Network Working Group
Request for Comments: 4604
Updates: 3376, 3810
Category: Standards Track

H. Holbrook
Arastra, Inc.
B. Cain
Acopia Networks
B. Haberman
JHU APL

August 2006

Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast

Status of This Memo

Copyright Notice

Abstract

The Internet Group Management Protocol Version 3 (IGMPv3) and the Multicast Listener Discovery Protocol Version 2 (MLDv2) are protocols that allow a host to inform its neighboring routers of its desire to receive IPv4 and IPv6 multicast transmissions, respectively. Source-specific multicast (SSM) is a form of multicast in which a receiver is required to specify both the network-layer address of the source and the multicast destination address in order to receive the multicast transmission. This document defines the notion of an "SSM-aware" router and host, and clarifies and (in some cases) modifies the behavior of IGMPv3 and MLDv2 on SSM-aware routers and hosts to accommodate source-specific multicast. This document updates the IGMPv3 and MLDv2 specifications.

1. Introduction

The Internet Group Management Protocol (IGMP) [RFC1112, IGMPv2, IGMPv3] allows an IPv4 host to communicate IP multicast group membership information to its neighboring routers. IGMP version 3 (IGMPv3) [IGMPv3] provides the ability for a host to selectively request or filter traffic from individual sources within a multicast group.

The Multicast Listener Discovery Protocol (MLD) [RFC2710, MLDv2] offers similar functionality for IPv6 hosts. MLD version 2 (MLDv2) provides the analogous "source filtering" functionality of IGMPv3 for IPv6.

Due to the commonality of function, the term "Group Management Protocol", or "GMP", will be used to refer to both IGMP and MLD. The term "Source Filtering GMP", or "SFGMP", will be used to refer jointly to the IGMPv3 and MLDv2 group management protocols.

The use of source-specific multicast is facilitated by small changes to the SFGMP protocols on both hosts and routers. [SSM] defines general requirements that must be followed by systems that implement the SSM service model; this document defines the concrete application of those requirements to systems that implement IGMPv3 and MLDv2. In doing so, this document defines modifications to the host and router portions of IGMPv3 and MLDv2 for use with SSM, and presents a number of clarifications to their behavior when used with SSM addresses. This document updates the IGMPv3 and MLDv2 specifications.

1.1. 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].

In order to emphasize the parts of this document that modify the existing protocol specifications ([RFC2710, MLDv2, IGMPv3]), as opposed to merely clarify them, any protocol modifications are marked with the tag "MODIFICATION".

2. Host Requirements for Source-Specific Multicast

This section defines the notion of an "SSM-aware" host and then goes on to describe the API requirements and the SFGMP protocol requirements of an SSM-aware host. It is important to note that SSM can be used by any host that supports source filtering APIs and whose operating system supports the appropriate SFGMP. The SFGMP

modifications described in this section make SSM work better on an SSM-aware host, but they are not strict prerequisites for the use of SSM.

The 232/8 IPv4 address range is currently allocated for SSM by IANA [IANA-ALLOCATION]. In IPv6, the FF3x::/32 range (where 'x' is a valid IPv6 multicast scope value) is reserved for SSM semantics [RFC3306], although today SSM allocations are restricted to FF3x::/96. ([SSM] has a more thorough discussion of this topic.) A host that knows the SSM address range and is capable of applying SSM semantics to it is described as an "SSM-aware" host.

A host or router may be configured to apply SSM semantics to addresses other than those in the IANA-allocated range. The GMP module on a host or router SHOULD have a configuration option to set the SSM address range(s). If this configuration option exists, it MUST default to the IANA-allocated SSM range. The mechanism for setting this configuration option MUST at least allow for manual configuration. Protocol mechanisms to set this option may be defined in the future.

2.1. API Requirements

If the host IP module of an SSM-aware host receives a non-source-specific request to receive multicast traffic sent to an SSM destination address, it SHOULD return an error to the application, as specified in [MSFAPI] (MODIFICATION). On a non-SSM-aware host, an application that uses the wrong API (e.g., "join(G)", "IPMulticastListen(G,EXCLUDE(S1))" for IGMPv3, or "IPv6MulticastListen(G,EXCLUDE(S2))" for MLDv2) to request delivery of packets sent to an SSM address will not receive the requested service, because an SSM-aware router (following the rules of this document) will refuse to process the request, and the application will receive no indication other than a failure to receive the requested traffic.

2.2. GMP Requirements

This section defines the behavior of the SFGMP protocol module on an SSM-aware host, including two modifications to the protocols as described in [IGMPv3, MLDv2]. It also includes a number of clarifications of protocol operations. In doing so, it documents the behavior of an SSM-aware host with respect to sending and receiving the following GMP message types:

- IGMPv1/v2 and MLDv1 Reports (2.2.1)
- IGMPv3 and MLDv2 Reports (2.2.2)
- IGMPv1 Queries, IGMPv2 and MLDv1 General Queries (2.2.3)

- IGMPv2 Leave and MLDv1 Done (2.2.4)
- IGMPv2 and MLDv1 Group Specific Query (2.2.5)
- IGMPv3 and MLDv2 Group Specific Query (2.2.6)
- IGMPv3 and MLDv2 Group-and-Source Specific Query (2.2.7)

2.2.1. IGMPv1/v2 and MLDv1 Reports

An SSM-aware host operating according to [IGMPv3, MLDv2] could send an IGMPv1, IGMPv2, or MLDv1 report for an SSM address when it is operating in "older-version compatibility mode." This is an exceptional (error) condition, indicating that the router(s) cannot provide the SFGMP support needed for SSM, and an error is logged when the host enters compatibility mode for an SSM address, as described below. In this situation, it is likely that traffic sent to a channel (S,G) will not be delivered to a receiving host that has requested to receive channel (S,G).

[IGMPv3] and [MLDv2] specify that a host MAY allow an older-version report to suppress its own IGMPv3 or MLDv2 Membership Record. An SSM-aware host, however, MUST NOT allow its report to be suppressed in this situation (MODIFICATION). Suppressing reports in this scenario would provide an avenue for an attacker to deny SSM service to other hosts on the link.

2.2.2. IGMPv3 and MLDv2 Reports

A host implementation may report more than one SSM channel in a single report either by including multiple sources within a group record or by including multiple group records.

A Group Record for a source-specific destination address may (under normal operation) be any of the following types:

- MODE_IS_INCLUDE as part of a Current-State Record

- ALLOW_NEW_SOURCES as part of a State-Change Record

- BLOCK_OLD_SOURCES as part of a State-Change Record

A report may include both SSM destination addresses and non-source-specific, i.e., Any-Source Multicast (ASM) destination addresses, in the same message.

Additionally, a CHANGE_TO_INCLUDE_MODE record may be sent by a host in some cases, for instance, when the SSM address range is changed through configuration. A router should process such a record according to the normal SFGMP rules.

An SSM-aware host SHOULD NOT send any of the following record types for an SSM address.

- MODE_IS_EXCLUDE as part of a Current-State Record

- CHANGE_TO_EXCLUDE_MODE as part of a Filter-Mode-Change Record

This is a MODIFICATION to [IGMPv3, MLDv2], imposing a restriction on its use for SSM destination addresses. The rationale is that EXCLUDE mode does not apply to SSM addresses, and an SSM-aware router will ignore MODE_IS_EXCLUDE and CHANGE_TO_EXCLUDE_MODE requests in the SSM range, as described below.

2.2.3. IGMPv1 Queries, IGMPv2 and MLDv1 General Queries

If an IGMPv1 Query, or an IGMPv2 or MLDv1 General Query is received, the SFGMP protocol specifications require the host to revert to the older (IGMPv1, IGMPv2, or MLDv1) mode of operation on that interface. If this occurs, the host will stop reporting source-specific subscriptions on that interface and will start using IGMPv1, IGMPv2, or MLDv1 to report interest in all SSM destination addresses, unqualified by a source address. As a result, SSM semantics will no longer be applied to the multicast group address by the router.

A router compliant with this document would never generate an IGMPv1, IGMPv2, or MLDv1 query for an address in the SSM range; thus, this situation only occurs either if the router is not SSM-aware, or if the host and the router disagree about the SSM address range (for instance, if they have inconsistent manual configurations).

A host SHOULD log an error if it receives an IGMPv1, IGMPv2, or MLDv1 query for an SSM address (MODIFICATION).

In order to mitigate this problem, it must be administratively assured that all routers on a given shared-medium network are compliant with this document and are in agreement about the SSM address range.

2.2.4. IGMPv2 Leave and MLDv1 Done

IGMP Leave and MLD Done messages are not processed by hosts. IGMPv2 Leave and MLDv1 Done messages should not be sent for an SSM address, unless the sending host has reverted to older-version compatibility mode, with all the caveats described above.

2.2.5. IGMPv2 and MLDv1 Group Specific Query

If a host receives an IGMPv2 or MLDv1 Group Specific Query for an address in any configured source-specific range, it should process the query normally, as per [IGMPv3, MLDv2], even if the group queried is a source-specific destination address. The transmission of such a query likely indicates either that the sending router is not compliant with this document or that it is not configured with the same SSM address range(s) as the receiving host. A host SHOULD log an error in this case (MODIFICATION).

2.2.6. IGMPv3 and MLDv2 Group-Specific Query

If an SSM-aware host receives an SFGMP Group-Specific Query for an SSM address, it must respond with a report if the group matches the source-specific destination address of any of its subscribed source-specific channels, as specified in [IGMPv3, MLDv2].

The rationale for this is that, although in the current SFGMP protocol specifications a router would have no reason to send one, the semantics of such a query are well-defined in this range and future implementations may have reason to send such a query. Be liberal in what you accept.

2.2.7. IGMPv3 and MLDv2 Group-and-Source-Specific Query

An SFGMP router typically uses a Group-and-Source-Specific Query to query an SSM channel that a host has requested to leave via a BLOCK_OLD_SOURCES record. A host must respond to a Group-and-Source-Specific Query for which the group and source in the query match any channel for which the host has a subscription, as required by [IGMPv3, MLDv2]. The use of an SSM address does not change this behavior.

A host must be able to process a query with multiple sources listed per group, again as required by [IGMPv3, MLDv2]. The use of an SSM address does not modify the behavior of the SFGMPs in this regard.

3. Router Requirements for Source-Specific Multicast

Routers must be aware of the SSM address range in order to provide the SSM service model. A router that knows the SSM address range and is capable of applying SSM semantics to it as described in this section is described as an "SSM-aware" router. An SSM-aware router MAY have a configuration option to apply SSM semantics to addresses other than the IANA-allocated range, but if such an option exists, it MUST default to the IANA-allocated range.

This section documents the behavior of routers with respect to the following types of SFGMP messages for source-specific destination addresses:

- IGMPv3 and MLDv2 Reports (3.1)
- IGMPv3 and MLDv2 General Query (3.2)
- IGMPv3 and MLDv2 Group-Specific Query (3.3)
- IGMPv3 and MLDv2 Group-and-Source Specific Query (3.4)
- IGMPv1/v2 and MLDv1 Reports (3.5)
- IGMPv1/v2 and MLDv1 Queries (3.6)
- IGMPv2 Leave and MLDv1 Done (3.7)

3.1. IGMPv3 and MLDv2 Reports

SFGMP Reports are used to report source-specific subscriptions in the SSM address range. A router SHOULD ignore a group record of either of the following types if it refers to an SSM destination address:

- MODE_IS_EXCLUDE Current-State Record

- CHANGE_TO_EXCLUDE_MODE Filter-Mode-Change Record

A router MAY choose to log an error in either case. It MUST process any other group records within the same report. These behaviors are MODIFICATIONS to [IGMPv3, MLDv2] to prevent non-source-specific semantics from being applied to SSM addresses, and to avoid reverting to older-version compatibility mode.

A CHANGE_TO_INCLUDE_MODE Filter-Mode-Change Record is processed per the normal SFGMP rules; Section 2.2.2 describes a legitimate scenario when this could occur.

3.2. IGMPv3 and MLDv2 General Queries

An SSM router sends periodic SFGMP General Queries as per the IGMPv3 and MLDv2 specifications. No change in behavior is required for SSM.

3.3. IGMPv3 and MLDv2 Group-Specific Queries

SFGMP routers that support source-specific multicast may send group-specific queries for addresses in the source-specific range. This specification does not explicitly prohibit such a message, although, at the time of this writing, a router conformant to [IGMPv3, MLDv2] would not send one.

3.4. IGMPv3 and MLDv2 Group-and-Source-Specific Queries

SFGMP Group-and-Source-Specific Queries are used when a receiver has indicated that it is no longer interested in receiving traffic from a particular (S,G) pair to determine if there are any remaining directly-attached hosts with interest in that (S,G) pair. Group-and-Source-Specific Queries are used within the source-specific address range when a router receives a BLOCK_OLD_SOURCES Record for one or more source-specific groups. These queries are sent normally, as per [IGMPv3, MLDv2].

3.5. IGMPv1/v2 and MLDv1 Reports

An IGMPv1/v2 or MLDv1 report for an address in the source-specific range could be sent by a non-SSM-aware host. A router SHOULD ignore all such reports and specifically SHOULD NOT use them to establish IP forwarding state. This is a MODIFICATION to [IGMPv3, MLDv2]. A router MAY log an error if it receives such a report (also a MODIFICATION).

3.6. IGMPv1/v2 and MLDv1 Queries

An SFGMP router that loses the querier election to a lower version router must log an error, as specified by [IGMPv3, MLDv2].

3.7. IGMPv2 Leave and MLDv1 Done

An IGMPv2 Leave or MLDv1 Done message may be sent by a non-SSM-aware host. A router SHOULD ignore all such messages in the source-specific address range and MAY log an error (MODIFICATION).

4. Security Considerations

The specific protocol modifications described in this document are not known to create any security concerns that are not already present when IGMPv3 or MLDv2 is used with ASM-style multicast. The reader is referred to [SSM] for an analysis of SSM-specific security issues.

It is important that a router not accept non-source-specific reception requests for an SSM destination address. The rules of [IGMPv3] and [MLDv2] require a router, upon receiving such a membership report, to revert to earlier version compatibility mode for the group in question. If the router were to revert in this situation, it would prevent an IGMPv3-capable host from receiving SSM service for that destination address, thus creating a potential for an attacker to deny SSM service to other hosts on the same link.

5. Acknowledgements

The authors would like to thank Vince Laviano, Nidhi Bhaskar, Steve Deering, Toerless Eckert, and Pekka Savola for their input and careful review.

6. Normative References

[IGMPv2] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.

[IGMPv3] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.

[MSFAPI] Thaler, D., Fenner, B., and B. Quinn, "Socket Interface Extensions for Multicast Source Filters", RFC 3678, January 2004.

[RFC1112] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, August 1989.

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

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

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

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

8. Informative References

[IANA-ALLOC] Internet Assigned Numbers Authority, http://www.iana.org/assignments/multicast-addresses.

[RFC3306] Haberman, B. and D. Thaler, "Unicast-Prefix-based IPv6 Multicast Addresses", RFC 3306, August 2002.

Authors' Addresses

Hugh Holbrook
Arastra, Inc.
P.O. Box 10905
Palo Alto, CA 94303

Phone: +1 650 331-1620
EMail: holbrook@arastra.com

Brad Cain
Acopia Networks

EMail: bcain99@gmail.com

Brian Haberman
Johns Hopkins University Applied Physics Lab
11100 Johns Hopkins Road
Laurel, MD 20723-6099

EMail: brian@innovationslab.net

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).