          Tuning the Behavior of the Internet Group Management Protocol (IGMP)
                  and Multicast Listener Discovery (MLD)
                 for Routers in Mobile and Wireless Networks

Abstract

   The Internet Group Management Protocol (IGMP) and Multicast Listener
   Discovery (MLD) are the protocols used by hosts and multicast routers
   to exchange their IP multicast group memberships with each other.
   This document describes ways to achieve IGMPv3 and MLDv2 protocol
   optimization for mobility and aims to become a guideline for the
   tuning of IGMPv3/MLDv2 Queries, timers, and counter values.

Copyright Notice

Table of Contents

1.  Introduction

   The Internet Group Management Protocol (IGMP) [1] for IPv4 and the
   Multicast Listener Discovery (MLD) [2] protocol for IPv6 are the
   standard protocols for hosts to initiate joining or leaving of
   multicast sessions.  These protocols must also be supported by
   multicast routers or IGMP/MLD proxies [5] 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.  The motion
of a host may cause disruption of multicast service initiation and
termination in the new or previous network.  Slow multicast service
activation following a join may incur additional delay in receiving
multicast packets and degrade reception quality.  Slow service
termination triggered by a rapid departure of the mobile host without
first 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 a
bidirectional tunnel is used with the mobility entities described in
[6] and [7], the mobile host experiences additional latency because
the round-trip time using a bidirectional tunnel between mobility
entities is larger compared to the case where a host and an upstream
router attach to a LAN.

This document describes ways to tune IGMPv3 and MLDv2 protocol
behavior -- on the multicast router and proxy side -- concentrating
in particular on wireless and mobile networks, including the tuning
of queries and related timers.  This selective optimization provides
tangible benefits to mobile hosts and routers by keeping track of the
membership status of downstream hosts, and of various IGMP/MLD Query
types and values, in order to appropriately tune the number of
response messages.  This document does not make any changes to the
IGMPv3 and MLDv2 protocols and only suggests optimal settings for the
configurable parameters of the protocols in mobile and wireless
environments.

2.  Terminology

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

3.  Explicit Tracking of Membership Status

   Mobile hosts use IGMP and MLD to make a 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.  An IGMP/MLD Query is therefore necessary to obtain 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.

The "explicit tracking function" [8] is a 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 request transmission of a
Current-State Report message from the receiver hosts, since the
router implicitly recognizes the (potential) last member host when it
receives the State-Change Report message reporting a leave.  The
router can therefore send IGMP/MLD Group-Specific and Group-and-
Source-Specific Queries LMQC/LLQC times (see Section 4.3) only when
it recognizes that the last member has left 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, possibly, substantial memory for routers to store all membership
status information.  This resource requirement is potentially
impacted, especially when a router needs to maintain a large number
of receiver hosts.  Therefore, this document recommends that adjacent
upstream multicast routers enable 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 or not routers enable the explicit
tracking function, 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 the IGMP/MLD General Query Interval

   IGMP and MLD are unreliable 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]) [1] [2].  Although this
   behavior increases the protocol's robustness, it does not guarantee
   that the State-Change Report reaches the routers.  Therefore, routers
   still need to refresh their downstream membership information by
   receiving a Current-State Report, as periodically solicited by an
   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.  This procedure also supports situations where mobile hosts are
   powered off or moved from one network to another network managed by a
   different router without any notification (e.g., a leave request).

The [Query Interval] is the interval between General Queries sent by
the regular IGMPv3/MLDv2 querier; the default value is 125 seconds
[1] [2].  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 a [Query Interval] value of 150 seconds by
changing the Querier's Query Interval Code (QQIC) field in the IGMP/
MLD Query message, for the case where a router that enables the
explicit tracking function 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 Report message
traffic and battery-power consumption for mobile hosts.

On the other hand, this document also proposes a [Query Interval]
value of 60 to 90 seconds for the case where a router that enables
the explicit tracking function attaches to a higher-capacity wireless
link.  This shorter interval contributes to quick synchronization of
the membership information tracked by the router but may consume
battery power on 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 [7] 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
increase the query interval.  This happens, for example, when the
home agent detects network congestion.  In this case, the home agent
starts forwarding queries with the default [Query Interval] value and
increases the value in a gradual manner.

4.2.  Tuning the 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
as "Max Resp Code=100" for IGMPv3 [1] and "Maximum Response
Code=10000" for MLDv2 [2].  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 the hosts'
responses are spread out over a larger interval, but will increase
join latency when a State-Change Report (i.e., join request) is
missing.

According to our experimental analysis, this document proposes two
scenarios for tuning the [Query Response Interval] value in different
wireless link conditions: one scenario is for a wireless link with

lower resource capacity or a lossy link, and the other scenario is
for a wireless link with enough capacity or whose condition is
reliable enough 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 a
longer [Query Response Interval] value, such as 10 to 20 (seconds).
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 Records) are lost on the
router.  Note that as defined in Section 4.1.1 of [1], in IGMPv3, a
Max Resp Code larger than 128 represents the exponential values and
changes the granularity.  For example, if one wants to set the Max
Response Time to 20.0 seconds, the Max Resp Code should be expressed
as "0b10001001", which is divided into "mant=0b1001" and "exp=0b000".

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

4.3.  Tuning the 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 LMQI and LLQI are changeable, it is reasonable to use the
default value (i.e., 1 second) for LMQI and LLQI in a wireless
network.  LMQC and LLQC, whose default value is the [Robustness
Variable] value, are also tunable.  Therefore, LMQC and LLQC can be
set to "1" for routers that enable 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 ought to 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 can set LMQC and LLQC to "2" for their
routers that enable 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 the 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, a shortened value, such as 1 second, would help
contribute to shortening handover delay for mobile hosts in, for
example, the base solution with Proxy Mobile IPv6 (PMIPv6) [9].  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 need to properly configure this value.

4.5.  Tuning the 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 [1] [2].  The QRV (Querier's Robustness Variable) field
in the IGMP/MLD Query contains the [Robustness Variable] value used
by the querier.  The default [Robustness Variable] value defined in
IGMPv3 [1] and MLDv2 [2] is "2".

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

4.6.  Tuning Scenarios for Various Mobile IP Networks

In mobile IP networks, IGMP and MLD are used with three deployment
scenarios: (1) running directly between a host and access router on a
wireless network, (2) running between a host and home router through
a tunnel link, and (3) running between a 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 in PMIPv6 [6],
the mobile access gateway, whose role is similar to a foreign router,
acts as a multicast router or proxy.

The second scenario occurs when a bidirectional tunnel established
between a host and home router is used to exchange IGMP/MLD messages
[7] [10].  Tuning the parameters is difficult in this situation
because the condition of the tunnel link 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 IGMP/MLD message transmission
through a tunnel link ought to be considered when parameters are set.
For example, the [Query Interval] and [Query Response Interval] could
be set shorter to compensate for transmission delay, and the
[Robustness Variable] could be increased to compensate for possible
packet loss.

The third scenario occurs in [9], in which the mobile access gateway
(i.e., foreign router) acts as the IGMP/MLD Proxy [5] in PMIPv6 [6].
Through the bidirectional 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, which influences the parameter
setting, the [Query Response Interval] on the local mobility anchor
could be set to a smaller value because the number of mobile access
gateways is much smaller compared to the number of hosts, and the
chance of packet burst is low for the same reason.  Additionally, the
power consumption due to a lower query interval is not an issue for
the mobile access gateways because the mobile access gateways are
usually not battery-powered.

Ideally, the IGMP/MLD querier router adjusts its parameter settings
according to the actual mobile IP network conditions to benefit
service performance and resource utilization.  It would be desirable
for a home router to determine the aforementioned timers and values
according to the delay between the initiating IGMP/MLD Query and the
responding IGMP/MLD Report.  However, describing how these timers and
values can be dynamically adjusted is out of scope for this document.

5.  Destination Address of a Specific Query

IGMP/MLD Group-Specific and Group-and-Source-Specific Queries defined
in [1] and [2] 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 the multicast
membership state of hosts on an attached network.

Group-Specific Queries are sent with an IP destination address equal
to the multicast address of interest, as defined in [1] and [2].
Using the multicast group of interest in the specific query is
preferred in this environment 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 to IGMP/MLD Reports.

6.  Interoperability

   IGMPv3 [1] and MLDv2 [2] 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) [3].

   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
   are IGMPv3/MLDv2 capable, regardless of whether the protocols are the
   full or lightweight version.  This document does not consider
   interoperability with older protocol versions.  One of the reasons
   for this lack of interoperability with older IGMP/MLD protocols is
   that the explicit tracking function does not work properly with older
   IGMP/MLD protocols because of a report-suppression mechanism; a host
   would not send a pending IGMP/MLD Report if a similar report was sent
   by another listener on the link.

7.  Security Considerations

   This document neither provides new functions nor modifies the
   standard functions defined in [1], [2], and [4].  Therefore, no
   additional security considerations are provided.

8.  Acknowledgements

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

9.  References

9.1.  Normative References

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

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

   [3]    Holbrook, H. and B. Cain, "Source-Specific Multicast for IP",
          RFC 4607, August 2006.

   [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.

9.2.  Informative References

   [5]    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.

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

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

   [8]    Asaeda, H. and N. Leymann, "IGMP/MLD-Based Explicit Membership
          Tracking Function for Multicast Routers", Work in Progress,
          April 2012.

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

   [10]   Perkins, C., Ed., "IP Mobility Support for IPv4, Revised",
          RFC 5944, November 2010.

Appendix A.  Unicasting a General Query

   This appendix describes the possible IGMP and MLD protocol extensions
   for further optimization in mobile and wireless environments.  It
   might be beneficial to include the following considerations when a
   newer version or modification of IGMP and MLD protocols is considered
   in the future.

   IGMPv3 and MLDv2 specifications [1] [2] explain 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 an IGMP/
   MLD General Query.  On the other hand, according to [1] and [2], a
   router may be able to unicast a General Query to the tracked member
   hosts in [Query Interval], if the router keeps track of membership
   information (Section 3).

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

   However, there is a concern regarding the unicast General Query: if a
   multicast router sends a 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 for membership information by sending a
   multicast General Query.  This concern 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 a
   protocol extension that is beyond the scope of this document.  If a
   router does not distinguish multicast and unicast General Query
   Intervals, the router should only use and enable multicast General
   Queries.

   Also, the unicast General Query does not remove the need for the
   multicast General Query.  The multicast General Query is necessary
   for updating membership information if the information is not
   correctly synchronized due to missing reports.  Therefore, the

   unicast General Query should not be used for an implementation that
   does not allow the configuration of different query interval timers
   such 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
   Queries.

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.
   Building Q14, No. 156, Beiqing Rd.
   Beijing  100095
   China

   EMail: helen.liu@huawei.com


   Qin Wu
   Huawei Technologies Co., Ltd.
   101 Software Avenue
   Yuhua District
   Nanjing, Jiangsu  210012
   China

   EMail: bill.wu@huawei.com