v6ops WG
Internet-Draft
Intended status: Standards Track
Expires: January 26, 2011

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

July 25, 2010

Unicast Transmission of IPv6 Multicast Messages on Link-layer
draft-gundavelli-v6ops-l2-unicast-01.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 a need to transmit an IPv6 multicast 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 January 26, 2011.

Table of Contents

1. Introduction

This document is about a clarification to the construction and processing rules of IPv6 multicast messages. This clarification makes it valid for an IPv6 receiver node to consider a received IPv6 multicast message with a multicast destination address in the IPv6 header, but containing a unicast destination address in the link-layer header, to be valid withstanding all other validity considerations specified in the IPv6 standards specifications. Consequentially, it is also legal for an IPv6 sender node to transmit an IPv6 multicast message as a unicast message on the link-layer. This change follows the principles of protocol layer design more tightly.

There are various deployment scenarios where there is a need to transmit an IPv6 multicast message as an unicast message on the link-layer. For example, an 802.11 wireless access point may be hosting multiple IPv6 subnets/VLAN's and it would need the ability to selectively advertise hosted IPv6 prefixes on a per-node basis. Such segregation can only be possible by ensuring the Router Advertisements received by any IPv6 node includes only those prefixes that are associated with their respective layer-3 subnet. This essentially requires the ability to transmit IPv6 multicast messages as unicast messages on the link-layer. Another such example where this semantic is needed is in ISATAP [RFC5214] for sending a unicast Router Advertisement message on ISTAP interfaces. However, it is ambiguous from the protocol specification perspective, on the legality of such transmission and any discussions on this subject always resulted in differing opinions. Therefore, it is the intent of this document to make the specification clear on this aspect.

The function of the link-layer is purely for transmitting the frame to a peer or to a set of peers on a given media. A received multicast message may have been transmitted as a unicast message on the link-layer and so the destination address in the link-layer 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 to go across the layers and check the semantics of message delivery in the link-layer header. 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, 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. Case and Point:

- Microsoft Windows Vista
- Linux Operating System
- Cisco IOS Operating System
- BSD Variants based on IPv6 KAME implementation

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 3.0 of this document defines the additional normative considerations for IPv6 sender and receiver nodes for allowing 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, withstanding all other validity considerations as specified in the relevant IPv6 standards specifications.

- An IPv6 sender node MAY choose to transmit an IPv6 multicast message as a link-layer unicast message. 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. It is up to to the system architecture as when to transmit an IPv6 multicast message as an link-layer unicast message.

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 makes it valid for an IPv6 receiver node to consider a received IPv6 multicast message with a multicast destination address in the IPv6 header, but containing an unicast destination address in the link-layer header, to be valid withstanding all other validity considerations specified in the IPv6 standards specifications. This change follows the principles of protocol layer design more tightly and does not introduce any security vulnerabilities.

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

6. Acknowledgements

The authors would like to acknowledge Stig Venaas, Fred Baker, Hemant Singh, Olaf Bonness, Suresh Krishnan, Behcet Sarikaya, Eric Levy, Pascal Thubert 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

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

[RFC5214] Templin, F., Gleeson, T., and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", RFC 5214, March 2008.

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