**LISP EID Anonymity**
**draft-farinacci-lisp-eid-anonymity-01**

Abstract

   This specification will describe how ephemeral LISP EIDs can be used
   to create source anonymity.  The idea makes use of frequently
   changing EIDs much like how a credit-card system uses a different
   credit-card numbers for each transaction.

Requirements Language

   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].

Status of This Memo

Copyright Notice

Table of Contents

## 1.  Introduction

   The LISP architecture [RFC6830] specifies two namespaces, End-Point
   IDs (EIDs) and Routing Locators (RLOCs).  An EID identifies a node in
   the network and the RLOC indicates the EID's topological location.
   Typically EIDs are globally unique so a end-node system can connect
   to any other end-node system on the Internet.  Privately used EIDs
   are allowed when scoped within a VPN but must always be unique within
   that scope.  Therefore, address allocation is required by network
   administration to avoid address collisions or duplicate address use.
   In a multiple namespace architecture like LISP, typically the EID
   will stay fixed while the RLOC can change.  This occurs when the EID
   is mobile or when the LISP site the EID resides in changes its
   connection to the Internet.

   LISP creates the opportunity where EIDs are fixed and won't change.
   This can create a privacy problem more so than what we have on the
   Internet today.  This draft will examine a technique to allow a end-
   node system to use a temporary address.  The lifetime of a temporary
   address can be the same as a lifetime of an address in use today on
   the Internet or can have traditionally shorter lifetimes, possibly on

the order of a day or even change as frequent as new connection
attempts.

## 2.  Definition of Terms

Ephemeral-EID -  is an IP address that is created randomly for use
   for a temporary period of time.  An Ephemeral-EID has all the
   properties of an EID as defined in [RFC6830].  Ephemeral-EIDs are
   not stored in the Domain Name System (DNS) and should not be used
   in long-term address referrals.

Client End-Node -  is a network node that originates and consumes
   packets.  It is a system that originates packets or initiates the
   establishment of transport-layer connections.  It does not offer
   services as a server system would.  It accesses servers and
   attempts to do it anonymously.

## 3.  Overview

A client end-node can assign its own ephemeral EID and use it to talk
to any system on the Internet.  The system is acting as a client
where it initiates communication and desires to be an inaccessible
resource from any other system.  The ephemeral EID is used as a
destination address solely to return packets to resources the
ephemeral EID connects to.

Here is the procedure a client end-node would use:

1.  Client end-node desires to talk on the network.  It creates and
    assigns an ephemeral-EID on any interface.

2.  If the client end-node is a LISP xTR, it will register the
    ephemeral-EID with a globally routable RLOC.  If the client end-
    node is not a LISP xTR, it can send packets on the network where
    a LISP router xTR will register the ephemeral-EID with its RLOC.

3.  The client end-node originates packets with a source address
    equal to the ephemeral-EID and will receive packets addressed to
    the ephemeral-EID.

4.  When the client end-node decides to stop using the ephemeral-EID,
    it will deregister it from the mapping system and create and
    assign a new ephemeral-EID, or decide to configure a static
    global address, or participate in DHCP to get assigned a leased
    address.

   Note that the ephemeral-EID can be mobile just like any other EID so
   if it is initially registered to the mapping system with one or more
   RLOCs, later the RLOC-set can change as the ephemeral-EID roams.

4.  Design Details

   This specification proposes the use of the experimental LISP EID-
   block 2001:5::/32 when IPv6 is used.  See IANA Considerations section
   for a specific sub-block allocation request.  When IPv4 is used, the
   Class E block 240.0.0.0/4 is being proposed.

   The client end-node system will use the rest of the host bits to
   allocate a random number to be used as the ephemeral-EID.  The EID
   can be created manually or via a programatic interface.  When the EID
   address is going to change frequently, it is suggested to use a
   programatic interface.  The probability of address collision is
   unlikely for IPv6 EIDs but could occur for IPv4 EIDs.  A client end-
   node can create a ephemeral-EID and then look it up in the mapping
   system to see if it exists.  If the EID exists in the mapping system,
   the client end-node can attempt creation of a new random number for
   the ephemeral-EID.  See Section 7 where ephemeral-EIDs can be
   preallocated and registered to the mapping system before use.

   When the client end-node system is co-located with the RLOC and acts
   as an xTR, it should register the binding before sending packets.
   This eliminates a race condition for returning packets not knowing
   where to encapsulate packets to the ephemeral-EID's RLOCs.  When the
   client end-node system is not acting as an xTR, it should send some
   packets so its ephemeral-EID can be discovered by an xTR which
   supports EID-mobility [I-D.portoles-lisp-eid-mobility] so mapping
   system registration can occur before the destination returns packets.
   See Section 7 for alternatives for fixing this race condition
   problem.

5.  Interworking Considerations

   If a client end-node is communicating with a system that is not in a
   LISP site, the procedures from [RFC6832] should be followed.  The
   PITR will be required to originate route advertisements for the
   ephemeral-EID sub-block [I-D.draft-ietf-lisp-eid-block] so it can
   attract packets sourced by non-LISP sites destined to ephemeral-EIDs.
   However, in the general case, the coarse block from
   [I-D.draft-ietf-lisp-eid-block] will be advertised which would cover
   the sub-block.  For IPv4, the 240.0.0.0/4 must be advertised into the
   IPv4 routing system.

6.  **Multicast Considerations**

   A client end-node system can be a member of a multicast group fairly
   easily since its address is not used for multicast communication as a
   receiver.  This is due to the design characteristics of IGMP
   [RFC3376] [RFC2236] [RFC1112] and MLD [RFC2710] [RFC3810].

   When a client end-node system is a multicast source, there is
   ephemeral (S,G) state that is created and maintained in the network
   via multicast routing protocols such as PIM [RFC4602] and when PIM is
   used with LISP [RFC6802].  In addition, when
   [I-D.draft-ietf-lisp-signal-free-multicast] is used, ephemeral-EID
   state is created in the mapping database.  This doesn't present any
   problems other than the amount of state that may exist in the network
   if not timed out and removed promptly.

   However, there exists a multicast source discovery problem when PIM-
   SSM [RFC4607] is used.  Members that join (S,G) channels via out of
   band mechanisms.  These mechanisms need to support ephemeral-EIDs.
   Otherwise, PIM-ASM [RFC4602] or PIM-Bidir [RFC5015] will need to be
   used.

7.  **Performance Improvements**

   An optimization to reduce the race condition between registering
   ephemeral-EIDs and returning packets as well as reducing the
   probability of ephemeral-EID address collision is to preload the
   mapping database with a list of ephemeral-EIDs before using them.  It
   comes at a expense of rebinding all of registered ephemeral-EIDs when
   there is an RLOC change.  There is work in progress to consider
   adding a level of indirection here so a single entry gets the RLOC
   update and the list of ephemeral-EIDs point to the single entry.

8.  **Security Considerations**

   When LISP-crypto [I-D.draft-ietf-lisp-crypto] is used the EID payload
   is more secure through encryption providing EID obfuscation of the
   ephemeral-EID as well as the global-EID it is communicating with.
   But the obfuscation only occurs between xTRs.  So the randomness of a
   ephemeral-EID inside of LISP sites provide a new level of privacy.

9.  **IANA Considerations**

   This specification is requesting the sub-block 2001:5:ffff::/48 for
   ephemeral-EID usage.

## 10.  References

### 10.1.  Normative References

   [RFC1112]  Deering, S., "Host extensions for IP multicasting", STD 5,
              RFC 1112, DOI 10.17487/RFC1112, August 1989,
              <http://www.rfc-editor.org/info/rfc1112>.

   [RFC2119]  Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <http://www.rfc-editor.org/info/rfc2119>.

   [RFC2236]  Fenner, W., "Internet Group Management Protocol, Version
              2", RFC 2236, DOI 10.17487/RFC2236, November 1997,
              <http://www.rfc-editor.org/info/rfc2236>.

   [RFC2710]  Deering, S., Fenner, W., and B. Haberman, "Multicast
              Listener Discovery (MLD) for IPv6", RFC 2710,
              DOI 10.17487/RFC2710, October 1999,
              <http://www.rfc-editor.org/info/rfc2710>.

   [RFC3376]  Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A.
              Thyagarajan, "Internet Group Management Protocol, Version
              3", RFC 3376, DOI 10.17487/RFC3376, October 2002,
              <http://www.rfc-editor.org/info/rfc3376>.

   [RFC3810]  Vida, R., Ed. and L. Costa, Ed., "Multicast Listener
              Discovery Version 2 (MLDv2) for IPv6", RFC 3810,
              DOI 10.17487/RFC3810, June 2004,
              <http://www.rfc-editor.org/info/rfc3810>.

   [RFC4602]  Pusateri, T., "Protocol Independent Multicast - Sparse
              Mode (PIM-SM) IETF Proposed Standard Requirements
              Analysis", RFC 4602, DOI 10.17487/RFC4602, August 2006,
              <http://www.rfc-editor.org/info/rfc4602>.

   [RFC4607]  Holbrook, H. and B. Cain, "Source-Specific Multicast for
              IP", RFC 4607, DOI 10.17487/RFC4607, August 2006,
              <http://www.rfc-editor.org/info/rfc4607>.

   [RFC5015]  Handley, M., Kouvelas, I., Speakman, T., and L. Vicisano,
              "Bidirectional Protocol Independent Multicast (BIDIR-
              PIM)", RFC 5015, DOI 10.17487/RFC5015, October 2007,
              <http://www.rfc-editor.org/info/rfc5015>.

   [RFC6802]  Baillargeon, S., Flinta, C., and A. Johnsson, "Ericsson
              Two-Way Active Measurement Protocol (TWAMP) Value-Added
              Octets", RFC 6802, DOI 10.17487/RFC6802, November 2012,
              <http://www.rfc-editor.org/info/rfc6802>.

   [RFC6830]  Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "The
              Locator/ID Separation Protocol (LISP)", RFC 6830,
              DOI 10.17487/RFC6830, January 2013,
              <http://www.rfc-editor.org/info/rfc6830>.

   [RFC6832]  Lewis, D., Meyer, D., Farinacci, D., and V. Fuller,
              "Interworking between Locator/ID Separation Protocol
              (LISP) and Non-LISP Sites", RFC 6832,
              DOI 10.17487/RFC6832, January 2013,
              <http://www.rfc-editor.org/info/rfc6832>.

## 10.2.  Informative References

   [I-D.draft-ietf-lisp-crypto]
              Farinacci, D. and B. Weis, "LISP Data-Plane
              Confidentiality", draft-ietf-lisp-crypto-03 (work in
              progress).

   [I-D.draft-ietf-lisp-eid-block]
              Iannone, L., Lewis, D., Meyer, D., and V. Fuller, "LISP
              EID Block", draft-ietf-lisp-eid-block-13.txt (work in
              progress).

   [I-D.draft-ietf-lisp-signal-free-multicast]
              Farinacci, D. and V. Moreno, "Signal-Free LISP Multicast",
              draft-ietf-lisp-signal-free-multicast-00.txt (work in
              progress).

   [I-D.portoles-lisp-eid-mobility]
              Portoles-Comeras, M., Ashtaputre, V., Moreno, V., Maino,
              F., and D. Farinacci, "LISP L2/L3 EID Mobility Using a
              Unified Control Plane", draft-portoles-lisp-eid-
              mobility-01 (work in progress), October 2016.

## Appendix A.  Acknowledgments

   The author would like to thank the LISP WG for their review and
   acceptance of this draft.

## Appendix B.  Document Change Log

   [RFC Editor: Please delete this section on publication as RFC.]

### B.1.  Changes to draft-farinacci-lisp-eid-anonymity-01

   o  Posted October 2016.

   o  Update document timer.

### B.2.  Changes to draft-farinacci-lisp-eid-anonymity-00

   o  Posted April 2016.

   o  Initial posting.

Authors' Addresses

   Dino Farinacci
   lispers.net
   San Jose, CA
   USA

   Email: farinacci@gmail.com


   Padma Pillay-Esnault
   Huawei Technologies
   San Clara, CA
   USA

   Email: padma@huawei.com