v6ops WG
Internet-Draft
Intended status: Standards Track
Expires: February 17, 2011

S. Gundavelli
M. Townsley
O. Troan
W. Dec
Cisco

August 16, 2010

Unicast Transmission of IPv6 Multicast Messages on Link-layer
draft-gundavelli-v6ops-l2-unicast-03.txt

Abstract

When transmitting an IPv6 packet to a multicast group, the destination address in the link-layer header is typically set to the corresponding mapped address of the destination address from the IP header. However, it is not mandatory that the destination address in the link-layer header is always a mapped multicast equivalent of its IP destination address. There are various deployment scenarios where there is an opportunity for the sender to transmit the message as an unicast message on the link-layer. Unfortunately, the IPv6 specifications do not clearly state this. This document explicitly clarifies this point and makes such packet construct and transmission legal and valid.

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 February 17, 2011.

Table of Contents

1. Introduction

This document is about a clarification to the construction and processing rules of IPv6 multicast messages [RFC2464]. When there are multiple link-layer receivers for an IP multicast message on a broadcast LAN, the link layer multicast address corresponding to the IP address is the one to be used. However, if there is only one receiver and its link-layer address is known (Example: as in some cases of sparse mode multicast, or in other intended use-cases such as proposed in [I-D.costa-6man-dad-proxy-00], in which a Duplicate Address Detection Proxy sends layer-2 unicast messages when appropriate to limit VLAN flooding), it is legal to send the IP multicast to the unicast link-layer address of that system. Senders therefore have that option, and receivers should not refuse the message on that basis.

The function of the link-layer is purely for transmitting the frame to a node or to a set of nodes on a given link. A received multicast message may have been transmitted as a unicast message on the link-layer. The destination address in the link-layer header of that packet will be a unicast address, while the destination address in the IP header will be a multicast address. Which link-layer address was used has no consequence for further processing of the packet by the IP stack. Any implementation that checks that the both the network and link-layer addresses are multicast would be in violation of the principles of protocol layering and does not serve any purpose. Unfortunately, [RFC4861] or [RFC2464] does not explicitly state this. However, we have verified this on many open source and commercial IPv6 implementations on the behavior of the existing IPv6 stacks, firewalls and we could not find any implementation that drops IPv6 packets sent to a multicast destination address in the IP header, but with a unicast destination address in the link-layer header.

The function of the link-layer is purely for transmitting the frame to a node or to a set of nodes on a given link. A received multicast message may have been transmitted as a unicast message on the link-layer. The destination address in the link-layer header of that packet will be a unicast address, while the destination address in the IP header can be a multicast address. It is inconsequential for the network layer protocols or the IP stack to go across the layers and check the semantics of message delivery. Any such check is a violation of the principles of protocol layering and does not serve any purpose. Unfortunately, [RFC4861] or [RFC2464] does not explicitly state this. However, the authors of this document have verified many open source and commercial IPv6 implementations on the behavior of the existing IPv6 stacks, firewalls and they could not find any implementation that drops IPv6 packets sent to a multicast

destination address in the IP header, but with a unicast destination address in the link-layer header.

As a result of this analysis, it appears to be quite safe to explicitly state that such message construct is valid, so future implementations do not drop packets based on these checks. Section 3 of this document defines the additional normative considerations for IPv6 nodes to allow this mode of packet transmission.

2. Conventions

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].

3. Sending and Receiving IPv6 Multicast Packets

The following additional considerations MUST be applied by all IPv6 nodes when sending and receiving IPv6 multicast messages.

- An IPv6 receiver node SHOULD NOT drop a received IPv6 multicast message containing a multicast destination address in the IPv6 header, but with a unicast destination address in the link-layer header.

- An IPv6 sender node in some special cases and specifically when the link-layer address of the target node is known, MAY choose to transmit an IPv6 multicast message as a link-layer unicast message to that node. In this case, the destination address in the IPv6 header will be a multicast group address, but the destination address in the link-layer header will be an unicast address.

4. IANA Considerations

This specification does not require any IANA actions.

5. Security Considerations

This document is about a clarification to the construction and processing rules of IPv6 multicast messages. This clarification explicitly permits an IPv6 node to send an IPv6 multicast message to the unicast link-layer address of the target node. This change does not introduce any new security vulnerabilities.

Network firewalls and Deep Packet inspection tools that perform any such checks, matching the destination address types in the IPv6 header and the link-layers have to modified to allow such packet transmission. However, the authors of this document could not find a single existing implementation that performs this check.

6. Acknowledgements

The authors would like to acknowledge Stig Venaas, Fred Baker, Dave Thaler, Phil Roberts, Mark Smith, Hemant Singh, Wes Beebee, Olaf Bonness, Suresh Krishnan, Behcet Sarikaya, Eric Levy, Pascal Thubert, Alain Durand, Jean-Michel Combes, and Eric Voit for all the discussions on this topic.

7. References

7.1. Normative References

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

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

7.2. Informative References

[I-D.costa-6man-dad-proxy-00] Costa, F., Combes, J-M., Pougnard, X., and H. Li, "Duplicate Address Detection Proxy", draft-costa-6man-dad-proxy (work in progress).

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.

Authors' Addresses

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: sgundave@cisco.com

Mark Townsley
Cisco
L'Atlantis, 11, Rue Camille Desmoulins
ISSY LES MOULINEAUX, ILE DE FRANCE 92782
France

Email: townsley@cisco.com

Ole Troan
Cisco
Skoyen Atrium, Drammensveien 145A
Oslo, N-0277
Norway

Email: otroan@cisco.com

Wojciech Dec
Cisco
Haarlerbergweg 13-19
Amsterdam, Noord-Holland 1101 CH
Netherlands

Email: wdec@cisco.com