

Individual submission
Internet Draft
[draft-haberman-ipngwg-host-anycast-01.txt](#)
May 2002
Expires November 2002

B. Haberman

D. Thaler
Microsoft

Host-based Anycast using MLD

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#) [[RFC 2026](#)].

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/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Abstract

This specification defines extended uses of the Multicast Listener Discovery protocol to support hosts participating in anycast groups. The extensions presented in this document allow hosts to notify the routing system of membership changes in an anycast group.

[1](#). Introduction

This specification defines extended uses of the Multicast Listener Discovery protocol [[RFC 2710](#)] to support hosts participating in anycast groups. The extensions presented in this document allow hosts to notify the routing system of membership changes in an anycast group, just as MLD currently allows hosts to notify the routing system of membership changes in a multicast group.

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](#) [[RFC 2119](#)].

Haberman, Thaler

1

Internet Draft

Using MLD for Anycast Membership

November 2002

[2.](#) Overview

Like multicast, hosts participating in an anycast group must be able to notify the routing system of changes in their group membership status (joins and leaves). Routers must be able to query hosts as to their membership status. In fact, for multicast and anycast, the host-to-router membership communications is the same.

For this reason, the existing MLD messages can be extended to support the host-to-router membership exchanges for anycast groups. The following sections will detail the modifications needed for both hosts and routers.

[3.](#) Host Behavior

3.1 Joining An Anycast Group

A host will generate an MLD Report message when it wishes to join an anycast group. The host will set the Multicast Address field of the Report message to the anycast group address it wishes to join. All other Report message fields are initialized as specified in [RFC 2710](#).

The IPv6 Destination Address field is set to the link-local All-Routers address (FF02::2).

A host must also join the Solicited Node multicast address for the anycast address as specified in [[RFC 2373](#)].

3.2 Leaving An Anycast Group

When a host wishes to leave an anycast group, it will generate an MLD Leave message. The host will set the Multicast Address field of the Leave message to the anycast group address it wishes to leave. All other Leave message fields are initialized as specified in [RFC 2710](#).

The IPv6 Destination Address field is set to the link-local All-Routers address (FF02::2).

A host must also leave the Solicited Node multicast address that corresponds to the anycast group address as specified in [[RFC 2373](#)].

3.3 Responding to Query Messages

When a host receives a General Query, it must generate a Report message for every anycast group in which it is a member.

Haberman, Thaler

2

Internet Draft

Using MLD for Anycast Membership

November 2002

When a host receives an Address-Specific Query, if it is listening to the specified anycast group it must generate a Report message for that anycast group.

[4.](#) Router Behavior

4.1 Generating Query Messages

A router supporting anycast groups must manage anycast group membership in the same manner that it manages multicast group membership. That is, all timers and databases used for multicast are also used for anycast.

A router generating General Query messages will initialize the MLD fields in the same manner described in [RFC 2710](#). The goal is to learn of all group members on an attached segment, both anycast and multicast.

A router generating Address-Specific Query messages will initialize the MLD fields as described in [RFC 2710](#). The Multicast Address field will be set to the anycast group to be queried. The Maximum Response Delay field must be set to 0. The IPv6 Destination Address must be set to the Solicited Node multicast address corresponding to the anycast address.

4.2 Receiving Report Messages

When a router receives an MLD Report message, an anycast Report message is distinguished from a multicast Report message by the MLD Multicast Address field. An anycast group address can be managed in

the same manner as a multicast group address. All of the timers and state machines defined in [RFC 2710](#) also apply to anycast group management.

The receiving router must verify that:

- The IPv6 Source Address is a link-local address
- The MLD checksum field is valid

4.3 Receiving Leave Messages

When a router receives an MLD Leave message, the anycast Leave message is distinguishable from a multicast Leave message by the MLD Multicast Address field. The router can manage the anycast group information in the same manner as it does multicast group information. The reception of an anycast Leave message must trigger the transmission of an Address-Specific Query for the specified anycast address.

Haberman, Thaler

3

Internet Draft

Using MLD for Anycast Membership

November 2002

The receiving router must verify that:

- The IPv6 Source Address is a link-local address
- The MLD checksum field is valid

[5](#). Security

Unlike multicast, allowing nodes to join arbitrary anycast groups can result in denial-of-service attacks. Whereas joining a multicast group does not prevent other nodes from seeing the same traffic, joining an anycast group can cause traffic previously seen by another node to be redirected to the newly joining node instead.

To prevent such attacks, it is expected that routers will employ some filtering mechanism when receiving a Report message containing a non-multicast address. For example, one policy might be to deny all anycast joins except those that match a configured list of (source address, anycast address) pairs.

[6](#). References

[RFC 2026] S. Bradner, "The Internet Standards Process -- Revision 3", [BCP 9](#), [RFC 2026](#), October 1996.

- [RFC 2710] S. Deering, W. Fenner, and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", [RFC 2710](#), October 1999.
- [RFC 2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), [BCP14](#), March 1999.
- [RFC 2373] R. Hinden and S. Deering, "IP Version 6 Addressing Architecture", [RFC 2373](#), July 1998.

Haberman, Thaler

4

Author's Address

Brian Haberman
1-919-949-4828
Email : bkhab@nc.rr.com

Dave Thaler
Microsoft Corporation
One Microsoft Way
Redmond, WA 48105-6399
1-425-703-8835
Email: dthaler@microsoft.com

