Network Working Group
Internet Draft
Intended status: Standards

Rajiv Asati
Toerless Eckert
Cisco
March 7, 2011

Expires: September 2011

# Time To Live (TTL) Guideline for Link-Local-Scope Multicast Packets
## draft-asati-eckert-multicast-local-ttl-00.txt

Abstract

This document specifies the value for the Time-to-Live in an IP packet that is destined to a link-local scope IP multicast address. These guidelines may be used for verification purposes.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

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/1id-abstracts.txt

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

This Internet-Draft will expire on September 7, 2011.

Table of Contents



## 1. Introduction

It has been a common practice to encode Time to Live (TTL) for the IP multicast packets that have link-local scope,

There has not been any standard document that specified the TTL value for the IPv4 multicast packets (such as the ones belonging to the protocols listed below) that have link-local scope, even though a common practice has been to encode the smallest Time to Live (TTL) value (=1).

- Protocol Independent Multicast (PIM) [RFC4601]
- IGMP/MLD
- Routing Protocol (OSPF, EIGRP etc.) Discovery

o LDP Discovery

This document specifies the IPv4 TTL value for such link-local multicast packets.

Note: This document does not define any behavior for link-local scope IP unicast packets.

## 2. Conventions used in this document

In examples, "C:" and "S:" indicate lines sent by the client and server respectively.

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 [RFC2119].

## 3. TTL Value

This document specifies that any protocol generating link-local IPv4 multicast packets must encode the corresponding TTL value to be one (= 1).

IPv6 Neighbor Discover (ND) [RFC4861] is excluded from this for historic reasons (see below).

## 4. Security Considerations

This specification improves the security of many link-local protocols.

## 5. IANA Considerations

None.

## 6. Conclusions

This document specifies the value = 1 for IPv4 TTL to be used on IP multicast packets that are not meant to be forwarded beyond the first hop.

## 7. Appendix

### 7.1. Discussion TTL=1 or TTL=255

The use of a TTL=1 for link-local-scope IP multicast packets evolved out of the logic that link-local-scope networks have a hop-count of

1 and that limiting the TTL of such packets to 1 did provide appropriate protection against such packets leaking to other subnets.

GTSM was introduced for unicast packets first, specifying a TTL of 255 and filtering of packets with a TTL smaller than 255 on receipt. This was used as a mean to protect against attackers from other networks sending packets with a TTL just large enough that it would end up as a TTL of 1 on the target network.

Attacks such as those that GTSM protects against are not possible with link-local scope IP multicast packets because all devices that forward IP multicast packets and decrement the TTL are IP multicast routers that do not forward link-local scope IP multicast packets at all. There is no indication that any devices exist that break this standard behavior. If one would choose to recommend GTSM for link-local IP multicast packets on the premise of unknown devices, then one should even more be concerned about unknown devices forwarding link-local IP multicast packets without decrementing the TTL.

In IPv6 ND, a TTL of 255 is used, based on the early premise that link-local-scope in IPv6 could optionally include networks with more than one hop. This premise was later dropped, so the use of TTL=255 in ND is mostly for historic reasons.

## 8. References

### 8.1. Normative References

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

### 8.2. Informative References

[RFC4861] Narten, T., et. al, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.

[RFC5796] Atwood, W., Islam, S., and Siami, M., "Authentication and Confidentiality in Protocol Independent Multicast Sparse Mode (PIM-SM) Link-Local Messages", RFC 5796, March 2010.

## 9. Acknowledgments

The authors would like to thank Stig Venaas for his review.

This document was prepared using 2-Word-v2.0.template.dot.

Authors' Addresses

Rajiv Asati
Cisco
7025 Kit Creek Rd, RTP, NC 27709
Email: rajiva@cisco.com

Toerless Eckert
Cisco
510 McCarthy Blvd., Milpitas, CA 95035
Email: eckert@cisco.com