Network Working Group
Request for Comments: 3590
Updates: 2710
Category: Standards Track

B. Haberman
Caspian Networks

September 2003

Source Address Selection for the Multicast Listener Discovery (MLD) Protocol

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

It has come to light that there is an issue with the selection of a suitable IPv6 source address for Multicast Listener Discovery (MLD) messages when a node is performing stateless address autoconfiguration. This document is intended to clarify the rules on selecting an IPv6 address to use for MLD messages.

1. Introduction

The original specification of the Multicast Listener Discovery Protocol (MLD) for IPv6 [RFC 2710] mandates the use of a link-local IPv6 source address for the transmission of MLD messages. In addition, MLD also requires nodes to send MLD Report messages when joining any IPv6 multicast group (except the All-Nodes address and addresses of scope less than 2).

These MLD requirements conflict with the use of IPv6 multicast within the Neighbor Discovery Protocol [RFC 2461]. For stateless autoconfiguration, as defined in [RFC 2462], a node is required to join several IPv6 multicast groups in order to perform Duplicate Address Detection prior to its use. Since the only address the node has is tentative, and cannot be used for communication, it does not have a suitable address to utilize as a source address.

This document will clarify the IPv6 source address selection rules for use with MLD when no link-local addresses are available.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119].

3. Justification

In [RFC 2710], Section 3 requires that all MLD messages be sent with a valid link-local IPv6 source address. However, a node in the process of performing duplicate address detection for its link-local (LL) address will not have one available to use as a source address. For this reason, this document allows the unspecified address to be used as a source address for MLD messages being used during duplicate address detection.

The discrepancies in the rules defined in [RFC 2710] and [RFC 2462] has led to implementation issues. Several IPv6 implementations skip sending MLD Report messages during duplicate address detection because they have no valid link-local address. This leads to operational problems when a node is attached to switches that perform MLD snooping. In this scenario, duplicate address detection (DAD) will complete successfully and collisions can occur once the address is put into use because switches may not have forwarded the DAD messages to all nodes on the link as required. This document fixes this problem by specifying that MLD reports are to be sent using an unspecified source address prior to DAD being started in order to ensure that messages sent to LL multicast addresses (e.g., including MLD) are forwarded to all appropriate nodes as required.

4. MLD Source Address Selection Guidelines

An MLD speaking node is required to choose a suitable IPv6 source address for all MLD messages (Report, Done, and Query).

MLD Query messages MUST be sent with a valid link-local address as the IPv6 source address. If a node (router or host) receives a query message with an IPv6 source address set to the unspecified address (::), it MUST silently discard the message and SHOULD log a warning.

MLD Report and Done messages are sent with a link-local address as the IPv6 source address, if a valid address is available on the interface. If a valid link-local address is not available (e.g., one has not been configured), the message is sent with the unspecified address (::) as the IPv6 source address.

Once a valid link-local address is available, a node SHOULD generate new MLD Report messages for all multicast addresses joined on the interface.

Routers receiving an MLD Report or Done message with the unspecified address as the IPv6 source address MUST silently discard the packet without taking any action on the packets contents.

Snooping switches MUST manage multicast forwarding state based on MLD Report and Done messages sent with the unspecified address as the IPv6 source address.

5. Source Address Selection Implications

In RFC 2710, MLD Report and Done messages are required to have an IPv6 source address that is link-local. This memo augments that rule by allowing these messages to contain the unspecified address (::) as the source address.

The behavior of RFC 2710 implementations, when receiving a message with a source address of ::, is dependent upon how the implementation treats the unspecified address. That is, these messages will be dropped if the implementation does not consider the unspecified address to be link-local in scope.

As the unspecified address is only used when there is no link-local address, RFC 2710 implementations discarding these packets will have no affect on the packet's sender as the use should only be for joining the link-local solicited-node multicast group [RFC 2462].

There is an implication to senders with respect to joining other multicast groups prior to the activation of a link-local address. The dropping of Reports using the unspecified address as a source address could cause a lack of multicast traffic that is expected by the node. This black hole will be temporary until the node can send a Report with a valid link-local address.

6. Security Considerations

General security issues related to MLD are discussed in [RFC 2710].

For hosts and routers, all received MLD messages from an unspecified source address are silently discarded. This is the required behavior from [RFC 2710] and is not changed by this document. Thus, the changes have no new security impacts.

In the case of snooping switches, multicast forwarding state will be maintained based on Report and Done messages sent with the unspecified address as the source address. However, the security vulnerabilities in this scenario are similar to those describing forged messages in the security considerations section of [RFC 2710].

7. Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property 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; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication 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 implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

8. References

8.1. Normative References

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

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

8.2. Informative References

[RFC 2461] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[RFC 2462] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

9. Author's Address

Brian Haberman
Caspian Networks
753 Bridgewater Drive
Sykesville, MD 21784

Phone: +1-410-552-1421
EMail: brian@innovationslab.net

10. Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.

Acknowledgement

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