Mobile Multicast Requirements on IGMP/MLD Protocols

draft-liu-multimob-igmp-mld-mobility-req-01

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of 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/1id-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 April 16, 2009.
Abstract

This document presents the requirements for IGMP/MLD protocols to allow the deployment of mobile multicast service. It is intended to provide useful guideline when adapting current IGMP/MLD protocols to support terminal mobility.
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 [1].

Table of Contents

1. Introduction ................................................. 4
2. Problem Statement ........................................... 5
3. The Behavior of IGMP and MLD Protocols ........................ 7
   3.1. IGMP Version 1 ........................................ 7
   3.2. IGMP Version 2 ........................................ 7
   3.3. IGMP Version 3 ........................................ 8
   3.4. Multicast Listener Discovery Protocols ................... 9
   3.5. Lightweight IGMPv3/MLDv2 ............................... 9
4. Requirements for IGMP/MLD to Support Mobile Multicast .......... 10
   4.1. Functional Requirements for Mobile Multicast .......... 10
   4.2. Requirements on Tuning IGMP/MLD Protocol Parameters .... 10
   4.3. Requirements for Handover ................................ 11
   4.4. Requirements for Point-To-Point Link .................... 12
   4.5. Requirements for Explicit Tracking ...................... 12
5. Security Considerations ...................................... 13
6. References .................................................. 14
   6.1. Normative References .................................. 14
   6.2. Informative References ................................. 14
Authors’ Addresses .............................................. 15
Intellectual Property and Copyright Statements .................. 16
1. Introduction

IP multicast efficiently distributes data to a number of receiver hosts in IP networks simultaneously thereby saving network and server resources. The receiver hosts use IGMP for IPv4 [2] and MLD for IPv6 [3] to receive or to stop receiving data via multicast (using join/leave or a subscribe/unsubscribe requests). The intermediate routers construct multicast tree between the source and receiver hosts with multicast routing protocols.

IGMP and MLD protocols work on broadcast shared links and point-to-point links. These protocols can also work on a wireless link. However, it is necessary to consider how to make a router and mobile hosts using IGMP and MLD protocols better fit the properties of a wireless link. In this document, the requirements for IGMP and MLD protocols that enable mobile multicast services via a wireless link are discussed. This document mainly focuses on IEEE 802.11 and 802.16 as the target wireless link to adapt the requirements for the general use, whereas 3GPP or 3GPP2 might be the additional target in the revised version of this document.

Receiver mobility is the target of this document, because it has more promising application scenarios and exhibits less deployment complexity. In addition, in IP multicast the IGMP/MLD protocols describe the interaction between multicast receivers and their first hop routers, sources do not require IGMP/MLD support unless they are also receivers, and so there is not expected to be any IGMP/MLD requirements for multicast source or network mobility.

IGMP or MLD protocol can work with any mobile protocols (e.g., MIPv6 [9], PMIPv6 [10], NEMO [11]) independently, if these protocols support multicast. However, context transfer or other procedures to provide seamless handover depend on the mobile protocols. Therefore, this document does not assume mobile protocols that mobile hosts use, and only protocol-independent considerations and requirements regarding how mobile protocols should work with IGMP/MLD for seamless handover are discussed.
2. Problem Statement

A mobile host usually accesses to a network via a wireless link. When a mobile host wants to join or leave an IP multicast session, it sends IGMP/MLD messages for the request to its upstream equipment. The upstream equipment may be a wireless access router (in case of MIPv6), a mobile router (in case of NEMO), a gateway (in case of PMIPv6), or a switch or router that supporting IGMP/MLD Proxy. In the following part of this document, it is expressed as an "upstream router" or "multicast router".

The upstream router should maintain all group membership states indicating which multicast sessions mobile hosts have joined on a wireless LAN. In many cases, current upstream wireless routers and switches do not maintain this information and flood all multicasts received onto each wireless LAN, which is not an efficient use of wireless bandwidth.

According to the properties of a wireless link, bandwidth usage and packet loss should be carefully considered. It is also necessary to take care of battery consumption of a mobile host. These conditions encourage the minimization of exchanged data packets and control messages including IGMP/MLD protocol messages if possible.

On the other hand, IGMP and MLD are asymmetric and non-reliable protocols; multicast routers need solicited membership reports by periodical IGMP/MLD Queries, in order to be robust in front of host or link failures and packet loss. It is encouraged that host-and-router communication is effectively coordinated to support limited wireless or terminal resources.

When a host receiving multicast data moves from an access link to another access link, the host wants to continuously receive the multicast data without any packet loss and session interruption, and the network provider wants to minimize the amount of duplicated multicast traffic. This seamless handover is a necessary component of mobile multicast communication, which introduces additional requirements on IGMP/MLD protocols during handover. Precisely, the moving host’s membership information should be transmitted to the new access link as quickly as possible. This procedure reduces the host’s join latency. Or, if there is no member host on the access link after the host moves, then the upstream router should leave from the multicast session quickly as well. This contributes to releasing the unnecessary resources.

In the following sections of this document, we briefly introduce the IGMP/MLD protocols, analyze the protocol behavior and the requirements of IP multicast mobile service, and discuss the
possibility of the modification or extension of the protocols if needed. The illustration below will consider both IPv4 and IPv6 networks.
3. The Behavior of IGMP and MLD Protocols

A multicast receiving host using IGMP protocols to join and leave a multicast group on an IPv4 network, and using MLD protocols on an IPv6 network.

3.1. IGMP Version 1

IGMP Version 1 [5] defines the basic operating model between a multicast receiving host and its upstream router to determine group membership. The router periodically sends Host Membership Queries to its attached network. A host sends a Host Membership Report to the router when it decides to join a group, or it responds to the Queries passively.

IGMPv1 introduces two specific mechanisms to avoid the implosion of concurrent reports when the host answers the Query—delaying response and report suppression. Delaying response means when a host receives the Query, it does not respond with a report immediately, but rather waits a random period of time. Report suppression means the host will withdraw its own report when it hears a report scheduled to be sent from other host joining the same group. It contributes to minimizing the number of responses but is impossible for the multicast router to track per host’s membership status by reports.

An IGMPv1 host does not send group leave message explicitly. It silently leaves the group by ignoring a Host Membership Query, which causes an undesirably long leave latency.

IGMPv1 is an obsolete protocol; hence it is not recommended for mobile hosts to implement IGMPv1, whereas upstream routers may need to support IGMPv1 to keep compatibility with non-upgraded mobile hosts.

3.2. IGMP Version 2

IGMP Version 2 [6] makes a series of optimizations to improve the protocol behavior. An IGMPv2 host can explicitly send a Leave Report when it decides to stop receiving multicast data. This enables fast leave from the multicast group. When a multicast router receives a leave message, it will generate a Group-Specific Query specifying the multicast group address in order to recognize whether there is other receiver for the same group on its network. IGMPv2 also supports the case when multiple multicast routers are connected to the same network. In this case, a single Querier is elected by ordering the IP addresses to take on the duty of sending Query packets.
Several timers are defined for IGMPv2 operations and these values are configurable. Query Interval is the interval between General Queries sent by a router, which has influence on the total number of IGMPv2 messages on a link. Query Response Interval is the maximum response time of a report after a host receives the General Query. It will reduce the bursty traffic of the reports on a link. Startup Query Interval is the interval between the queries sent by the Querier in startup. Last Member Query Interval is the maximum response time used by Group-Specific Queries in response to leave from session. This value can be tuned to modify the leave latency of the network.

IGMPv2 also introduces timer related counters to make the protocol function more robust. For example, it defines Robustness Variable to quantify the number of reports sent out to prevent packet loss. Last Member Query count is used to set the number of Group-Specific Queries sent before the router assumes there is no local member. Startup Query Count is the number of Queries issued on startup. These values can be tuned according to the expected packet loss on a link.

3.3. IGMP Version 3

IGMP Version 3 [2] introduces a big enhancement to the previous two versions. It defines INCLUDE and EXCLUDE filter mode on both the host and router side. With the filter mode, a host can specify the desired or undesired source address(es) and multicast address(es) in IGMP report messages.

IGMPv3 router uses filter mode to process the group record properly. The router also maintains a group-timer to indicate the filter mode switch over and a source-timer to time each valid source. A new type of Source-and-Group-Specific Query is utilized to verify there are no receivers desiring to receive traffic from listed sources for a particular group, which has been requested to no longer be forwarded.

Another modification is that IGMPv3 does not adopt the report suppression mechanism, because the various packet type and the diverse information carried in the report make it rather difficult to define a uniform suppression policy. Without suppression, the number of report messages may increase greatly on a link. IGMPv3 solves this problem by make pending reports or queries merged into a combined packet.

An advantage of eliminating report suppression is that it provides the possibility for the router to keep track of host membership status on a link. This Explicit Tracking consumes memory on the router, but provides feasibility to manage end users.
3.4. Multicast Listener Discovery Protocols

MLDv1 and MLDv2 are respectively derived from IGMPv2 and IGMPv3 to be used for IPv6 host and router. The important difference between MLD and IGMP is that MLD is a sub-protocol of ICMPv6 and its message types are a subset of ICMPv6 messages. For MLDv1 parts of the message types are renamed to distinguish from those of IGMPv2.

3.5. Lightweight IGMPv3/MLDv2

IGMPv3 and MLDv2 enable the support of Source-Specific Multicast (SSM) communication [8] by indicating desired sources in the INCLUDE Group Record. Its usage of excluding undesired sources by an EXCLUDE filter mode operation has little practical prototype use and no desired use case. Moreover, when a host requests to join or leave session whose operation changes INCLUDE filter mode to EXCLUDE filter mode or vice versa, both the host and the upstream router cause complex state transition and scalability problems.

In [4], simplified version protocols of IGMPv3/MLDv2 are defined to keep the INCLUDE source-filtering characteristics to support SSM communication and remove the EXCLUDE filter mode operation. Not only are LW-IGMPv3 and LW-MLDv2 compatible with the standard IGMPv3 and MLDv2, but also the protocol operations made by hosts and routers or switches (performing IGMPv3/MLDv2 snooping) are simplified by reducing the complex processes and the scalability problems. The number of report types are reduced, and the host-side kernel implementation and the router’s operation are greatly simplified. Besides, less states need to be stored by lightweight router compared to their full IGMPv3/MLDv2 counterpart. These improvements are especially desirable for multicast mobility, as wireless devices typically have limited storage and CPU processing capabilities.
4. Requirements for IGMP/MLD to Support Mobile Multicast

4.1. Functional Requirements for Mobile Multicast

Any-Source Multicast (ASM) is a traditional multicast communication model in which receivers request all data from a multicast address, which is denoted with (*,G). A host joining a (*,G) session will receive data from all the sources sending to the specified multicast address. On the other hand, in the SSM communication, a host specifies both source and multicast addresses and receives the traffic from the specified source(s). The subscribed source-specific multicast session is denoted by an (S,G) and called a channel.

All the versions of IGMP/MLD support the ASM communication. It is not recommended to use IGMPv1 in mobile communications since it does not have a robust mechanism to retransmit report messages, does not provide fast leave, and does not support SSM, as described in Section 2. IGMPv2 and MLDv1 are possible to be used in mobile communications, but they do not support SSM subscription.

To enable the SSM communication, a mobile host must use IGMPv3/MLDv2 or LW-IGMPv3/LW-MLDv2. As described in [4], there is no functional difference to subscribe (S,G) channels between the full versions of IGMPv3/MLDv2 and the lightweight version protocols. The lightweight version protocols have the advantage of simpler processing.

IGMP/MLD protocols (except IGMPv1) implement fast join and fast leave functions. When a host joins a multicast session, it sends unsolicited join report to its upstream router immediately. The Startup Query Interval has been set to 1/4 of the General Query value to enable the faster join at startup. When the host ceases from listening a session, it sends a request to leave the session immediately. The Group-Specific or Source-and-Group-Specific Queries are triggered when an IGMP/MLD router knows that the reception for a group or a source-specific group has been terminated. This helps the router acquire the multicast membership information as fast as possible when all the members as a whole leave a group. The time to complete leaving from a session is referred to as leave latency. Lower leave latency (i.e. fast leave) has the advantage of quickly releasing the network resources.

4.2. Requirements on Tuning IGMP/MLD Protocol Parameters

Within each protocol’s scope, the number of transmitted packets on a wireless link could be further decreased by tuning timer values. For example, Query Interval can be set to a larger value to reduce the packet quantity. The Query Response interval could be widened to avoid the burst of messages.
On the other hand, to cover the possibility of a State-Change Report being missed by one or more multicast routers, a host transmits the same State-Change Report [Robustness Variable] times in all [2][3]. However, this manner does not only guarantee that the State-Change Report is reached to the routers, but also increases the number or amount of State-Change Report messages on a wireless link. It is required to tune these values with the good balance of protocol robustness and the amount of traffic.

As well, various IGMP/MLD timers should be configurable. If non-default settings are used, they MUST be consistent among all routers on a single network.

4.3. Requirements for Handover

[12] categorized the diversified mobile IP schemes by their group subscription manner principally as home subscription and remote subscription. These two different subscription has important influences on the handover behaviour. Since different mobile and handover protocols may need different parameters and different optimizations, this document describes the possible scenarios with examples in MIPv6 [9] but only discussed the possible requirements related to the group-subscription related behavior.

In home subscription, the IGMP/MLD message should be encapsulated and tunneled to the home network. The multicast router (e.g., Home Agent) on home network will be responsible for joining and pruning a multicast tree. When a mobile host moves to a new foreign network, it does not need to re-join the multicast group.

In the remote subscription approach, a mobile host joins the group via a local multicast router on the foreign network. The router intercepts the host’s report message and joins or prunes the multicast tree. After handover to another foreign network, the host needs to resend new reports to routers on the new network. If the old multicast branches have been torn down before the new branches being constructed, the host will suffer from packets loss during the handover.

To prevent packet loss, a make-before-break mechanism SHOULD be provided. It requires a mobile host to join the group on the new network as soon as possible once it decides to switch to the new network. The host keeps the reception of the "old" multicast data until the traffic from new branches arrives. Then the host begins issuing leave reports to the previous attached multicast router.

The possibility of packet loss can be reduced by predicting the movement of a mobile node during handover. The handover can be
initiated either by the mobile host or by the network. In the mobile-initiated handover, the host acquires the handover information quickly and can send early reports. In the network-initiated handover, the network entity indicates the possible handover situation and the mobile host does not invoke any process.

It may be possible that IGMP and MLD could be extended to carry the handover indication from a previous router to a new router to facilitate the fast join and fast leave. Since IGMP/MLD protocol or message extension may require additional operational costs or interoperability problems, it must be carefully defined.

IGMP/MLD hosts and routers can adjust their timer and counter values to make faster join/leave during handover, as described in Section 4.2. The adjustment is carried out by the application according to the actual wireless situations and policies of the management.

4.4. Requirements for Point-To-Point Link

A wireless link assumed in this document is categorized as a shared link or a point-to-point (PTP) or point-to-multipoint (PMP) link. For a shared link, the interface state maintained by a multicast router on the link is the summary of the receiving state for member hosts on the link.

But for a PTP link, a multicast router has to maintain the interface state for each link, and this condition may introduce protocol overhead for the router. When a large number of receivers attach on the wireless link, the multicast router may introduce protocol overhead for the router. Protocol simplification may give some benefit for the processing cost and memory usage to deal with a PTP link.

4.5. Requirements for Explicit Tracking

Since the full and lightweight IGMPv3 and MLDv2 protocols disable a report suppression mechanism (described in Section 3.3), multicast routers working with these protocols can choose to implement explicit tracking of mobile hosts. The explicit tracking enables the router to learn the reception state of each receiver, but at the meantime consumes substantial memory resources on the router.

The advantage of explicit tracking is that it provides better manageability of mobile receivers. It is unnecessary to issue Group-Specific queries and Source-Specific Queries to stop receiving on subnets whose router keeps track of group and source receivers.
5. Security Considerations

Apart from the security issue of IGMP/MLD, additional requirements should be considered for the features of the wireless link. They will be described in the later version of this draft.
6. References

6.1. Normative References


6.2. Informative References


Authors’ Addresses

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

Email: liuhui47967@huawei.com

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/

T.M. Eubanks
Iformata Communications
130 W. Second Street
Dayton, Ohio 45402
USA

Phone: +1 703 501 4376
Email: marshall.eubanks@iformata.com
URI: http://www.iformata.com/
Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.