IGMP/MLD Optimizations in Wireless and Mobile Networks
draft-liu-multimob-igmp-mld-wireless-mobile-03

Abstract

   This document proposes a variety of optimization approaches for IGMP
   and MLD in wireless and mobile networks. It aims to provide useful
   guidelines to allow efficient multicast communication in these
   networks using IGMP or MLD protocols.

Requirements Language

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

Status of this Memo

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

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

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

   This Internet-Draft will expire on August 26, 2013.

Table of Contents

1. Introduction

The deployments of various wireless access techniques are being combined with the use of video and other applications which rely upon IP Multicast. Wireless and mobile multicast are attracting increasing interest from content and service providers. Multicast faces challenges with dynamic group membership management being under the constant update of delivery paths introduced by node movement. There is a high probability of loss and congestion due to limited reliability and capacity of wireless links.

Multicast networks are generally constructed by the IGMP and MLD group management protocols (respectively for IPv4 and IPv6 networks) to track valid receivers and by multicast routing protocol building multicast delivery paths. This document focuses only on IGMP and MLD, the protocols used by a host to subscribe to a multicast group and the protocols that are most likely to be exposed to wireless links when supporting terminal mobility. As IGMP and MLD were designed for fixed users on a wired link, they do not necessarily work well for different wireless link types and mobile scenarios. IGMP/MLD should be enhanced to be more applicable in these mobile/ wireless environments.

This memo proposes a variety of optimizations for IGMP and MLD, in wireless and mobile networks, to improve network performance, with minimum changes on the protocol behavior and without introducing interoperability issues. These solutions can also be applied in wired networks when efficiency or reliability is required.

For generality, this memo does not put limitations on the type of wireless techniques running below IGMP or MLD. They could be cellular, WiMAX, WiFi and etc, and are modeled as different abstract link models as described in section 2.2. Even though some of them (such as WiFi) have multicast limitations, it is probable that IGMP/ MLD is enabled on the wireless terminal and multicast is supported across the network. The mobile IP protocol adopted on the core side, upstream from the access router, could be PMIP, MIPv4, or MIPv6.

2. Requirements

2.1. Characteristics of Wireless and Mobile Multicast

Several limitations should be considered when supporting IP multicast in wireless and mobile networks, including:

O Limited link bandwidth: wireless links usually have limited bandwidth, and the situation will be made even worse if a high volume

of video multicast data has to be carried. Additionally, the
bandwidth available in the upstream and downstream directions may be
asymmetrical.

O High loss rate: wireless links usually have packet loss ranging
from 1% to 30% according to different links types and conditions.
Also when packets have to travel between home and access networks
(e.g. through a tunnel), they are prone to loss if the two networks
are distant from each other.

O Frequent membership change: in fixed multicast, membership change
only happens when a user leaves or joins a group, while in mobile
scenario membership may also change when a user changes its location.

O Prone to performance degradation: the possible increased
interaction of protocols across layers for mobility management, and
the limitation of link capacity, may lead to network performance
degradation and even to complete connection loss.

O Increased Leave Latency: the leave latency in mobile multicast
might be increased due to user movement, especially if the traffic
has to be transmitted between access and home networks, or if there
is a handshake between networks.

2.2. Wireless Link Model

Wireless links can typically be categorized into three models: point-
to-point (PTP), point-to- multipoint (PTMP), and broadcast link
models.

In the PTP model, one link is dedicated for two communication
facilities. For multicast transmission, each PTP link normally has
only one receiver and the bandwidth is dedicated for that receiver.
Such link model may be implemented by running PPP on the link or
having separate VLAN assignment for each receiver. In a mobile
network, a tunnel between entities of home and foreign networks
should be recognized as a PTP link.

PTMP is the model for multipoint transmission wherein there is one
centralized transmitter and multiple distributed receivers. PTMP
provides common downlink channels for all receivers and dedicated
uplink channel for each receiver. Bandwidth downstream is shared by
all receivers on the same link.

Broadcast links can connect two or more nodes and support broadcast
transmissions. It is quite similar to fixed Ethernet link model and
its link resource is shared in both uplink and downlink directions.

2.3. **Requirements on IGMP and MLD**

   IGMP and MLD are usually run between mobile or wireless terminals and
   their first-hop access routers (i.e. home or foreign routers) to
   subscribe to a IP multicast channel. Currently the version in-use
   includes IGMPv2 [RFC2236] and its IPv6 counterpart MLDv1 [RFC2710],
   IGMPv3 [RFC3376] and its IPv6 counterpart MLDv2 [RFC3810], and LW-
   IGMPv3/MLDv2 [RFC5790]. All these versions have basic group
   management capability required by a multicast subscription. The
   differences lie in that IGMPv2 and MLDv1 can only join and leave a
   non-source-specific group, while IGMPv3 and MLDv2 can select
   including and excluding specific sources for their join and leave
   operation, and LW-IGMPv3/MLDv2 simplifies IGMPv3/MLDv2 procedures by
   discarding excluding-source function. Among these versions, (LW-)
   IGMPv3/MLDv2 has the capability of explicitly tracking each host
   member.

   From the illustration given in section 2.1 and 2.2, it is desirable
   for IGMP and MLD to have the following characteristics when used in
   wireless and mobile networks:

   o Adaptive to link conditions: wireless networks have various link
   types, each with different bandwidth and performance features. IGMP
   or MLD should be able to be adaptive to different link models and
   link conditions to optimize its protocol operation.

   o Minimal group join/leave latency: because mobility and handover may
   cause a user to join and leave a multicast group frequently, fast
   join and leave by the user helps to accelerate service activation and
   to release unnecessary resources quickly to optimize resource
   utilization.

   o Robust to packet loss: the unreliable packet transmission due to
   instable wireless link conditions and limited bandwidth, or long
   distance transmission in mobile network put more strict robustness
   requirement on delivery of IGMP and MLD protocol messages.

   o Reducing packet exchange: wireless link resources are usually more
   limited, precious, and congested compared to their wired counterpart.
   This requires packet exchange be minimized without degrading protocol
   performance.

   o Packet burst avoidance: large number of packets generated in a
   short time interval may have the tendency to deteriorate wireless
   network conditions. IGMP and MLD should be optimized to reduce the
   probability of packet burst.

3. **IGMP/MLD Optimization for Wireless and Mobile Networks**

   This section introduces several optimizations for IGMP and MLD in
   wireless or mobile environment. The aim is to meet the requirements
   described in section 2.3. It should be noted that because an
   enhancement in one direction might result in weakening effect in
   another, balances should be taken cautiously to realize overall
   performance elevation.

3.1. **Switching Between Unicast and Multicast Queries**

   IGMP/MLD protocols use multicast Queries whose destinations are
   multicast addresses and also allows use of unicast Query with unicast
   destination to be sent only to one host. Unicast Query has the
   advantage of not affecting other hosts on the same link, and is
   desirable for wireless communication because a mobile terminal often
   has limited battery power [RFC6636]. But if the number of valid
   receivers is large, using unicast Query for each receiver is
   inefficient because large number of Unicast Queries have to be
   generated, in which situation normal multicast Query will be a good
   choice because only one General Query is needed. If the number of
   receivers to be queried is small, unicast Query is advantageous over
   the multicast one.

   More flexibly, the router can choose to switch between unicast and
   multicast Queries according to the practical network conditions. For
   example, if the receiver number is small, the router could send
   unicast Queries respectively to each receiver, without arousing other
   non-member terminal which is in dormant state. When the receiver
   number reaches a predefined level, the router could change to use
   multicast Queries. To have the knowledge of the number of the valid
   receivers, a router is required to enable explicit tracking, and
   because Group-Specific Query and Group-and-Source-Specific Query are
   usually not used under explicit tracking [RFC6636], the switching
   operation mostly applies to General Queries.

3.2. **General Query Supplemented with Unicast Query**

   The Unicast Query can be used in assistance to General Query to
   improve the robustness of solicited reports when General Query fails
   to collect all of its valid members. It requires the explicit
   tracking to be enabled and can be used when a router after sending a
   periodical General Query collects successfully most of the valid
   members' responses while losing some of which are still valid in its
   database. This may be because these reports are not generated or
   generated but lost for some unknown reasons. The router could choose
   to unicast a Query respectively to each non-respondent valid receiver
   to check whether they are still alive for the multicast reception,

without affecting the majority of receivers that have already
responded. Unicast Queries under this condition could be sent at the
end of the [Maximum Response Delay] after posting a General Query,
and be retransmitted for [Last Member Query Count] times, at an
interval of [Last Member Query Interval].

3.3. Retransmission of Queries

In IGMP and MLD, apart from the continuously periodical transmission,
General Query is also transmitted during a router's startup. It is
transmitted for [Startup Query Count] times by [Startup Query
Interval]. There are some other cases where retransmission of
General Query is beneficial which are not covered by current IGMP and
MLD protocols as shown as following.

For example, a router which keeps track of all its active receivers,
if after sending a General Query, fails to get any response from the
receivers which are still valid in its membership database. This may
be because all the responses of the receivers happen to be lost, or
the sent Query does not arrive at the other side of the link to the
receivers. The router could compensate this situation by
retransmitting the General Query to solicit its active members. The
retransmission can also be applied to Group-Specific or Group-and-
Source-Specific Query on a router without explicit tracking
capability, when these Specific Queries cannot collect valid
response, to prevent missing valid members caused by lost Queries and
Reports.

The above compensating Queries could be sent [Last Member Query
Count] times, at the interval of [Last Member Query Interval], if the
router cannot get any feedback from the receivers.

3.4. General Query Suppression

In IGMP and MLD, the General Query is sent periodically and
continuously without any limitation. It helps soliciting the state
of current valid member but has to be processed by all hosts on the
link, whether they are valid multicast receivers or not. When there
is no receiver, the transmission of the General Query is a waste of
resources for both the host and the router.

An IGMP/MLD router could suppress its transmission of General Query
if it knows there is no valid multicast receiver on an interface,
e.g. in the following cases:

O When the last member reports its leave for a group. This could be
judged by an explicit tracking router checking its membership
database, or by a non-explicit-tracking router getting no response

after sending Group-Specific or Group-and-Source-Specific Query.

O When the only member on a PTP link reports its leaving

O When a router after retransmitting General Queries on startup fails to get any response

O When a router previously has valid members but fails to get any response after several rounds of General Queries.

In these cases the router could make the decision that no member is on the interface and totally stop its transmission of periodical General Queries. If afterwards any valid member joins a group, the router could resume the original cycle of general Querying. Because General Query influences all hosts on a link, suppressing it when it is not needed is beneficial for both the link efficiency and terminal power saving.

3.5. Tuning Response Delay According to Link Type and Status

IGMP and MLD use delayed response to spread unsolicited Reports from different hosts to reduce possibility of packet burst. This is implemented by a host responding to a Query in a specific time randomly chosen between 0 and [Maximum Response Delay], the latter of which is determined by the router and is carried in Query messages to inform the hosts for calculation of the response delay. A larger value will lessen the burst better but will increase leave latency (the time taken to cease the traffic flowing after the last member requests the escaping of a channel).

In order to avoid message burst and reduce leave latency, the Response Delay may be dynamically calculated based on the expected number of responders, and link type and status, as shown in the following:

O If the expected number of reporters is large and link condition is bad, longer Maximum Response Delay is recommended; if the expected number of reporters is small and the link condition is good, smaller Maximum response Delay should be set.

o If the link type is PTP, the Maximum Response Delay can be chosen smaller, whereas if the link is PTMP or broadcast medium, the Maximum Response Delay can be configured larger.

The Maximum Response Delay could be configured by the administrator as mentioned above, or be calculated automatically by a software tool implemented according to experiential model for different link modes. The measures to determine the instant value of Maximum Response Delay

are out of this document's scope.

3.6. Triggering Reports and Queries Quickly During Handover

When a mobile terminal is moving from one network to another, if it
is receiving multicast content, its new access network should try to
deliver the content to the receiver without disruption or performance
deterioration. In order to implement smooth handover between
networks, the terminal's membership should be acquired as quickly as
possible by the new access network.

An access router could trigger a Query to a terminal as soon as it
detects the terminal's attaching on its link. This could be a
General Query if the number of the entering terminals is not small
(e.g when they are simultaneously in a moving train). Or this Query
could also be a unicast Query for this incoming terminal to prevent
unnecessary action of other terminals in the switching area.

For the terminal, it could send a report immediately if it is
currently in the multicast reception state, when it begins to connect
the new network. This helps establishing more quickly the membership
state and enable faster multicast stream injection, because with the
active report the router does not need to wait for the query period
to acquire the terminal's newest state.

4. Applicability and Interoperability Considerations

Among the optimizations listed above, 'Switching between unicast and
multicast Queries'(3.1) and 'General Query Supplemented with Unicast
Query'(3.2) requires a router to know beforehand the valid members
connected through an interface, thus require explicit tracking
capability. An IGMP/MLD implementation could choose any combination
of the methods listed from 3.1 to 3.6 to optimize multicast
communication on a specific wireless or mobile network.

For example, an explicit-tracking IGMPv3 router, can switch to
unicast General Queries if the number of members on a link is small
(3.1), can trigger unicast Query to a previously valid receiver if
failing to get expected responses from it (3.2), can retransmit a
General Query if after the previous one cannot collect reports from
all valid members (3.3), and can stop sending a General Query when
the last member leaves the group (3.4), and etc.

For interoperability, it is required if multiple multicast routers
are connected to the same network for redundancy, each router are
configured with the same optimization policy to synchronize the
membership states among the routers.

5. IGMP/MLD Suspend and Resume

5.1. IGMP/MLD Suspend Request

   IGMP/MLD Suspend is an operation triggered by a host that subscribes
   multicast channels or an IGMP/MLD proxy [refs.Proxy] to which hosts
   subscribing multicast channels attached. An IGMP/MLD Suspend message
   requests an adjacent upstream router to suspend forwarding subscribed
   data, while to keep the subscription state (i.e., not to prune the
   routing path). It is useful especially in a mobile network. When a
   mobile host moves from a current network (i.e., a mobile host's point
   of attachment) to a different network, an IGMP/MLD Suspend message is
   sent by the host itself (or an IGMP/MLD proxy to which mobile hosts
   attached).

   When an IGMP/MLD proxy receives IGMP/MLD Suspend messages on its
   downstream interface, it forwards the Suspend message to its upstream
   router via its upstream interface if needed (see Section 5.3.

5.2. IGMP/MLD Resume Request

   When a host that has subscribed multicast channels and sent IGMP/MLD
   Suspend messages attaches to a new network, it immediately sends
   IGMP/MLD Resume messages to request its upstream router to resume
   forwarding the data. The Resume Records specified in the IGMP/MLD
   Resume message will be the same as that of the Suspend Records the
   host sent.

5.3. IGMP/MLD Suspend Reception

   When a multicast router receives an IGMP/MLD Suspend message from the
   downstream member hosts or IGMP/MLD proxy, it examines whether the
   message sender is the sole member of the reported channels at the
   downstream link or not. There are two ways to know it. One is done
   by the Group-Specific or Group-and-Source Specific Queries. The
   other is done by the explicit tracking function [refs.explicit].

   The router sends the Group-Specific or Group-and-Source Specific
   Queries for all records in the Suspend messages. If the router
   receives IGMP/MLD reports including some or all of the Suspend
   Records, it eliminates the reported records from the Suspend Records
   and keeps forwarding these data. If the router does not receive
   IGMP/MLD reports for some or all of the Suspend Records, it
   recognizes that the Suspend message sender is the sole member host
   for these channels on the link. After the router organizes the new
   Suspend Records (that eliminate reported records from the original
   one), it suspends data forwarding for them.

The explicit tracking function gives advantage of organizing the new
Suspended Records. If a router enables the explicit tracking
function, it can recognize whether the message sender host is the
sole member without sending the Group-Specific or Group-and-Source
Specific Queries. Then the router suspends data forwarding based on
the up-to-date Suspend Records.

The multicast router maintains Suspend Records until it receives the
corresponding IGMP/MLD Resume message (described in the next section)
or the IGMP/MLD Suspend Interval timer (described in Section 6.1) is
expired. When either the Resume message reception or the timer
expiration occurs, the router resume data forwarding for the Suspend
Records and discards the Suspend Records.

If a multicast router receives an IGMP/MLD Suspend message, which
includes Multicast Address Records already suspended, the router
restarts the IGMP/MLD Suspend Interval timer for the corresponding
Multicast Address Records.

When an IGMP/MLD proxy receives an IGMP/MLD Suspend message from a
downstream host, it behaves as a multicast router as described above,
because the proxy device performs the router portion of the IGMP or
MLD protocol on its downstream interfaces.

When a mobile node that has sent the IGMP/MLD Suspend message
receives the corresponding Group-Specific or Group-and-Source
Specific Queries for the Suspend Records, it replies the standard
IGMP/MLD Report messages as defined in [refs.IGMPv3][refs.MLDv2].

5.4. IGMP/MLD Resume Reception

When a multicast router receives an IGMP/MLD Resume message, the
router examines the message sender and an IGMP/MLD Suspend Interval
timer. If the router has the Suspend Records given from the Resume
message sender, it compares the Suspend Records with the notified
Multicast Address Records specified in the Resume message. For the
matched Multicast Address Records, the router then removes the
entries from the Suspend Records and resumes data forwarding with
restarting the group or source timers. For the mismatched Multicast
Address Records, the router keeps unchanged (then will be removed by
timeout) or explicitly starts the leave (or prune) procedures for the
channels, while it depends on the implementation.

If either the router does not have the corresponding Suspend Records
or the IGMP/MLD Suspend Interval timer has expired, then the router
does not take any action.

If a router that did not recognize an IGMP/MLD Suspend message (e.g.,

due to packet loss or some troubles in its transmission) receives an
IGMP/MLD Resume message, it will accept the message as a regular
Current-State Report IGMP/MLD message.

6. Timers, Counters, and Their Default Values

6.1. IGMP/MLD Suspend Interval Timer

After a multicast router receiving an IGMP/MLD Suspend message will
identify the corresponding multicast sessions/channels, it suspends
data forwarding and keeps the Suspend Records until the given amount
of timer value is expired. This timer is named the "IGMP/MLD Suspend
Interval timer", which is a configurable value.

The Suspend Interval is used to allow a multicast router to resume
the multicast session. Therefore, if the multicast router does not
receive the corresponding IGMP/MLD Resume message for the IGMP/MLD
Resume operation within the Suspend Interval, it leaves the sessions/
channels recorded in the Suspend Records and discards the Suspend
Records. Note that the router does not send any IGMP/MLD Query
message for the timeout sessions/channels and immediately leaves from
them.

7. IANA Considerations

This document makes no request of IANA.

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

8. Security Considerations

Since the methods only involve the tuning of protocol behavior by
e.g. retransmission, changing delay parameter, or other compensating
operations, they do not introduce additional security weaknesses.
The security consderations described in [RFC2236], [RFC3376],
[RFC2710] and [RFC3810] can be reused. And to achieve some security
level in insecure wireless network, it is possible to take stronger
security procedures during IGMP/MLD message exchange, which are out
of the scope of this memo.

9. Acknowledgements

The authors would like to thank Behcet Sarikaya, Qin Wu, Stig Venaas,

Gorry Fairhurst, Thomas C. Schmidt, Marshall Eubanks, Suresh
Krishnan, J.William Atwood, WeeSan Lee, Imed Romdhani, Liu Yisong and
Wei Yong for their valuable comments and suggestions on this
document.

10. References

10.1. Normative References

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

[RFC2236]   Fenner, W., "Internet Group Management Protocol, Version
            2", RFC 2236, November 1997.

[RFC2710]   Deering, S., Fenner, W., and B. Haberman, "Multicast
            Listener Discovery (MLD) for IPv6", RFC 2710,
            October 1999.

[RFC3376]   Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A.
            Thyagarajan, "Internet Group Management Protocol, Version
            3", RFC 3376, October 2002.

[RFC3810]   Vida, R. and L. Costa, "Multicast Listener Discovery
            Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC5790]   Liu, H., Cao, W., and H. Asaeda, "Lightweight Internet
            Group Management Protocol Version 3 (IGMPv3) and Multicast
            Listener Discovery Version 2 (MLDv2) Protocols", RFC 5790,
            February 2010.

[RFC6636]   Asaeda, H., Liu, H., and Q. Wu, "Tuning the Behavior of
            the Internet Group Management Protocol (IGMP) and
            Multicast Listener Discovery (MLD) for Routers in Mobile
            and Wireless Networks", RFC 6636, May 2012.

[refs.IGMPv1]
            Deering, S., "Host Extensions for IP Multicasting",
            RFC 1112, August 1989.

[refs.IGMPv2]
            Fenner, W., "Internet Group Management Protocol, Version
            2", RFC 2373, July 1997.

[refs.IGMPv3]
            Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A.
            Thyagarajan, "Internet Group Management Protocol, Version

                3", RFC 3376, October 2002.

   [refs.KEYWORDS]
                Bradner, S., "Key words for use in RFCs to indicate
                requirement levels", RFC 2119, March 1997.

   [refs.LW]   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.

   [refs.MLDv1]
                Deering, S., Fenner, W., and B. Haberman, "Multicast
                Listener Discovery (MLD) for IPv6", RFC 2710,
                October 1999.

   [refs.MLDv2]
                Vida, R. and L. Costa, "Multicast Listener Discovery
                Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

   [refs.PIM]
                Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas,
                "Protocol Independent Multicast - Sparse Mode (PIM-SM):
                Protocol Specification (Revised)", RFC 4601, August 2006.

   [refs.Proxy]
                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.

10.2. Informative References

   [refs.MIPv6]
                Johnson, D., Perkins, C., and J. Arkko, "Mobility Support
                in IPv6", RFC 3775, June 2004.

   [refs.Noel]
                Jelger, C. and T. Noel, "Multicast for Mobile Hosts in IP
                Networks: Progress and Challenges", IEEE Wireless
                Comm. pp.58-64, October 2002.

   [refs.PMIPv6]
                Gundavelli, S, Ed., Leung, K., Devarapalli, V., Chowdhury,
                K., and B. Patil, "Proxy Mobile IPv6", RFC 5213,
                August 2008.

   [refs.explicit]

              Asaeda, H., "IGMP/MLD-Based Explicit Membership Tracking
              Function for Multicast Routers",
              draft-ietf-pim-explicit-tracking-04.txt (work in
              progress), January 2013.

Authors' Addresses

    Hui Liu

    Email: liu_helen@126.com

    Mike McBride
    Huawei Technologies
    2330 Central Expressway
    Santa Clara CA 95050
    USA

    Email: michael.mcbride@huawei.com

    Hitoshi Asaeda
    National Institute of Information and Communications Technology (NICT)
    Network Architecture Laboratory
    4-2-1 Nukui-Kitamachi
    Koganei, Tokyo 184-8795
    Japan

    Email: asaeda@nict.go.jp