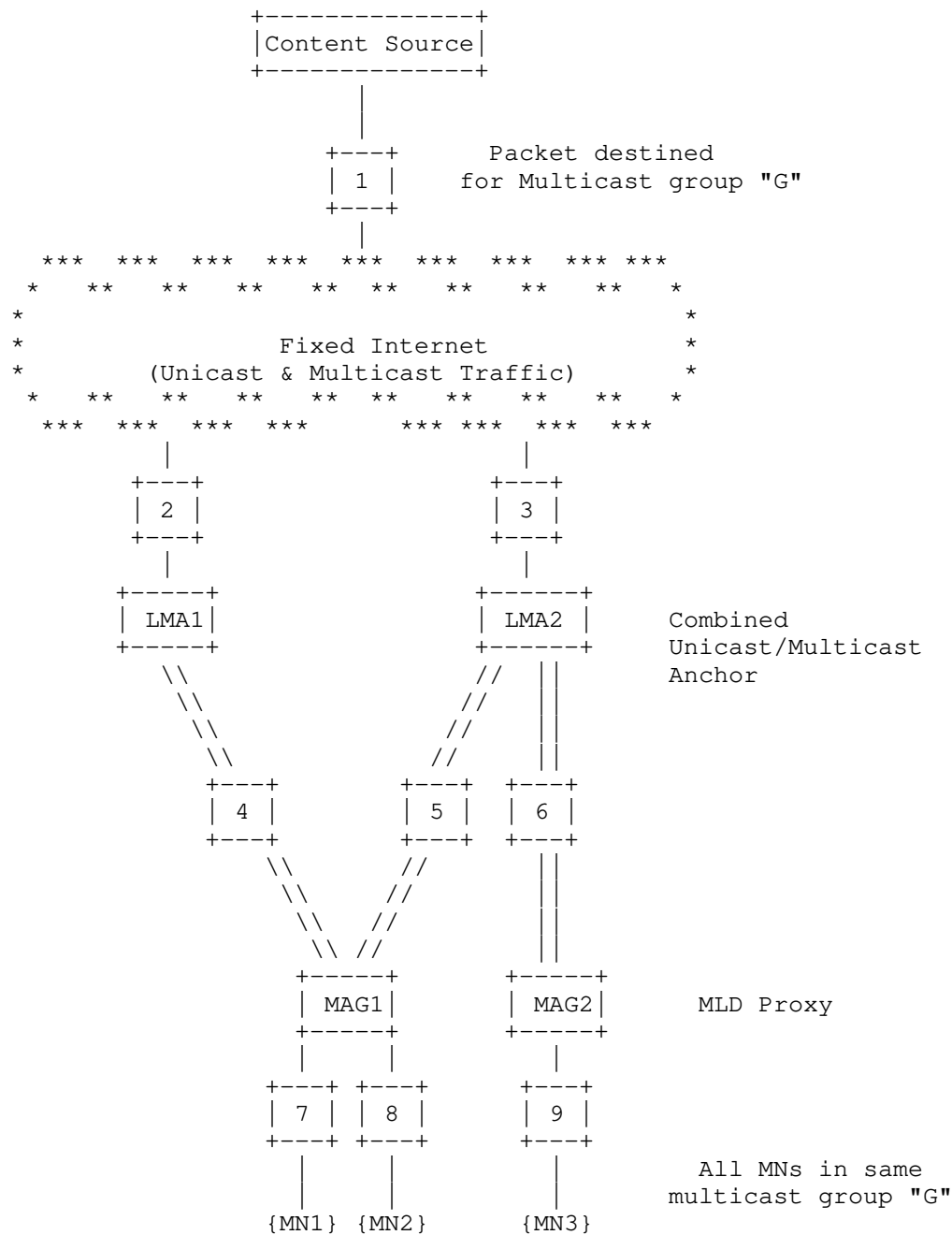


Figure 8. Packet Flow in a Combined Unicast/Multicast LMA

4 Direct routing

Direct routing uses native multicast infrastructure, allowing a MAG to connect a multicast router directly. A MAG can act as a MLD proxy or multicast router for redirecting multicast packets. The key idea of direct routing is to provide optimal routing for local content. As a consequence, it does not give the LMA processing burden for channel management and data delivery of locally available content. Direct routing is simple and easy to deploy.

When thinking on the MAG reception of the multicast flow being forwarded to the attached MNs, two models for the MAG subscription to the multicast flow (on behalf of the MNs) can be considered:

- Local subscription, which refers to the situation where the multicast channel is forwarded to the MAG by a multicast router within the PMIPv6 domain
- Remote subscription, which refers to the situation where the multicast channel is forwarded to the MAG through the tunnel interface from the home network

In the architecture described in [RFC6224], if MLD proxy is installed on a MAG, all MAGs that participate in the multicast traffic distribution in a PMIPv6 domain are considered to act as MLD proxies. An important consequence derived from such characterization is that every MLD proxy instance defined in the MAG has a unique upstream interface, and thus, an MLD proxy instance cannot dynamically choose among local or remote multicast subscription. For instance, one possible scenario pushing for local source deployment, and consequently local subscription, could be the one where there is an extremely high number of multicast channels, all of them with active subscriptions in all the MAGs along the PMIPv6 domain, resulting in the MTMA replicating the totally of the multicast flows to all the MAGs (leading to the known as "avalanche problem").

Once a decision is taken (at configuration time) about what kind of subscription, either local or remote, is applicable for a certain instance regarding all the multicast channels for all the attached MNs, this cannot be changed without resetting and reconfiguring the whole MLD instance.

In order to have such kind of flexibility, the MAG needs to act as a multicast router, that is, it must implement some multicast routing protocol able to choose between local or remote subscription, for one or all the subscribed multicast channels, by using some routing criteria leveraged by the network routing information or by the network management systems. The most commonly deployed multicast

routing protocol nowadays is PIM [RFC4601].

So it is possible to distinguish among two situations depending on the MAG functionality. The following sub-sections describe the applying constraints.

4.1 MAG as MLD proxy

In case of the MAG only incorporates MLD proxy functionality, for every one of the MLD proxy instances invoked in the MAG it is necessary to define at configuration time the upstream interface from where the multicast traffic will be received. This decision actually requires to define whether the multicast subscription by an MLD proxy instance for all the multicast channels will be local (if the upstream interface points to a multicast router internal to the PMIPv6 domain) or remote (in case of the upstream interface is the bi-directional tunnel towards the LMA, for the architecture in [RFC6224], or the MTMA, for the multicast listener optimization described in this document).

4.1.1 Local subscription when the MAG implements MLD proxy functionality

If the MAG has MLD proxy functionality only, once this MLD proxy instance is configured to obtain the multicast traffic locally, the system behavior when operating with local subscription remains static.

4.1.1.1 Local subscription architecture

Figure 9 shows the proposed local routing architecture using native multicasting infrastructure [I-D.deng-multimob-pmip6-requirement]. To forward IGMP/MLD signaling and multicast packets, a MLD proxy function defined in [RFC4605], SHOULD be placed on a MAG. This solution is much simpler than the base solution and easy to deploy because multicasting functions are totally separated from mobility anchor by using a native multicasting infrastructure.

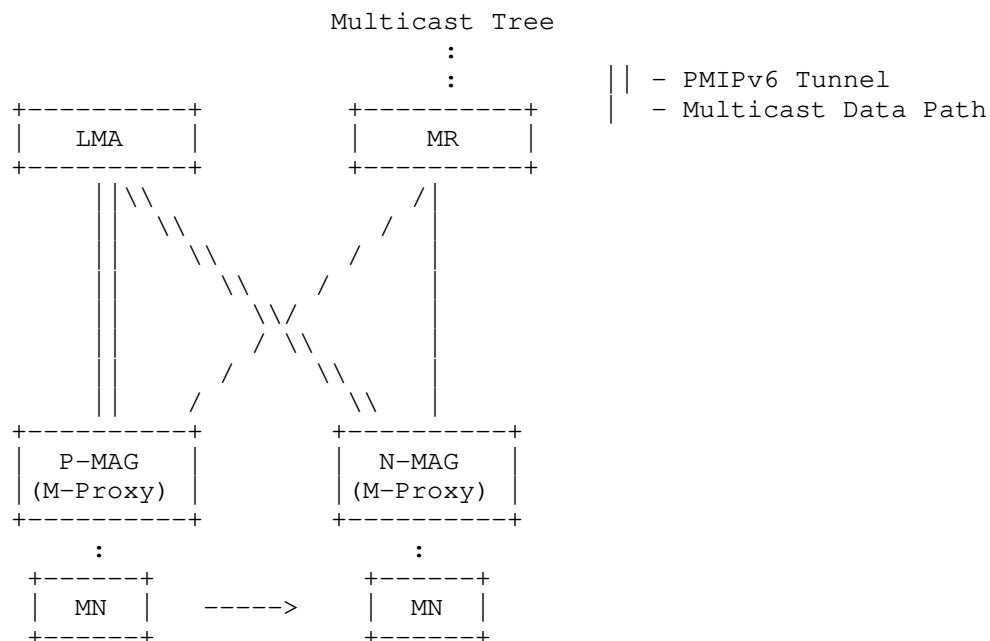


Figure 9. Direct routing solution for PMIPv6 Multicasting

4.1.1.2 Handover procedure for local routing

Figure 10 shows the handover operation in local routing architecture. When an MN hands off to the next MAG (N-MAG) from the previous MAG (P-MAG), the N-MAG detects the newly arrived MN and 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 MR. 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.

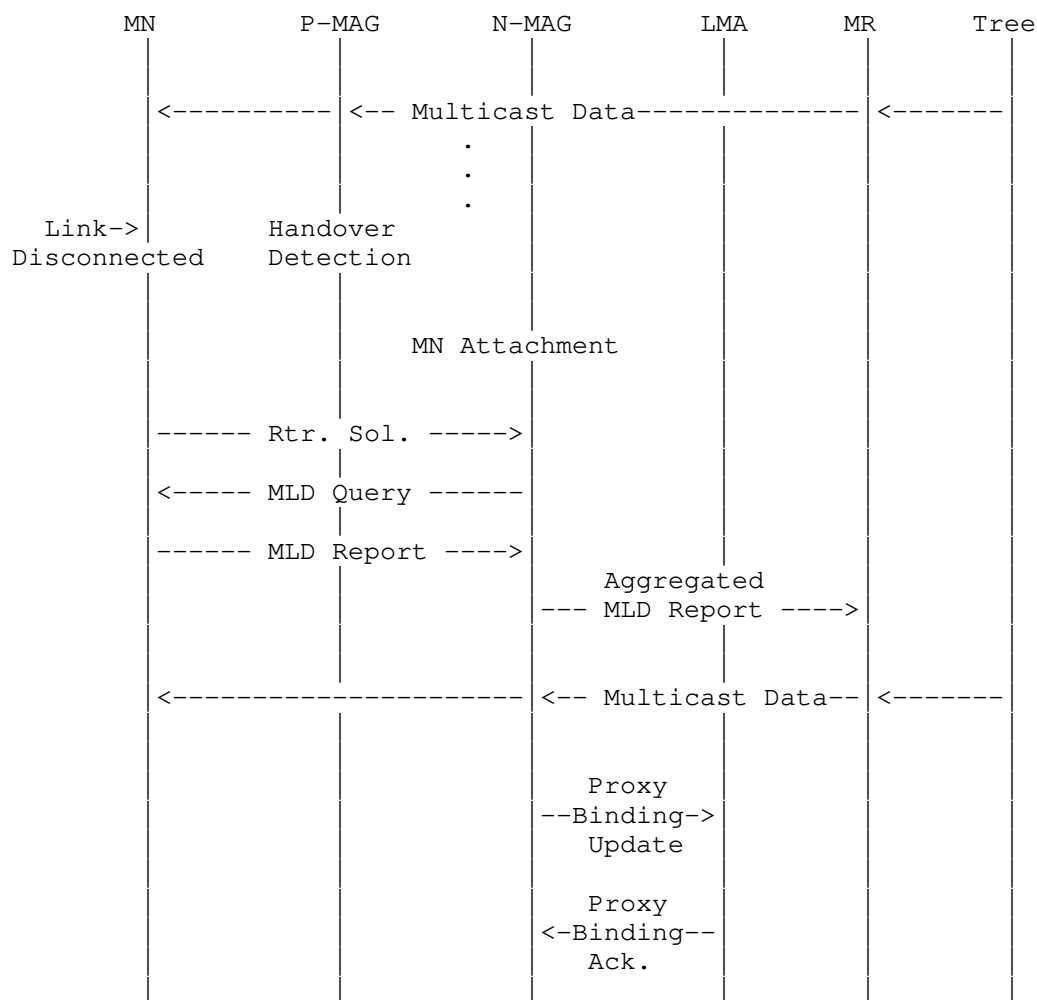


Figure 10. Handover procedure in direct routing architecture

4.1.2 Remote subscription when the MAG implements MLD proxy functionality

If the MAG has only MLD proxy functionality, the system behavior when operating with remote subscription is as described in chapter 3. Once the MLD proxy instance is configured to obtain the multicast traffic remotely, this remains static.

4.2 MAG as multicast router

If the MAG behaves as a multicast router, the MAG then implements a multicast routing protocol. This allows the MAG to make decisions about from where to receive the traffic of any multicast channel, based in routing information and/or network management criteria. The selected incoming interface for receiving multicast traffic will be then the one matching such criteria, and it could drive to either a local or remote subscription. Some situations are introduced in the next section.

4.2.1 Local subscription when the MAG implements a multicast routing protocol

If the MAG is a multicast router, the system behavior when operating with local subscription is as before, but extending the role of the MAG to be a multicast router, and running a multicast routing protocol among the MAG and local multicast router serving the multicast traffic. Once the MAG decides to obtain the multicast traffic locally based in routing information and/or network management criteria, this can be dynamically changed if such criteria change.

4.2.2 Remote subscription when the MAG implements a multicast routing protocol

If the MAG is a multicast router, the system behavior when operating with remote subscription is as described in chapter 3, considering that a multicast routing protocol is running among the MAG and the MTMA on the tunnel interface. Once the MAG decides to obtain the multicast traffic remotely based in routing information and/or network management criteria, this can be dynamically changed if such criteria change.

5 Dynamic selection of local versus remote multicast subscription

As mentioned above, the MAG as multicast router provides some flexibility for choosing local versus remote multicast subscription. Considering PIM as the multicast routing protocol running on the MAG, it is possible to find out two situations where such dynamic selection can occur, according to the PIM flavor on place. For all the scenarios below we consider a certain multicast flow being injected by two different sources, one local to the PMIPv6 domain and one remote through the home network, by using an MTMA.

5.1 Any source multicast scenario

This situation applies for both PIM-SM and BIDIR PIM variants. In this case, once the MAG receives the MLD report from the MN requesting the multicast channel in the form (*,G), the MAG could decide what multicast flow subscribes to (the local or the remote one).

The subscription can be statically pre-configured or dynamically configured based on some rule. For instance, static configuration can be made per MN (user), such as "multicast traffic from user X should always go through the home (i.e., via the tunnel with the MTMA/LMA-as-per-RFC6224), while traffic from user Y should go via local subscription". Also, configuration profiles can also be more complex and include considerations on types of traffic or IP flows, such as "traffic of type A from user X should always go through the home, traffic of type B from user X should be subscribed locally" using routing information and/or network management criteria. Similarly, routing information can be received dynamically, for example, at user's registration time PBU/PBA signaling can be used to carry the profile information similar to what is described in [I-D.gundavelli-netext-pmipv6-sipto-option]. Also, routing information can be exchanged dynamically when the multicast group subscription is made.

When focusing on PIM-SM, another scenario is possible. PIM-SM allows for switching from a multicast shared-tree to a source-specific tree to optimize the path for traffic delivery. The location of the rendezvous point and the multicast source can be either in the PMIPv6 domain or the home network, so the optimization could be from local subscription to remote subscription or vice versa. The possibility of switching to a source-based tree, and the time for doing is implementation-dependent, and it could be triggered immediately (after reception of the first multicast packet) or last to some time, or even not switching never.

5.2 Source specific multicast scenario

This situation applies for PIM-SSM. Then, in a source-specific multicast scenario [RFC4607], the MAG would send the PIM request to the corresponding interface based on the multicast source address indicated on the (S,G) subscription requested by the MN in the MLD Report, using the routing information.

6 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].

7 IANA Considerations

This document makes no request of IANA.

8 Contributors

The following people have considerably contributed to this draft:

Akbar Rahman
InterDigital Communications, LLC
Email: Akbar.Rahman@InterDigital.com

Ignacio Soto
Universidad Politecnica de Madrid
Email: isoto@dit.upm.es

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.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [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.
- [RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.
- [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.

- [RFC5847] Devarapalli, V., Koodli, R., Lim, H., Kant, N., Krishnan, S., Laganier, J., "Heartbeat Mechanism for Proxy Mobile IPv6", RFC 5847, June 2010.
- [RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.
- [RFC4607] Holbrook, H., and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.

9.2 Informative References

- [RFC6224] Schmidt, T.C., Waehlich, M., and S.Krishnan, "Base Deployment for Multicast Listener Support in PMIPv6 Domains", RFC 6224, April 2011.
- [ERCIM] L.M. Contreras, C.J. Bernardos, I. Soto, "On the efficiency of a dedicated LMA for multicast traffic distribution in PMIPv6 domains", 5th ERCIM Workshop in eMobility, Vilanova i la Geltru, Spain, June 2011.
- [I-D.deng-multimob-pmip6-requirement] H. Deng, T. Schmidt, P. Seite, and P. Yang, "Multicast Support Requirements for Proxy Mobile IPv6", draft-deng-multimob-pmip6-requirement-02.txt (work in progress), July 2009.
- [I-D.gundavelli-netext-pmipv6-sipto-option] S. Gundavelli, X. Zhou, J. Korhonen, G. Feige, R. Koodli, "IP Traffic Offload Selector Option for Proxy Mobile IPv6", draft-gundavelli-netext-pmipv6-sipto-option-01.txt (work in progress), July 2011.

Author's Addresses

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

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

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

Seil Jeon
Soongsil University
Email: sijeon@dcn.ssu.ac.kr

Younghan Kim
Soongsil University
Email: yhkim@dcn.ssu.ac.kr