Network Working Group	D. Lewis	
Internet-Draft	D. Meyer	
Intended status: Experimental	D. Farinacci	
Expires: February 27, 2011	V. Fuller	
	Cisco Systems, Inc.	
	August 26, 2010	

TOC

Interworking LISP with IPv4 and IPv6
draft-ietf-lisp-interworking-01.txt

Abstract

This document describes techniques for allowing sites running the Locator/ID Separation Protocol (LISP) to interoperate with Internet sites (which may be using either IPv4, IPv6, or both) but which 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 Routers (PITR) (Section 5) to act as a intermediate LISP Ingress Tunnel Router (ITR) for non-LISP-speaking hosts. Second the document adds Network Address Translation (NAT) functionality to LISP Ingress and LISP Egress Tunnel Routers (xTRs) to substitute routable IP addresses for non-routable EIDs. Finally, this document introduces a Proxy Egress Tunnel Router (PETR) to handle cases where a LISP ITR cannot send packets to non-LISP sites without encapsulation.

Status of this Memo

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 February 27, 2011.

Table of Contents

---

1. Introduction

TOC

This document describes interoperation between LISP [LISP] (Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, “Locator/ID Separation Protocol (LISP),” January 2010.) sites which use non-globally-routed EIDs, and non-LISP sites. The first is the use of Proxy Ingress Tunnel router (PITRs), which originate highly-aggregated routes to EID prefixes for non-LISP sites to use. It also describes the use of NAT by LISP ITRs when sending packets to non-LISP hosts. Finally, it describes Proxy Egress Tunnel routers (PETRs) LISP for sites relying on PITRs, and which are faced with certain restrictions.

A key behavior of the separation of Locators and End-Point-IDs is that EID prefixes are normally not advertised into the Internet's Default Free Zone (DFZ). Specifically, only RLOCs are carried in the Internet's DFZ. Existing Internet sites (and their hosts) which do not run in the LISP protocol must still be able to reach sites numbered from LISP EID space. This draft 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 (PITR) to act as a 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), to substitute routable IP addresses for non-routable EIDs. The final network element is the LISP Proxy Egress Tunnel Routers (PETR), which act as an intermediate Egress Tunnel Router (ETR) for LISP sites which need to encapsulate packets 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 describes the different cases where interworking mechanisms are needed
- Section 3 defines terms used throughout the document
- 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 defines how NAT is used by ETRs to translate non-routable EIDs into routable IP addresses.
- Section 7 introduces and describes the operations of Proxy-ETRs

- 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.

---

2. LISP Interworking Models

TOC

There are 4 unicast connectivity cases which 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 [LISP] 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 site need not do anything new to receive packets. The only action the LISP site needs (with two possible caveats introduced below) to take is to know when not to LISP-encapsulate packets. This can be achieved by using one of two mechanisms:

1. At the ITR in the source site, if the destination of an IP packet is found to match a prefix from the BGP routing table, then the site is directly reachable by the BGP core that exists and operates today.

2. Second, if (from the perspective of the ITR at the source site) the destination address of an IP address is not found in the EID- to-RLOC mapping database, the ITR could infer that it is not a LISP-capable site, and decide to not LISP-encapsulate the packet.

3. In either of the two exceptions mentioned above there could be some situations where (unencapsualted) packets originated by a LISP site may not be forwarded to a non-LISP site. These cases are reviewed in section 7, (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 which cannot forward tin (due to lack of a default route), at which point the traffic is dropped. For traffic not to be dropped, either some some mechanism to make this destination EID routable must be in place. Section 5 (PITRs) and Section 6 (LISP-NAT) describe two such mechanisms.
Case 4 also applies to packets returning to the LISP site, in Case 3.

---

3. Definition of Terms

TOC

Endpoint ID (EID): Endpoint ID (EID): A 32-bit (for IPv4) or 128-bit (for IPv6) value used in the source and destination address fields of the first (most inner) IP header of a packet. The host obtains a destination EID the same way it obtains an destination address today, for example through a DNS lookup or SIP exchange. The source EID is obtained via existing mechanisms used to set a host's "local" IP address. An EID is allocated to a host from an EID-prefix block associated with the site where the host is located. An EID can be used by a host to refer to other hosts. EIDs MUST NOT be used as LISP RLOCs. Note that EID blocks may be assigned in a hierarchical manner, independent of the network topology, to facilitate scaling of the mapping database. In addition, an EID block assigned to a site may have site-local structure (subnetting) for routing within the site; this structure is not visible to the global routing system. When used in discussions with other Locator/ID separation proposals, a LISP EID will be called a "LEID". Throughout this document, any references to "EID" refers to an LEID.

EID-Prefix: A power-of-2 block of EIDs which are allocated to a site by an address allocation authority. EID-prefixes are associated with a set of RLOC addresses which make up a "database mapping". EID-prefix allocations can be broken up into smaller blocks when an RLOC set is to be associated with the smaller EID-prefix. A globally routed address block (whether PI or PA) is not an EID-prefix. However, a globally routed address block may be removed from global routing and reused as an EID-prefix. A site that receives an explicitly allocated EID-prefix may not use that EID-prefix as a globally routed prefix assigned to RLOCs

EID-Prefix Aggregate: A set of EID-prefixes said to be aggregatable in the [RFC4632] (Fuller, V. and T. Li, “Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation

Plan," August 2006.) sense. That is, an EID-Prefix aggregate is defined to be a single contiguous power-of-two EID-prefix block. Such a block is characterized by a prefix and a length. Provider Independent (PI) Addresses: an address block assigned from a pool where blocks are not associated with any particular location in the network (e.g. from a particular service provider), and is therefore not topologically aggregatable in the routing system.

Routing Locator (RLOC): The IPv4 or IPv6 address of an egress tunnel router (ETR). It is the output of a EID-to-RLOC mapping lookup. An EID maps to one or more RLOCs. Typically, RLOCs are numbered from topologically-aggregatable blocks that are assigned to a site at each point to which it attaches to the global Internet; where the topology is defined by the connectivity of provider networks, RLOCs can be thought of as PA addresses. Multiple RLOCs can be assigned to the same ETR device or to multiple ETR devices at a site.

EID-to-RLOC Mapping: A binding between an EID and the RLOC-set that can be used to reach the EID. We use the term "mapping" in this document to refer to a EID-to-RLOC mapping.

EID Prefix Reachability: An EID prefix is said to be "reachable" if one or more of its locators are reachable. That is, an EID prefix is reachable if the ETR (or its proxy) is reachable.

Default Mapping: A Default Mapping is a mapping entry for EID-prefix 0.0.0.0/0. It maps to a locator-set used for all EIDs in the Internet. If there is a more specific EID-prefix in the mapping cache it overrides the Default Mapping entry. The Default Mapping route can be learned by configuration or from a Map-Reply message [LISP] (Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "Locator/ID Separation Protocol (LISP)," January 2010.).

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 (PITR): PITRs are used to provide interconnectivity between sites which use LISP EIDs and those which do not. They act as gateways between those parts of the Internet which are not using LISP (the legacy Internet) A given PITR 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 Ingress Tunnel Routers are described in Section 5 (Proxy Ingress Tunnel Routers).

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 Network Address Translation is described in Section 6 (LISP-NAT).

LISP Proxy Egress Tunnel Router (PETR): PETRs provide a LISP (Routable or Non-Routable EID) site's ITRs the ability to send packets to non-LISP sites in cases where unencapsualted packets (the default mechanism) would fail to be delivered. PETRs are function by having an ITR encapsulate all non-LISP destined traffic to a pre-configured PETR. LISP Proxy Egress Tunnel Routers are described in Section 7 (Proxy Egress Tunnel Routers).

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

---

4. Routable EIDs

TOC

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

TOC

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 addressing. 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 using BGP

TOC

Non-LISP sites today use BGP to, among other things, enable ingress traffic engineering. Relaxing this requirement is another primary design goal of LISP.

4.3. Limiting the Impact of Routable EIDs

TOC

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

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

2. Section 6 (LISP-NAT) discusses another approach, LISP-NAT, in which NAT [RFC2993] (Hain, T., “Architectural Implications of NAT,” November 2000.) is combined with ITR functionality to limit the the impact of routable EIDs on the Internet routing infrastructure.

4.4. Use of Routable EIDs for sites transitioning to LISP

TOC

A primary design goal for LISP (and other Locator/ID separation proposals) is to facilitate topological aggregation of namespace used by 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 multi-homed sites that are not leaking more specific exceptions) and 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 sites does not require interworking machinery because the "PA" 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 Internet.
The continued announcements of an existing site's Provider Independent (or "PI") prefix(es) is of course under control of that site. Some period of transition, where a site is 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.

TOC

5. Proxy Ingress Tunnel Routers

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

Originating EID Advertisements: PITRs advertise highly aggregated EID-prefix space on behalf of LISP sites to so that non-LISP sites can reach them.

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

5.1. PITR EID announcements

TOC

A key part of PITR functionality is to advertise routes for highly-aggregated EID prefixes into part of the global routing system. Aggressive aggregation is performed to minimize the number of new announced routes. In addition, careful placement of PITRs can greatly reduce the advertised scope of these new routes. To this end, PITRs should be deployed close to non-LISP-speaking rather than close to LISP sites. Such deployment not only limits the scope of EID-prefix route advertisements, it also also allows traffic forwarding load to be spread among many PITRs.

5.2. Packet Flow with PITRs

TOC

What follows is an example of the path a packet would take when using a PITR. In this example, the LISP-NR site is given the EID prefix 240.0.0.0/24. For the purposes of this example, this prefix and no covering aggregate is present in the global routing system. In other words, without the Proxy-ITR announcing 240.0.0.0/24, a packet with this destination were to reach a router in the "Default Free Zone", it would be dropped.
A full protocol exchange example follows:

1. The source host makes a DNS lookup EID for destination, and gets 240.1.1.1 in return.

2. The source host has a default route to 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 route to 240.0.0.0/24 and the next hop is the PITR.

5. The PITR has or acquires a mapping for 240.1.1.1 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 PITR's RLOC.

6. The PITR looks up the RLOC, and forwards 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 240.1.1.1 host in the destination LISP site.

8. Packets from host 240.1.1.1 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 determine 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 PITR. This is because the LISP-NR site's ITR will discover that the originating site is not a LISP site, and not encapsulate the returning packet (see [LISP] (Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, “Locator/ID Separation Protocol (LISP),” January 2010.) for details of ITR behavior).
The asymmetric nature of traffic flows allows the PITR to be relatively simple - it will only have to encapsulate LISP packets.

5.3. Scaling PITRs

TOC

PITRs 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 PITR to prevent it from receiving more traffic than it can handle:

1. The PITR's aggregate routes might be selectively announced, giving a coarse way to control the quantity of traffic attracted by that PITR. 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 PITRs 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 PITRs 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 the network's IGP.

5.4. Impact of the PITRs placement in the network

TOC

There are several approaches that a network could take in placing PITRs. Placing the PITR near the source of traffic allows for 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 CRIO [CRIO] (Zhang, X., Francis, P., Wang, J., and K. Yoshida, “CRIO:Scaling IP Routing with the Core Router-Integrated Overlay,” .), have suggested grouping PITRs 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 PITRs

TOC

When packets destined for LISP-NR sites arrive and are encapsulated at a Proxy-ITR, a new LISP packet header is pre-pended. This causes the packet's destination to be set to the destination ETRs 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 which 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 to (via, for example, settlement-

free peering). A corollary to this would be that large transit providers, deploying PITRs may attract more traffic, and therefore more revenue, from their customers.

---

6. LISP-NAT

TOC

LISP Network Address Translation (LISP-NAT) is a limited form of NAT [RFC2993] (Hain, T., “Architectural Implications of NAT,” November 2000.). 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] (Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, “Address Allocation for Private Internets,” February 1996.) sites can use LISP-NAT to talk to both LISP or 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.
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.

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 as well as 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.

6.1. Using LISP-NAT with LISP-NR EIDs

TOC

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 a 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 220.1.1.0/24. In order to utilize LISP-NAT, the site has also been provided the PA EID of 128.200.1.0/24, and

uses the first address (128.200.1.1) as the site's RLOC. The rest of this PA space (128.200.1.2 to 128.200.1.254) 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
220.1.1.0/24	128.200.1.0/24	128.200.1.1	128.200.1.2-254

Figure 1: Example Translation Table

The Host 220.1.1.2 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 not a LISP site. How the ITR makes this determination is up to the ITRs implementation of the EID-to-RLOC mapping system used (see, for example [LISP-ALT] (Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, “LISP Alternative Topology (LISP+ALT),” Febuary 2010.)).
The ITR then rewrites the source address of the packet from 220.1.1.2 to 128.200.1.2, 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 128.200.1.2.
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.

6.2. LISP Sites with Hosts using RFC 1918 Addresses Sending to non-LISP Sites

TOC

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. The ITR providing the NAT service must use LISP-R EIDs for its global address pool as well as providing all the standard NAT functions required today.
The source of the packet must be translated to a LISP-R EID in a manner similar to Section 6 (LISP-NAT), and this packet must be forwarded to the ITR's next hop for the destination, without LISP encapsulation.

TOC

6.3. 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 source and destination ITR and ETRs continues as described in [LISP] (Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "Locator/ID Separation Protocol (LISP)," January 2010.).

An example of this translation and encapsulation follows. For this example, a host has been assigned a 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 of 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 ITRs implementation of the EID/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 [LISP] 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 forward to the proper host.

6.4. LISP-NAT and multiple EIDs

TOC

When a site has two addresses that a host might use for global reachability, care must be chosen on which EID is found in DNS. For example, whether applications such as DNS use the LISP-R EID or the LISP-NR EID. This problem exists for NAT in general, but the specific issue described above is unique to LISP. Using PITRs can mitigate this problem, since the LISP-NR EID can be reached in all cases.

TOC

6.5. When LISP-NAT and PITRs used by the same LISP Site

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 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 PITRs can mitigate this problem, because the LISP-NR EID can be reached in all cases.

---

7. Proxy Egress Tunnel Routers

TOC

Proxy Egress Tunnel Routers (PETRs) allow for LISP sites to send packets to non-LISP sites in the case where the access network does not allow for the LISP site send packets with the source address of the site's EID(s). A PETR 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 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 PETR.
There are two primary reasons why sites would want to utilize a PETR:

> **Avoiding strict uRPF failures:** Some provider's 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 the some of the intermediate network does not support the particular IP protocol desired (v4 or v6). PETRs can allow this LISP site's data to 'hop over' this by utilizing LISP's support for mixed protocol encapsulation.

7.1. Packet Flow with Proxy Egress Tunnel Routers

TOC

Packets from a LISP site can reach a non-LISP site with the aid of a Proxy-ETR (or PETR). An ITR is simply configured to send all non-LISP

traffic, which it normally would have forwarded natively (non-encapsulated), to a PETR. In the case where the ITR uses the Map-Resolver interface the ITR will encapsulate packets that match its 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 PETR should verify the (inner) source EID of the packet at 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 PETR. In this example, the LISP-NR (or LISP-R) site is given the EID prefix 240.2.0.0/24, and it is trying to reach host at a non-LISP site with the IP prefix of 192.0.2.0/24. For the purposes of this example, the destination is a non-LISP site and 192.0.2.0/24 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 192.0.2.100 (a host in a non-LISP site) in return.

2. The source host has a default route to 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 192.0.2.0/24.

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.

---

8. Discussion of Proxy ITRs (PITRs), LISP-NAT, and Proxy-ETRs (PETRs)

TOC

In summary, there are three 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 PITR

case, we the site is not required to manage the advertisement of it's 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 PITRs case 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 which are already using PITRs.

8.1. How Proxy-ITRs and Proxy-ETRs Interact

TOC

There is a subtle difference between Symmetrical (LISP-NAT) vs Asymmetrical (Proxy-ITR and Proxy-ETR) Interworking techniques. Operationally, Proxy-ITRs (PITRs) and Proxy-ETRs (PETRs) 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

TOC

Like any router or LISP ITR, PITRs 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 which request this behavior (via the drop action bit in Map-Reply packets for an EID or EID prefix).
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 PITRs to enable Interworking), packets will have the Site's EID as its source IP address. These EIDs may not be recognized by their Internet Service Provider'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 the EID prefix in the routing table. Another, more secure, option 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 egressing traffic destined to non-LISP sites to the Proxy-ETR (thus ensuring the outer IP source address is the site's RLOC).

10. Acknowledgments

TOC

Thanks goes to Christian Vogt, Lixia Zhang, Robin Whittle, Michael Menth, and 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. IANA Considerations

TOC

This document creates no new requirements on IANA namespaces [RFC2434] (Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs," October 1998.).

12. References

TOC

12.1. Normative References

TOC

[LISP]	Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "Locator/ID Separation Protocol (LISP)," draft-ietf-lisp-06 (work in progress), January 2010 (TXT).
[LISP-ALT]	Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "LISP Alternative Topology (LISP+ALT)," draft-ietf-lisp-alt-03.txt (work in progress), Febuary 2010.
[LISP-MS]	Farinacci, D. and V. Fuller, "LISP Map Server," draft-ietf-lisp-ms-03.txt (work in progress), Feb 2010.
[RFC1918]	Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets," BCP 5, RFC 1918, February 1996 (TXT).
[RFC4632]	Fuller, V. and T. Li, "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan," BCP 122, RFC 4632, August 2006 (TXT).

12.2. Informative References

TOC

[CRIO]	Zhang, X., Francis, P., Wang, J., and K. Yoshida, “CRIO:Scaling IP Routing with the Core Router-Integrated Overlay.”
[RFC2434]	Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” BCP 26, RFC 2434, October 1998 (TXT, HTML, XML).
[RFC2993]	Hain, T., “Architectural Implications of NAT,” RFC 2993, November 2000 (TXT).

Authors' Addresses

TOC

	Darrel Lewis
	Cisco Systems, Inc.
Email:	darlewis@cisco.com
	David Meyer
	Cisco Systems, Inc.
Email:	dmm@cisco.com
	Dino Farinacci
	Cisco Systems, Inc.
Email:	dino@cisco.com
	Vince Fuller
	Cisco Systems, Inc.
Email:	vaf@cisco.com