           Interworking between Locator/ID Separation Protocol (LISP) and
                            Non-LISP Sites

Abstract

   This document describes techniques for allowing sites running the
   Locator/ID Separation Protocol (LISP) to interoperate with Internet
   sites that may be using either IPv4, IPv6, or both but that are not
   running LISP. A fundamental property of LISP-speaking sites is that
   they use Endpoint Identifiers (EIDs), rather than traditional IP
   addresses, in the source and destination fields of all traffic they
   emit or receive. While EIDs are syntactically identical to IPv4 or
   IPv6 addresses, normally routes to them are not carried in the global
   routing system, so an interoperability mechanism is needed for non-
   LISP-speaking sites to exchange traffic with LISP-speaking sites.
   This document introduces three such mechanisms. The first uses a new
   network element, the LISP Proxy Ingress Tunnel Router (Proxy-ITR), to
   act as an intermediate LISP Ingress Tunnel Router (ITR) for non-LISP-
   speaking hosts. Second, this document adds Network Address
   Translation (NAT) functionality to LISP ITRs and LISP Egress Tunnel
   Routers (ETRs) to substitute routable IP addresses for non-routable
   EIDs. Finally, this document introduces the Proxy Egress Tunnel
   Router (Proxy-ETR) to handle cases where a LISP ITR cannot send
   packets to non-LISP sites without encapsulation.

Status of This Memo

   This document is not an Internet Standards Track specification; it is
   published for examination, experimental implementation, and
   evaluation.

   This document defines an Experimental Protocol for the Internet
   community. This document is a product of the Internet Engineering
   Task Force (IETF). It represents the consensus of the IETF
   community. It has received public review and has been approved for
   publication by the Internet Engineering Steering Group (IESG). Not
   all documents approved by the IESG are a candidate for any level of
   Internet Standard; see Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc6832.

Copyright Notice

Table of Contents

1. Introduction

   This document describes interoperation mechanisms between LISP
   [RFC6830] sites that use EIDs that are not globally routed, and
   non-LISP sites. A key behavior of the separation of Locators and
   Endpoint IDs is that EID-Prefixes are normally not advertised into
   the Internet's Default-Free Zone (DFZ). (See Section 4 for the
   exception case.) Specifically, only Routing Locators (RLOCs) are
   carried in the Internet's DFZ. Existing Internet sites (and their
   hosts) that do not run LISP must still be able to reach sites
   numbered from LISP EID space. This document describes three
   mechanisms that can be used to provide reachability between sites
   that are LISP-capable and those that are not.

The first mechanism uses a new network element, the LISP Proxy
Ingress Tunnel Router (Proxy-ITR), to act as an intermediate LISP
Ingress Tunnel Router (ITR) for non-LISP-speaking hosts. The second
mechanism adds a form of Network Address Translation (NAT)
functionality to Tunnel Routers (xTRs, where "xTR" refers to either
an ITR or ETR), to substitute routable IP addresses for non-routable
EIDs. The final network element is the LISP Proxy Egress Tunnel
Router (Proxy-ETR), which acts as an intermediate Egress Tunnel
Router (ETR) for LISP sites that need to encapsulate LISP packets
destined to non-LISP sites.

More detailed descriptions of these mechanisms and the network
elements involved may be found in the following sections:

- Section 2 defines terms used throughout this document.

- Section 3 describes the different cases where interworking
   mechanisms are needed.

- Section 4 describes the relationship between the new EID-Prefix
   space and the IP address space used by the current Internet.

- Section 5 introduces and describes the operation of Proxy-ITRs.

- Section 6 introduces and describes the operation of Proxy-ETRs.

- Section 7 defines how NAT is used by ETRs to translate
   non-routable EIDs into routable IP addresses.

- Section 8 describes the relationship between asymmetric and
   symmetric interworking mechanisms (Proxy-ITRs and Proxy-ETRs vs.
   LISP-NAT).

Note that any successful interworking model should be independent of
any particular EID-to-RLOC mapping algorithm. This document does not
comment on the value of any of the particular LISP mapping systems.

Several areas concerning the interworking of LISP and non-LISP sites
remain open for further study. These areas include an examination of
the impact of LISP-NAT on Internet traffic and applications,
understanding the deployment motivations for the deployment and
operation of Proxy Tunnel Routers, the impact of EID routes
originated into the Internet's Default-Free Zone, and the effects of
Proxy Tunnel Routers or LISP-NAT on Internet traffic and
applications. Until these issues are fully understood, it is
possible that the interworking mechanisms described in this document
will be hard to deploy or may have unintended consequences to
applications.

2. Definition of Terms

     Default-Free Zone: The Default-Free Zone (DFZ) refers to the
        collection of all Internet autonomous systems that do not require
        a default route to route a packet to any destination.

     LISP Routable (LISP-R) Site: A LISP site whose addresses are used as
        both globally routable IP addresses and LISP EIDs.

     LISP Non-Routable (LISP-NR) Site: A LISP site whose addresses are
        EIDs only; these EIDs are not found in the legacy Internet routing
        table.

     LISP Proxy Ingress Tunnel Router (Proxy-ITR): Proxy-ITRs are used to
        provide connectivity between sites that use LISP EIDs and those
        that do not. They act as gateways between those parts of the
        Internet that are not using LISP (the legacy Internet). A given
        Proxy-ITR advertises one or more highly aggregated EID-Prefixes
        into the public Internet and acts as the ITR for traffic received
        from the public Internet. LISP Proxy-ITRs are described in
        Section 5.

     LISP Network Address Translation (LISP-NAT): Network address
        translation between EID space assigned to a site and RLOC space
        also assigned to that site. LISP-NAT is described in Section 7.

     LISP Proxy Egress Tunnel Router (Proxy-ETR): Proxy-ETRs provide a
        LISP (routable or non-routable EID) site's ITRs with the ability
        to send packets to non-LISP sites in cases where unencapsulated
        packets (the default mechanism) would fail to be delivered.
        Proxy-ETRs function by having an ITR encapsulate all non-LISP
        destined traffic to a pre-configured Proxy-ETR. LISP Proxy-ETRs
        are described in Section 6.

      EID Sub-Namespace: A power-of-two block of aggregatable Locators
        set aside for LISP interworking.

     For definitions of other terms -- notably Map-Request, Map-Reply,
     Ingress Tunnel Router (ITR), and Egress Tunnel Router (ETR) -- please
     consult the LISP specification [RFC6830].

3. LISP Interworking Models

    There are 4 unicast connectivity cases that describe how sites can
    send packets to each other:

    1. non-LISP site to non-LISP site

    2. LISP site to LISP site

    3. LISP site to non-LISP site

    4. non-LISP site to LISP site

    Note that while Cases 3 and 4 seem similar, there are subtle
    differences due to the way packets are originated.

    The first case is the Internet as we know it today and as such will
    not be discussed further here. The second case is documented in
    [RFC6830], and there are no new interworking requirements because
    there are no new protocol requirements placed on intermediate
    non-LISP routers.

    In Case 3, LISP site to non-LISP site, a LISP site can (in most
    cases) send packets to a non-LISP site because the non-LISP site
    prefixes are routable. The non-LISP sites need not do anything new
    to receive packets. The only action the LISP site needs to take is
    to know when not to LISP-encapsulate packets. An ITR knows
    explicitly that the destination is non-LISP if the destination IP
    address of an IP packet matches a (negative) Map-Cache entry that has
    the action 'Natively-Forward'.

    There could be some situations where (unencapsulated) packets
    originated by a LISP site may not be forwarded to a non-LISP site.
    These cases are reviewed in Section 6 (Proxy Egress Tunnel Routers).

    Case 4, typically the most challenging, occurs when a host at a
    non-LISP site wishes to send traffic to a host at a LISP site. If
    the source host uses a (non-globally routable) EID as the destination
    IP address, the packet is forwarded inside the source site until it
    reaches a router that cannot forward it (due to lack of a default
    route), at which point the traffic is dropped. For traffic not to be
    dropped, some mechanism to make this destination EID routable must be
    in place. Sections 5 (Proxy-ITRs) and 7 (LISP-NAT) describe two such
    mechanisms. Case 4 also applies to non-LISP packets (as in Case 3)
    that are returning to the LISP site.

4. Routable EIDs

   An obvious way to achieve interworking between LISP and non-LISP
   hosts is for a LISP site to simply announce EID-Prefixes into the
   DFZ, much like the current routing system, effectively treating them
   as "Provider-Independent" (PI) prefixes. Having a site do this is
   undesirable, as it defeats one of the primary goals of LISP -- to
   reduce global routing system state.

4.1. Impact on Routing Table

   If EID-Prefixes are announced into the DFZ, the impact is similar to
   the case in which LISP has not been deployed, because these
   EID-Prefixes will be no more aggregatable than existing PI addresses.
   Such a mechanism is not viewed as a viable long-term solution but may
   be a viable short-term way for a site to transition a portion of its
   address space to EID space without changing its existing routing
   policy.

4.2. Requirement for Sites to Use BGP

   Routable EIDs might require non-LISP sites today to use BGP to, among
   other things, originate their site's routes into the DFZ, in order to
   enable ingress Traffic Engineering. Relaxing this requirement (and
   thus potentially reducing global DFZ routing state) while still
   letting sites control their ingress Traffic Engineering policy is a
   design goal of LISP.

4.3. Limiting the Impact of Routable EIDs

   Two schemes are proposed to limit the impact of having EIDs announced
   in the current global Internet routing table:

   1. Section 5 discusses the LISP Proxy Ingress Tunnel Router, an
       approach that provides ITR functionality to bridge LISP-capable
       and non-LISP-capable sites.

   2. Section 7 discusses another approach, LISP-NAT, in which NAT
       [RFC2993] is combined with ITR functionality to limit the impact
       of routable EIDs on the Internet routing infrastructure.

4.4. Use of Routable EIDs for Sites Transitioning to LISP

   A primary design goal for LISP (and other Locator/ID separation
   proposals) is to facilitate topological aggregation of namespaces
   used for the path computation, and thus decrease global routing
   system overhead. Another goal is to achieve the benefits of improved

   aggregation as soon as possible. Individual sites advertising their
   own routes for LISP EID-Prefixes into the global routing system is
   therefore not recommended.

   That being said, single-homed sites (or multihomed sites that are not
   leaking more-specific exceptions) that are already using provider-
   aggregated prefixes can use these prefixes as LISP EIDs without
   adding state to the routing system. In other words, such sites do
   not cause additional prefixes to be advertised. For such sites,
   connectivity to a non-LISP site does not require interworking
   machinery because the "PA" (Provider-Assigned) EIDs are already
   routable (they are effectively LISP-R type sites). Their EIDs are
   found in the LISP mapping system, and their (aggregate) PA prefix(es)
   are found in the DFZ of the Internet.

   The continued announcements of an existing site's Provider-
   Independent (PI) prefix(es) is of course under the control of that
   site. Some period of transition, where a site is found both in the
   LISP mapping system, and as a discrete prefix in the Internet routing
   system, may be a viable transition strategy. Care should be taken
   not to advertise additional more-specific LISP EID-Prefixes into
   the DFZ.

5. Proxy Ingress Tunnel Routers

   Proxy Ingress Tunnel Routers (Proxy-ITRs) allow non-LISP sites to
   send packets to LISP-NR sites. A Proxy-ITR is a new network element
   that shares many characteristics with the LISP ITR. Proxy-ITRs allow
   non-LISP sites to send packets to LISP-NR sites without any changes
   to protocols or equipment at the non-LISP site. Proxy-ITRs have two
   primary functions:

   Originating EID Advertisements: Proxy-ITRs advertise highly
      aggregated EID-Prefix space on behalf of LISP sites so that
      non-LISP sites can reach them.

   Encapsulating Legacy Internet Traffic: Proxy-ITRs also encapsulate
      non-LISP Internet traffic into LISP packets and route them towards
      their destination RLOCs.

5.1. Proxy-ITR EID Announcements

   A key part of Proxy-ITR functionality is to advertise routes for
   highly aggregated EID-Prefixes into parts of the global routing
   system. Aggressive aggregation is performed to minimize the number
   of new announced routes. In addition, careful placement of
   Proxy-ITRs can greatly reduce the advertised scope of these new
   routes. To this end, Proxy-ITRs should be deployed close to

   non-LISP-speaking sites rather than close to LISP sites. Such
   deployment not only limits the scope of EID-Prefix route
   advertisements but also allows the traffic forwarding load to be
   spread among many Proxy-ITRs.

5.2. Packet Flow with Proxy-ITRs

   What follows is an example of the path a packet would take when using
   a Proxy-ITR. In this example, the LISP-NR site is given the
   EID-Prefix 192.0.2.0/24. For the purposes of this example, neither
   this prefix nor any covering aggregate are present in the global
   routing system. In other words, without the Proxy-ITR announcing
   192.0.2.0/24, if a packet with this destination were to reach a
   router in the Default-Free Zone, it would be dropped. The following
   diagram describes a high-level view of the topology:

```
                     Internet DFZ


       .------------------------------.
      /                                \
     |      Traffic Encap'd to Site's   |
     |    +-----+     RLOC(s)           |          LISP Site:
     |    |P-ITR|=========>             |
     |    +-----+                 +--+      +-----+ |
     |       |                    |PE+------+CE 1 |-|
     |       | Originated Route   +--+      +-----+ | +----+
     |       V  192.0.2.0/24         |              |-|Host|
     |                            +--|      +-----+ | +----+
     |                            |PE+------+CE 2 |-|  192.0.2.1
     |           +---+            +--+      +-----+ |
      \          |PE |                 /
       '--------------+-+-+-----------'         Site EID-Prefix:
                      |                             192.0.2.0/24
                      |      ^
                      |      |
                   +--+--+   | Traffic
     Non LISP Site: | CE  |  |  to
                   +--+--+   | 192.168.2.1
                      |      |
                   -----------
                      |
                    +----+
                    |Host|
                    +----+
```
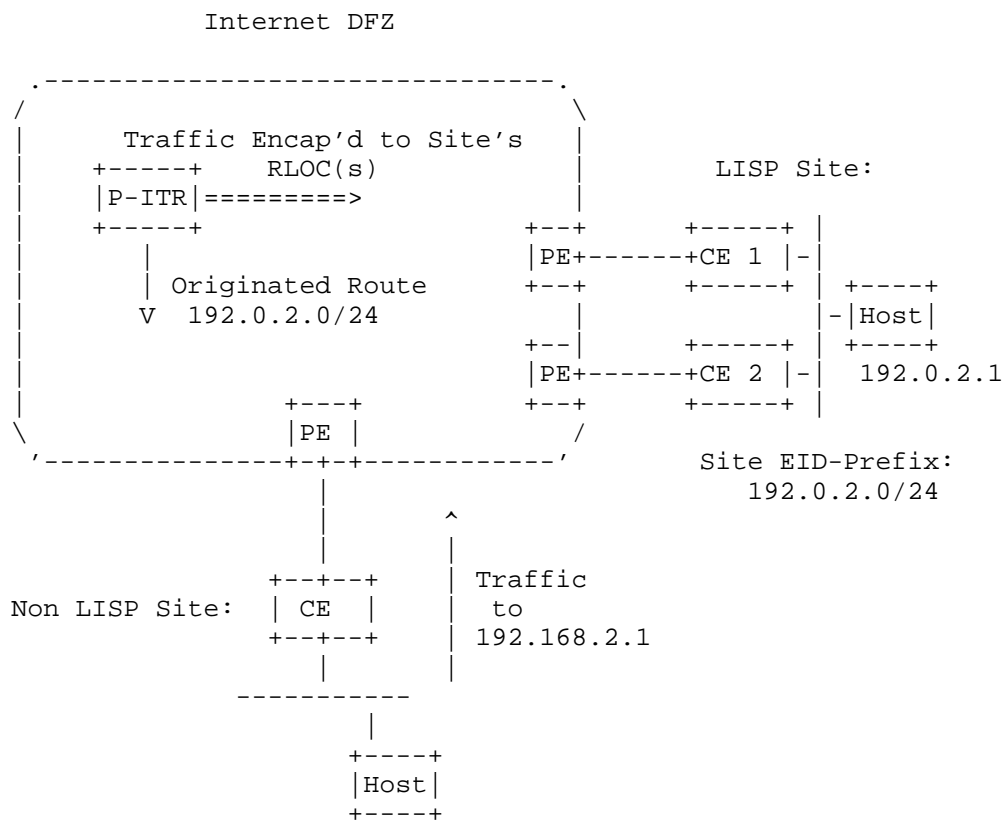
              Figure 1: Example of Proxy-ITR Packet Flow

A full protocol exchange example follows:

1. The source host makes a DNS lookup EID for the destination and
    gets 192.0.2.1 in return.

2. The source host has a default route to the Customer Edge (CE)
    router and forwards the packet to the CE.

3. The CE has a default route to its Provider Edge (PE) router and
    forwards the packet to the PE.

4. The PE has a route to 192.0.2.0/24, and the next hop is the
    Proxy-ITR.

5. The Proxy-ITR has or acquires a mapping for 192.0.2.1 and LISP-
    encapsulates the packet. The outer IP header now has a
    destination address of one of the destination EID's RLOCs. The
    outer source address of this encapsulated packet is the
    Proxy-ITR's RLOC.

6. The Proxy-ITR looks up the RLOC and forwards the LISP packet to
    the next hop, after which it is forwarded by other routers to the
    ETR's RLOC.

7. The ETR decapsulates the packet and delivers the packet to the
    192.0.2.1 host in the destination LISP site.

8. Packets from host 192.0.2.1 will flow back through the LISP
    site's ITR. Such packets are not encapsulated because the ITR
    knows that the destination (the original source) is a non-LISP
    site. The ITR knows this because it can check the LISP mapping
    database for the destination EID and on a failure determines that
    the destination site is not LISP enabled.

9. Packets are then routed natively and directly to the destination
    (original source) site.

Note that in this example the return path is asymmetric, so return
traffic will not go back through the Proxy-ITR. This is because the
LISP-NR site's ITR will discover that the originating site is not a
LISP site and will not encapsulate the returning packet (see
[RFC6830] for details of ITR behavior).

The asymmetric nature of traffic flows allows the Proxy-ITR to be
relatively simple -- it will only have to encapsulate LISP packets.

5.3. Scaling Proxy-ITRs

   Proxy-ITRs attract traffic by announcing the LISP EID namespace into
   parts of the non-LISP-speaking global routing system. There are
   several ways that a network could control how traffic reaches a
   particular Proxy-ITR to prevent it from receiving more traffic than
   it can handle:

   1. The Proxy-ITR's aggregate routes might be selectively announced,
       giving a coarse way to control the quantity of traffic attracted
       by that Proxy-ITR. For example, some of the routes being
       announced might be tagged with a BGP community and their scope of
       announcement limited by the routing policy of the provider.

   2. The same address might be announced by multiple Proxy-ITRs in
       order to share the traffic using IP Anycast. The asymmetric
       nature of traffic flows through the Proxy-ITR means that
       operationally, deploying a set of Proxy-ITRs would be very
       similar to existing anycasted services like DNS caches. Multiple
       Proxy-ITRs could advertise the same BGP Next Hop IP address as
       their RLOC, and traffic would be attracted to the nearest Next
       Hop according to the network's IGP.

5.4. Impact of the Proxy-ITR's Placement in the Network

   There are several approaches that a network could take in placing
   Proxy-ITRs. Placing the Proxy-ITR near the source of traffic allows
   the communication between the non-LISP site and the LISP site to have
   the least "stretch" (i.e., the least number of forwarding hops when
   compared to an optimal path between the sites).

   Some proposals, for example the Core Router-Integrated Overlay
   [CRIO], have suggested grouping Proxy-ITRs near an arbitrary subset
   of ETRs and announcing a 'local' subset of EID space. This model
   cannot guarantee minimum stretch if the EID-Prefix route
   advertisement points are changed (such a change might occur if a site
   adds, removes, or replaces one or more of its ISP connections).

5.5. Benefit to Networks Deploying Proxy-ITRs

   When packets destined for LISP-NR sites arrive and are encapsulated
   at a Proxy-ITR, a new LISP packet header is prepended. This causes
   the packet's destination to be set to the destination ETR's RLOC.
   Because packets are thus routed towards RLOCs, it can potentially
   better follow the Proxy-ITR network's Traffic Engineering policies
   (such as closest exit routing). This also means that providers that
   are not default-free and do not deploy Proxy-ITRs end up sending more
   traffic to expensive transit links (assuming their upstreams have

deployed Proxy-ITRs) rather than to the ETR's RLOC addresses, to
which they may well have cheaper and closer connectivity (via, for
example, settlement-free peering). A corollary to this would be that
large transit providers deploying Proxy-ITRs may attract more
traffic, and therefore more revenue, from their customers.

6. Proxy Egress Tunnel Routers

   Proxy Egress Tunnel Routers (Proxy-ETRs) allow LISP sites to send
   packets to non-LISP sites in the case where the access network does
   not allow the LISP site to send packets with the source address of
   the site's EID(s). A Proxy-ETR is a new network element that,
   conceptually, acts as an ETR for traffic destined to non-LISP sites.
   This also has the effect of allowing an ITR to avoid having to decide
   whether to encapsulate packets or not -- it can always encapsulate
   packets. An ITR would encapsulate packets destined for LISP sites
   (no change here), and these would be routed directly to the
   corespondent site's ETR. All other packets (those destined to
   non-LISP sites) will be sent to the originating site's Proxy-ETR.

   There are two primary reasons why sites would want to utilize a
   Proxy-ETR:

   Avoiding strict Unicast Reverse Path Forwarding (uRPF) failures:
      Some providers' access networks require the source of the packets
      emitted to be within the addressing scope of the access networks
      (see Section 9).

   Traversing a different IP Protocol: A LISP site may want to transmit
      packets to a non-LISP site where some of the intermediate network
      does not support the particular IP protocol desired (v4 or v6).
      Proxy-ETRs can allow this LISP site's data to 'hop over' this by
      utilizing LISP's support for mixed-protocol encapsulation.

6.1. Packet Flow with Proxy-ETRs

   Packets from a LISP site can reach a non-LISP site with the aid of a
   Proxy-ETR. An ITR is simply configured to send all non-LISP traffic,
   which it normally would have forwarded natively (non-encapsulated),
   to a Proxy-ETR. In the case where the ITR uses one or more
   Map-Resolvers, the ITR will encapsulate packets that match the
   received Negative Map-Cache to the configured Proxy-ETR(s). In the
   case where the ITR is connected to the mapping system directly, it
   would encapsulate all packets to the configured Proxy-ETR that are
   cache misses. Note that this outer encapsulation to the Proxy-ETR
   may be in an IP protocol other than the (inner) encapsulated data.
   Routers then use the LISP (outer) header's destination address to
   route the packets toward the configured Proxy-ETR.

A Proxy-ETR should verify the (inner) source EID of the packet at the
time of decapsulation in order to verify that this is from a
configured LISP site. This is to prevent spoofed inner sources from
being encapsulated through the Proxy-ETR.

What follows is an example of the path a packet would take when using
a Proxy-ETR. In this example, the LISP-NR (or LISP-R) site is given
the EID-Prefix 192.0.2.0/24, and it is trying to reach a host at a
non-LISP site with the IP prefix 198.51.100.0/24. For the purposes
of this example, the destination (198.51.100.0/24) is found in the
Internet's routing system.

A full protocol exchange example follows:

1. The source host makes a DNS lookup for the destination and gets
    198.51.100.100 (an IP address of a host in the non-LISP site) in
    return.

2. The source host has a default route to the Customer Edge (CE)
    router and forwards the packet towards the CE.

3. The CE is a LISP ITR and is configured to encapsulate traffic
    destined for non-LISP sites to a Proxy-ETR.

4. The Proxy-ETR decapsulates the LISP packet and forwards the
    original packet to its next hop.

5. The packet is then routed natively and directly to the
    destination (non-LISP) site 198.51.100.0/24.

Note that in this example the return path is asymmetric, so return
traffic will not go back through the Proxy-ETR. This means that in
order to reach LISP-NR sites, non-LISP sites must still use
Proxy-ITRs.

7. LISP-NAT

   LISP Network Address Translation (LISP-NAT) is a limited form of NAT
   [RFC2993]. LISP-NAT is designed to enable the interworking of
   non-LISP sites and LISP-NR sites by ensuring that the LISP-NR's site
   addresses are always routable. LISP-NAT accomplishes this by
   translating a host's source address from an 'inner' (LISP-NR EID)
   value to an 'outer' (LISP-R) value and keeping this translation in a
   table that it can reference for subsequent packets.

   In addition, existing RFC 1918 [RFC1918] sites can use LISP-NAT to
   talk to both LISP and non-LISP sites.

   The basic concept of LISP-NAT is that when transmitting a packet, the
   ITR replaces a non-routable EID source address with a routable source
   address, which enables packets to return to the site. Note that this
   section is intended as a rough overview of what could be done and is
   not an exhaustive guide to IPv4 NAT.

   There are two main cases that involve LISP-NAT:

   1. Hosts at LISP sites that use non-routable global EIDs speaking to
       non-LISP sites using global addresses.

   2. Hosts at LISP sites that use RFC 1918 private EIDs speaking to
       other sites, who may be either LISP or non-LISP sites.

   Note that LISP-NAT is not needed in the case of LISP-R (routable
   global EIDs) sources. This case occurs when a site is announcing its
   prefix into both the LISP mapping system and the Internet DFZ. This
   is because the LISP-R source's address is routable, and return
   packets will be able to natively reach the site.

7.1. Using LISP-NAT with LISP-NR EIDs

   LISP-NAT allows a host with a LISP-NR EID to send packets to non-LISP
   hosts by translating the LISP-NR EID to a globally unique address (a
   LISP-R EID). This globally unique address may be either a PI or PA
   address.

   An example of this translation follows. For this example, a site has
   been assigned a LISP-NR EID of 203.0.113.0/24. In order to utilize
   LISP-NAT, the site has also been provided the PA EID 192.0.2.0/24 and
   uses the first address (192.0.2.1) as the site's RLOC. The rest of
   this PA space (192.0.2.2 to 192.0.2.254) is used as a translation
   pool for this site's hosts who need to send packets to non-LISP
   hosts.

   The translation table might look like the following:

       Site NR-EID   Site R-EID   Site's RLOC   Translation Pool
       ===
       203.0.113.0/24 192.0.2.0/24   192.0.2.1   192.0.2.2-254

                    Figure 2: Example Translation Table

The host 203.0.113.2 sends a packet (which, for the purposes of this
example, is destined for a non-LISP site) to its default route (the
ITR). The ITR receives the packet and determines that the
destination is not a LISP site. How the ITR makes this determination
is up to the ITR's implementation of the EID-to-RLOC mapping system
used (see, for example, [RFC6836]).

The ITR then rewrites the source address of the packet from
203.0.113.2 to 192.0.2.2, which is the first available address in the
LISP-R EID space available to it. The ITR keeps this translation in
a table in order to reverse this process when receiving packets
destined to 192.0.2.2.

Finally, when the ITR forwards this packet without encapsulating it,
it uses the entry in its LISP-NAT table to translate the returning
packets' destination IPs to the proper host.

7.2. LISP Sites with Hosts Using RFC 1918 Addresses Sending to Non-LISP
      Sites

In the case where hosts using RFC 1918 addresses desire to send
packets to non-LISP hosts, the LISP-NAT implementation acts much like
an existing IPv4 NAT device that is doing address translation only
(not port translation). The ITR providing the NAT service must use
LISP-R EIDs for its global address pool and also provide all the
standard NAT functions required today.

Note that the RFC 1918 addresses above are private addresses and not
EIDs, and that these RFC 1918 addresses are not found in the LISP
mapping system.

The source of the packet must be translated to a LISP-R EID in a
manner similar to that discussed in Section 7, and this packet must
be forwarded to the ITR's next hop for the destination, without LISP
encapsulation.

7.3. LISP Sites with Hosts Using RFC 1918 Addresses Sending Packets to
      Other LISP Sites

LISP-NAT allows a host with an RFC 1918 address to send packets to
LISP hosts by translating the RFC 1918 address to a LISP EID. After
translation, the communication between the source and destination ITR
and ETRs continues as described in [RFC6830].

While the communication of LISP EIDs to LISP EIDs is, strictly
speaking, outside the scope of interworking, it is included here in
order to complete the conceptual framework of LISP-NAT.

   An example of this translation and encapsulation follows. For this
   example, a host has been assigned an RFC 1918 address of 192.168.1.2.
   In order to utilize LISP-NAT, the site also has been provided the
   LISP-R EID-Prefix 192.0.2.0/24 and uses the first address (192.0.2.1)
   as the site's RLOC. The rest of this PA space (192.0.2.2 to
   192.0.2.254) is used as a translation pool for this site's hosts who
   need to send packets to both non-LISP and LISP hosts.

   The host 192.168.1.2 sends a packet destined for a non-LISP site to
   its default route (the ITR). The ITR receives the packet and
   determines that the destination is a LISP site. How the ITR makes
   this determination is up to the ITR's implementation of the
   EID-to-RLOC mapping system.

   The ITR then rewrites the source address of the packet from
   192.168.1.2 to 192.0.2.2, which is the first available address in the
   LISP EID space available to it. The ITR keeps this translation in a
   table in order to reverse this process when receiving packets
   destined to 192.0.2.2.

   The ITR then LISP-encapsulates this packet (see [RFC6830] for
   details). The ITR uses the site's RLOC as the LISP outer header's
   source and the translation address as the LISP inner header's source.
   Once it decapsulates returning traffic, it uses the entry in its
   LISP-NAT table to translate the returning packet's destination IP
   address and then forwards it to the proper host.

7.4. LISP-NAT and Multiple EIDs

   With LISP-NAT, there are two EIDs possible for a given host: the
   LISP-R EID and the LISP-NR EID. When a site has two addresses that a
   host might use for global reachability, name-to-address directories
   may need to be modified.

   This problem -- global vs. local addressability -- exists for NAT in
   general, but the specific issue described above is unique to
   location/identity separation schemes. Some of these have suggested
   running a separate DNS instance for new types of EIDs. This solves
   the problem but introduces complexity for the site. Alternatively,
   using Proxy-ITRs can mitigate this problem, because the LISP-NR EID
   can be reached in all cases.

8. Discussion of Proxy-ITRs, LISP-NAT, and Proxy-ETRs

   In summary, there are three suggested mechanisms for interworking
   LISP with non-LISP sites (for both IPv4 and IPv6). In the LISP-NAT
   option, the LISP site can manage and control the interworking on its
   own. In the Proxy-ITR case, the site is not required to manage the

advertisement of its EID-Prefix into the DFZ, with the cost of
potentially adding stretch to the connections of non-LISP sites
sending packets to the LISP site. The third option is Proxy-ETRs,
which are optionally used by sites relying on Proxy-ITRs to mitigate
two caveats for LISP sites sending packets to non-LISP sites. This
means Proxy-ETRs are not usually expected to be deployed by
themselves; rather, they will be used to assist LISP-NR sites that
are already using Proxy-ITRs.

8.1. How Proxy-ITRs and Proxy-ETRs Interact

There is a subtle difference between symmetrical (LISP-NAT) and
asymmetrical (Proxy-ITR and Proxy-ETR) interworking techniques.
Operationally, Proxy-ITRs and Proxy-ETRs can (and likely should) be
decoupled, since Proxy-ITRs are best deployed closest to non-LISP
sites and Proxy-ETRs are best located close to the LISP sites they
are decapsulating for. This asymmetric placement of the two network
elements minimizes the stretch imposed on each direction of the
packet flow while still allowing for coarsely aggregated
announcements of EIDs into the Internet's routing table.

9. Security Considerations

Like any router or LISP ITR, Proxy-ITRs will have the opportunity to
inspect traffic at the time that they encapsulate. The location of
these devices in the network can have implications for discarding
malicious traffic on behalf of ETRs that request this behavior (by
setting the ACT (action) bit in Map-Reply packets [RFC6830] to "Drop"
for an EID or EID-Prefix). This is an area that would benefit from
further experimentation and analysis.

LISP interworking via Proxy-ITRs should have no impact on the
existing network beyond what LISP ITRs and ETRs introduce when
multihoming. That is, if a site multihomes today (with LISP or BGP),
there is a possibility of asymmetric flows.

Proxy-ITRs and Proxy-ETRs will likely be operated by organizations
other than those of the end site receiving or sending traffic. Care
should be taken, then, in selecting a Proxy-ITR/Proxy-ETR provider to
insure that the quality of service meets the site's expectations.

Proxy-ITRs and Proxy-ETRs share many of the same security issues as
those discussed for ITRs and ETRs. For further information, see the
security considerations section of [RFC6830].

As with traditional NAT, LISP-NAT will obscure the actual host
LISP-NR EID behind the LISP-R addresses used as the NAT pool.

When LISP sites send packets to non-LISP sites (these non-LISP sites
rely on Proxy-ITRs to enable interworking), packets will have the
site's EID as the source IP address. These EIDs may not be
recognized by their ISP's Unicast Reverse Path Forwarding (uRPF)
rules enabled on the Provider Edge router. Several options are
available to the service provider. For example, they could enable a
less strict version of uRPF, where they only look for the existence
of the EID-Prefix in the routing table. Another option, which is
more secure, is to add a static route for the customer on the PE
router but not redistribute this route into the provider's routing
table. Finally, Proxy-ETRs can enable LISP sites to bypass this uRPF
check by encapsulating all of their egress traffic destined to
non-LISP sites to the Proxy-ETR (thus ensuring that the outer IP
source address is the site's RLOC).

10. Acknowledgments

Thanks go to Christian Vogt, Lixia Zhang, Robin Whittle, Michael
Menth, Xuewei Wang, and Noel Chiappa, who have made insightful
comments with respect to LISP interworking and transition mechanisms.

A special thanks goes to Scott Brim for his initial brainstorming of
these ideas and also for his careful review.

11. References

11.1. Normative References

   [RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and
              E. Lear, "Address Allocation for Private Internets",
              BCP 5, RFC 1918, February 1996.

   [RFC6830] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "The
              Locator/ID Separation Protocol (LISP)", RFC 6830,
              January 2013.

   [RFC6836] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis,
              "Locator/ID Separation Protocol Alternative Logical
              Topology (LISP+ALT)", RFC 6836, January 2013.

11.2. Informative References

   [CRIO]   Zhang, X., Francis, P., Wang, J., and K. Yoshida, "CRIO:
              Scaling IP Routing with the Core Router-Integrated
              Overlay", November 2006.

   [RFC2993] Hain, T., "Architectural Implications of NAT", RFC 2993,
              November 2000.

Authors' Addresses

   Darrel Lewis
   Cisco Systems

   EMail: darlewis@cisco.com

   David Meyer
   Cisco Systems

   EMail: dmm@1-4-5.net

   Dino Farinacci
   Cisco Systems

   EMail: farinacci@gmail.com

   Vince Fuller

   EMail: vaf@vaf.net