Layer 2 (L2) LISP Encapsulation Format
draft-smith-lisp-layer2-00.txt

Abstract

This memo describes an encapsulation method for carrying Ethernet and IEEE 802 media access control (MAC) frames within the Locator/ID Separation Protocol (LISP).

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), 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 11, 2011.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents
1. Introduction

LISP [LISP] specifies an architecture and method for separating the location of an endpoint from its network identifier. It does this by using two separate name spaces: EIDs representing the network identifier of the endpoint and RLOCs representing the network location of the endpoint. This document extends the LISP specifications to allow Ethernet/IEEE 802 MAC frames to be carried within the LISP frame. The MAC addresses of the encapsulated Ethernet/IEEE 802 MAC frames will be used as EIDs.

2. Conventions used in this document

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].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC-2119 significance.
3. Basic Overview

L2 LISP specifies the mechanism on which to carry L2 traffic over a LISP network. Within an L2 LISP environment, the source and destination MAC addresses of the Ethernet/IEEE 802.3 packet are used as the source and destination EIDs. The RLOCs can use IPv4 or IPv6 addressing. The entire MAC frame is encapsulated with the exception of the preamble and trailing FCS. It should be noted that L2 LISP introduces the possibility of packet reordering during route topology changes due to the usage of IP as the network substrate.

This memo addresses the data plane and frame format details of L2 LISP. The control plane details are outside the scope of this memo.
4. L2 LISP Encapsulation Details

The L2 LISP encapsulation is based on the LISP header defined in the LISP specification [LISP]. The UDP and LISP headers are shown below for reference.

When the headers are used for encapsulating L2 frames, the following settings are required:

The "Not Used" fields may be enabled in the future for usage in L2 LISP by allocating an unused bit in the flags field. This will be defined within the main LISP specification [LISP].

4.1. Header Field Descriptions

UDP Header: The UDP header contains a ITR selected source port when encapsulating a L2 LISP packet. The source port allows routers and bridges in the network to load-split the traffic across the equal cost paths available. The choice of the source port SHOULD be made based on a hash of some combination of the inner frame header fields such as but not limited to the source MAC address,
destination MAC address, Length/Ethertype, and IP header fields if present. The destination port MUST be set to the well-known IANA assigned port value 8472.

UDP Length: The UDP length field is for an IPv4 encapsulated packet, the length of the inner L2 frame plus the UDP and LISP header lengths are used. For an IPv6 encapsulated packet, the length of the inner L2 frame plus the size of the IPv6 header (40 bytes) plus the size of the UDP and LISP headers are used. The UDP header length is 8 bytes.

UDP Checksum: The UDP checksum field is used in accordance with the LISP specification [LISP].

I: The I bit is the Instance ID bit. When this bit is set to 1, it indicates that the Instance ID field carried the LISP header is valid. In L2 LISP, this bit MUST be set to 1.

Instance ID: An EID is scoped within the virtual L2 network which is specified through the usage of the Instance ID field. The Instance ID namespace is contained within a single administrative domain. The 24-bit Instance ID field is used in accordance with the LISP specification [LISP].

5. MTU Considerations

Since additional tunnel headers are prepended, the packet becomes larger and can exceed the MTU of any link traversed from the ITR to the ETR. It is recommended in IPv4 that packets do not get fragmented as they are encapsulated by the ITR.

6. Security Considerations

Security in a network carrying L2 LISP should be similar to security in a normal IPv4 network. Packet filtering on the L2 LISP inner frames will require that a firewall look inside the L2 LISP packet or that filtering is done at the ITR/ETR.

7. IANA Considerations

The IANA registry has allocated UDP port number 8472 for the L2 LISP data packets.
8. References

8.1. Normative References


8.2. Informative References

9. Acknowledgments

The authors would like to thank Dino Farinacci, Sumeet Singh, Ajit Sanzgiri, and Larry Kreeger for their technical and editorial commentary.

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

Michael Smith
Cisco Systems
Tasman Drive
San Jose, CA 95134

Email: michsmit@cisco.com

Dinesh Dutt
Cisco Systems
Tasman Drive
San Jose, CA 95134

Email: ddutt@cisco.com