Network Working Group
Internet-Draft
Intended status: Informational
Expires: February 3, 2011

D. Farinacci
V. Fuller
D. Lewis
D. Meyer
Cisco Systems, Inc.
August 2, 2010

LISP Mobile Node
draft-meyer-lisp-mn-03.txt

Abstract

This document describes how a lightweight version of LISP's ITR/ETR functionality can be used to provide seamless mobility to a mobile node. The LISP Mobility Architecture uses standard LISP functionality to provide scalable mobility for LISP mobile nodes.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

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

This Internet-Draft will expire on February 3, 2011.

Copyright Notice

Copyright (c) 2010 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

(http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

Table of Contents

1. Requirements Notation 3
2. Introduction 3
3. Definition of Terms 4
4. Architecture Overview 6
5. Design Requirements 6
5.1. User Requirements 6
5.2. Network Requirements 7
6. LISP Mobile Node Operation 7
6.1. Addressing Architecture 8
6.2. Control Plane Operation 8
6.3. Data Plane Operation 9
7. Protocol Operation 10
7.1. LISP Mobile Node to a Stationary Node in a LISP Site . . . 10
7.1.1. Handling Unidirectional Traffic 10
7.2. LISP Mobile Node to a Non-LISP Stationary Node 11
7.3. LISP Mobile Node to LISP Mobile Node 12
7.3.1. One Mobile Node is Roaming 12
7.3.2. Both Mobile Nodes are Roaming 12
7.4. Non-LISP Site to a LISP Mobile Node 13
7.5. LISP Site to LISP Mobile Node 13
8. Multicast and Mobility 13
9. RLOC Considerations 14
9.1. Mobile Node's RLOC is not Globally Routable 14
9.2. Mobile Node's RLOC is an EID 15
10. Mobility Example 16
10.1. Provisioning 17
10.2. Registration 17
11. LISP Implementation in a Mobile Node 17
12. Security Considerations 19
12.1. Proxy ETR Hijacking 19
12.2. LISP mobile node using an EID as its RLOC 19
13. Acknowledgments 19
14. IANA Considerations 19
15. References 20
15.1. Normative References 20
15.2. Informative References 21
Authors' Addresses 21

1. Requirements Notation

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].

2. Introduction

The Locator/ID Separation Protocol (LISP) [LISP] specifies an architecture and mechanism for replacing the addresses currently used in the Internet with two separate name spaces: Endpoint Identifiers (EIDs), used within sites, and Routing Locators (RLOCs), used by the transit networks that make up the Internet infrastructure. To achieve this separation, LISP defines protocol mechanisms for mapping from EIDs to RLOCs. The currently deployed mapping infrastructure is comprised of LISP Map-Servers and Map-Resolvers [LISP-MS], and is tied together with LISP+ALT [LISP-ALT].

This document specifies the behavior of a new LISP network element: the LISP Mobile Node in which a subset of LISP functionality can be implemented to provide mobile node roaming.

A LISP mobile node implements lightweight Ingress Tunnel Router and Egress Tunnel Router functionality. Design goals for the LISP mobility architecture include:

- Keeping TCP connections alive while roaming.
- Allowing the mobile node to communicate with other mobile nodes while either or both are roaming.
- Allowing the mobile node to multi-home (i.e., use multiple interfaces concurrently).
- Allow the mobile node to be a server. That is, any mobile node or stationary node can find and connect to a mobile node as a server.
- Provide shortest path bidirectional data paths between a mobile node and any other stationary or mobile node.
- Does not require fine-grained routes in the core network.
- Does not require home-agent or foreign agent network elements (and hence no triangle routing is required in the data plane [RFC3220]).

The LISP mobility architecture requires that the network use LISP

Map-Server [LISP-MS] and LISP Interworking [LISP-IW] technology to allow a LISP mobile node to roam and to be discovered in an efficient and scalable manner.

The protocol mechanisms described in this document apply those cases in which a node's IP address changes frequently. For example, when a mobile node roams, it is typically assigned a new IP address (i.e., one of its IP address changes). Similarly, a broadband subscriber may have its address change frequently; as such, a broadband subscriber can use the LISP Mobile Node mechanisms defined in this specification.

The remainder of this document is organized as follows: Section 3 defines the terms used in this document. Section 4 provides a overview of salient features of the LISP-MN architecture, and Section 5 describes design requirements for the LISP-MN architecture, Section 6 provides the detail of LISP-MN data and control plane operation. Section 7 specifies how the LISP-MN protocol operates. Section 8 specifies multicast operation for LISP mobile nodes, and Section 9 lists other considerations for the LISP-MN architecture. Section 12 outlines the security considerations for a LISP mobile node. Finally, Section 11 specifies the LISP implementation which resides in a mobile node.

3. Definition of Terms

This section defines the terms used in this document.

Stationary Node (SN): A non-mobile node who's IP address remains relatively unchanged. That is, its IP address does not change as frequently as a fast roaming mobile hand-set or broadband connection.

Endpoint ID (EID): This is the traditional LISP EID [LISP], and is the address that a LISP mobile node uses as its address for transport connections. A LISP mobile node never changes its EID, which is typically a /32 or /128 prefix and is assigned to a loopback interface. Note that the mobile node can have multiple EIDs, and these EIDs can be from different address families.

Routing Locator (RLOC): This is the traditional LISP RLOC, and is a routable address that can be used to reach a mobile node.

Ingress Tunnel Router (ITR): An ITR is a router that accepts an IP packet with a single IP header (more precisely, an IP packet that does not contain a LISP header). The router treats this "inner" IP destination address as an EID and performs an EID-to-RLOC

mapping lookup. The router then prepends an "outer" IP header with one of its globally routable RLOCs in the source address field and the result of the mapping lookup in the destination address field. Note that this destination RLOC may be an intermediate, proxy device that has better knowledge of the EID-to-RLOC mapping closer to the destination EID. In general, an ITR receives IP packets from site end-systems on one side and sends LISP-encapsulated IP packets toward the Internet on the other side. A LISP mobile node, however, when acting as an ITR LISP encapsulates all packet that it originates.

Egress Tunnel Router (ETR): An ETR is a router that accepts an IP packet where the destination address in the "outer" IP header is one of its own RLOCs. The router strips the "outer" header and forwards the packet based on the next IP header found. In general, an ETR receives LISP-encapsulated IP packets from the Internet on one side and sends decapsulated IP packets to site end-systems on the other side. A LISP mobile node, when acting as an ETR, decapsulates packets that are then typically processed by the mobile node.

LISP Mobile Node Architecture (LISP-MN Architecture): An architecture which uses LISP to provide fast roaming for mobile hand-sets.

LISP Mobile Node: A LISP capable fast roaming mobile hand-set.

Proxy ETR (PETR): An infrastructure element used to decapsulate packets sent from mobile nodes non-LISP sites. Proxy ETRs are described in [LISP-IW].

Map-cache: A data structure which contains an EID-prefix, its associated RLOCs, and the associated policy. Map-cache's are typically found in ITRs and PTRs.

Negative Map-Reply: A Negative Map-Reply is a Map-Reply that contains a coarsely aggregated non-LISP prefix. Negative Map-Replies are typically generated by Map-Resolvers, and are used to inform an ITR (mobile or stationary) that a site is not a LISP site. A LISP mobile node encapsulate packets to destinations covered by the negative Map-Reply are encapsulated to a PETR.

Proxy Tunnel Router (PTR): PTRs are used to provide interconnectivity between sites that use LISP EIDs and those that do not. They act as a gateway between the Legacy Internet and the LISP enabled Network. A given PTR advertises one or more highly aggregated EID prefixes into the public Internet and acts as the ITR for traffic received from the public Internet. Proxy Tunnel

Routers are described in [LISP-IW].

Roaming Event: A Roaming Event occurs when there is a change in a LISP mobile node's RLOC set.

4. Architecture Overview

The LISP-MN architecture described in this document uses the Map-Server/Map-Resolver service interface in conjunction with a light-weight ITR/ETR implementation in the mobile node to provide scalable fast mobility. The LISP-MN control-plane uses a Map-Server as an anchor point, which provides control-plane scalability. In addition, the LISP-MN data-plane takes advantage of shortest path routing, and therefore does not increase packet delivery latency.

5. Design Requirements

This section outlines the design requirements for the LISP-MN architecture, and is divided into User Requirements (Section 5.1) and Network Requirements (Section 5.2).

5.1. User Requirements

This section describes the user functionality that the LISP-MN architecture provides to a LISP mobile node.

Transport Connection Survivability: The LISP-MN architecture MUST allow a LISP mobile node to roam while keeping transport connections alive.

Simultaneous Roaming: The LISP-MN architecture MUST allow a LISP mobile node to talk to another LISP mobile node while both are roaming.

Multihoming: The LISP-MN architecture MUST allow for simultaneous use of multiple Internet connections by a LISP mobile node. In addition, the architecture MUST allow for the LISP mobile node to specify ingress traffic engineering policies as documented in [LISP]. That is, the mobile node must be able to specify both active/active and active/passive policies for ingress traffic.

Shortest Path Data Plane: The LISP-MN architecture MUST allow for shortest path bidirectional traffic between a LISP mobile node and a stationary node, and between a LISP mobile node and another LISP mobile node (i.e., without triangle routing in the data path). This provides a low-latency data path between the LISP mobile node

and the nodes that it is communicating with.

5.2. Network Requirements

This section describes the network functionality that the LISP-MN architecture provides to a LISP mobile node.

Routing System Scalability: The LISP-MN architecture MUST NOT require injection of fine-grained routes into the core network.

Mapping System Scalability: The LISP-MN architecture MUST NOT require additional state in the mapping system. In particular, any mapping state required to support LISP mobility MUST BE confined to the LISP mobile node's Map-Server and the ITRs which are talking to the LISP mobile node.

Component Reuse: The LISP-MN architecture MUST use existing LISP infrastructure components.

Home Agent/Foreign Agent: The LISP-MN architecture MUST NOT require the use of home-agent or foreign-agent infrastructure components [RFC3220].

Readdressing: The LISP-MN architecture MUST NOT require TCP connections to be reset when the mobile node roams. In particular, since the IP address associated with a transport connection will not change as the mobile node roams, TCP connections not reset.

6. LISP Mobile Node Operation

The LISP-MN architecture is built from three existing LISP components: A very lightweight implementation of LISP that runs in an LISP mobile node, and the existing Map-Server [LISP-MS] and Interworking [LISP-IW] infrastructures. A LISP mobile node typically sends and receives LISP encapsulated packets (exceptions include management protocols such as DHCP).

The LISP-MN architecture makes a single mobile node look like a LISP site in accordance with the LISP architecture as defined in [LISP]. The mobile node implements ITR and ETR functionality. All packets the mobile node originates are LISP encapsulated, and all packets received by a LISP mobile node will be LISP encapsulated.

When a mobile node roams onto a new network, it receives a new RLOC. Since the mobile node is an authoritative ETR for its EID-prefix, it MUST Map-Register it's updated RLOC set. As soon as the registration

is complete, new sessions can be established immediately. Sessions that are encapsulating to RLOCs that did not change during the roaming event are not by the roaming event (or subsequent mapping update). Finally, the mobile node MUST update the ITRs and PTRs that have cached a previous mapping. It does this using the techniques described in Section 6.2.

6.1. Addressing Architecture

A LISP mobile node is typically statically provisioned with an EID that it uses for all transport connections. This EID will change infrequently (if at all; assignment of a LISP mobile node's EID is is typically a subscription time event). The key point is that the relatively fixed EID allows the LISP mobile node's transport connections to survive roaming events. As usual, an EID can be either an IPv4 or an IPv6 address. The LISP mobile node's RLOC set changes dynamically during roaming events, and the RLOC set can contain both IPv4 or IPv6 addresses.

A LISP mobile node is also statically provisioned with the address of a Map-Server and with a corresponding authentication key. Like the mobile node's EID, both the Map-Server address and authentication key change very infrequently (again, these are anticipated to be subscription time parameters). Since the LISP mobile node's Map-Server is configured to advertise an aggregated EID-prefix that covers the LISP mobile node's EID, changes to the LISP mobile node's mapping are not propagated further into the mapping system. This property provides for scalable fast mobility.

A LISP mobile node is also be provisioned with the address of a Map-Resolver. A mobile node may also learn the address of a Map-Resolver though a dynamic protocol such as DHCP [RFC2131].

Finally, note that if, for some reason, a mobile node's EID is re-provisioned, the mobile node's Map-Server address may also have to change in order to keep mobile node's EID within the aggregate advertised by the Map-Server (this is discussed in greater detail in Section 6.2).

6.2. Control Plane Operation

A roaming event occurs when the LISP mobile node receives a new RLOC. Because the new address is a new RLOC from the LISP mobile node's perspective, it must update its EID-to-RLOC mapping with its Map-Server; it does this using the Map-Register mechanism described in [LISP].

Note that a LISP mobile node may or may not respond to Map-Requests.

In particular, a LISP mobile node MAY instruct its Map-Server to proxy respond to Map-Requests by setting the Proxy-Map-Reply bit in the Map-Register message [LISP]. In this case the Map-Server responds with a non-authoritative Map-Reply so that an ITR or PTR will know that the ETR didn't directly respond. A mobile node may want the Map-Server to respond on its behalf for a variety of reasons, including minimizing control traffic on radio links and minimizing battery utilization.

Because the mobile node's Map-Server is pre-configured to advertise an aggregate covering the LISP mobile node's EID prefix, the database mapping change associated with the roaming event is confined to the Map-Server and those ITRs that have cached the previous mapping. The LISP mobile node can cause the mappings cached in remote ITRs to be refreshed by using small Time To Live (TTL) on its mappings, sending Map-Requests with piggybacked mapping data, or by setting the Solicit Map Request (SMR) bit in subsequent data packets.

If a LISP mobile node does not have a mapping for a destination it wants to communicate with, it sends a Map-Request to its Map-Resolver as detailed in [LISP-MS]. The mobile node respects the priority and weights of the destination LISP site's mapping and as such adheres to the policy of the destination site. Finally, if the destination address matches a negative map-cache entry, the mobile node encapsulates the matching packets to a PETR.

6.3. Data Plane Operation

A key feature of LISP-MN control-plane architecture is the use of the Map-Server as an anchor point; this allows control of the scope to which changes to the mapping system must be propagated during roaming events.

The LISP-MN data-plane architecture, on the other hand, does not rely on additional LISP infrastructure for communication between LISP nodes (mobile or stationary). Data packets take the shortest path to and from the mobile node to other LISP nodes; as noted above, low latency shortest paths in the data-plane is an important goal for the LISP-MN architecture (and is important for delay-sensitive applications like gaming and voice-over-IP). Note that a LISP mobile node will need additional interworking infrastructure when talking to non-LISP sites [LISP-IW]; this is consistent with the design of any host at a LISP site which talks to a host at a non-LISP site.

In general, the LISP mobile node data-plane operates in the same manner as the standard LISP data-plane with one exception: all packets generated by a LISP mobile node are LISP encapsulated. Because data packets are always encapsulated to a RLOC, packets

travel on the shortest path from LISP mobile node to another LISP stationary or mobile node. When the LISP mobile node is sending packets to a stationary or mobile node in a non-LISP site, it sends LISP-encapsulated packets to a PETR which then decapsulates the packet and forwards it to its destination.

7. Protocol Operation

There are five distinct connectivity cases considered by the LISP-MN architecture. The five mobility cases are:

LISP Mobile Node to a Stationary Node in a LISP Site.

LISP Mobile Node to a Non-LISP Site.

LISP Mobile Node to a LISP Mobile Node.

Non-LISP Site to a LISP Mobile Node.

LISP Site to a LISP Mobile Node.

The remainder of this section covers these cases in detail.

7.1. LISP Mobile Node to a Stationary Node in a LISP Site

After a roaming event, a LISP mobile node MUST immediately register its EID-to-RLOC mapping with its configured Map-Server(s). This allows LISP sites sending Map-Requests to the LISP mobile node to receive the current mapping.

On the other hand, ITRs and PTRs which may have cached previous mappings must be informed that the mapping has changed. A LISP mobile node MAY use the SMR bit on data packets it is sending to LISP sites, or it MAY send a Map-Request with Map-Data to update active ITRs to effect this update.

7.1.1. Handling Unidirectional Traffic

A problem may arise when traffic is flowing unidirectionally between sites. In this case, data-plane techniques such as setting the SMR bit to update the mappings can't be used.

For example, consider the "square routing" packet flow case depicted in Figure 1. In this case, a host X with site border routers A and B wants to send packets to a host Y with site border routers C and D. Suppose that X has a default route pointing at A, and that A forwards traffic for Y to C (which then forwards it on it on to Y). Y also

has a default route that points at D, which forwards traffic destined for X to B. In this scenario, routers A, B, C, and D see only unidirectional traffic between hosts X and Y.

If X is a LISP mobile node and B is a ITR (or PTR), the mobile node can't use the data-plane techniques described in Section 7.1 to update the PTR's mapping because the mobile node forwards neither data nor control traffic to the PTR. Thus the ITR's map-cache entry for the mobile node will have to have its TTL expire before it can learn a new mapping for the mobile node. As a result, LISP mobile SHOULD set the TTL on the mappings in its Map-Replies to be in the 1-2 minute range.

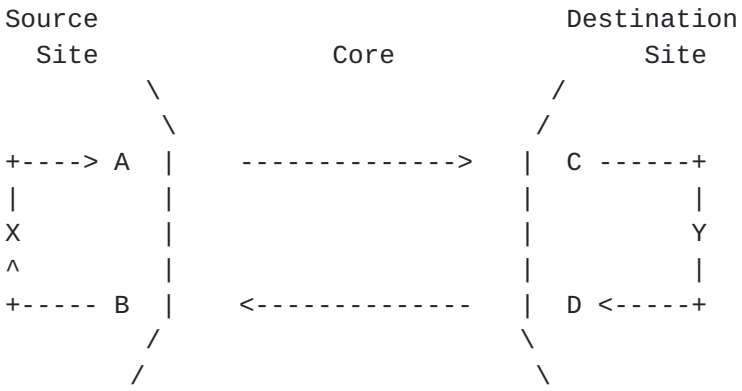


Figure 1: Square Routing Packet Flow

7.2. LISP Mobile Node to a Non-LISP Stationary Node

LISP mobile nodes use the LISP Interworking infrastructure (specifically a PETR) to reach non-LISP sites. In general, the PETR will be co-located with the LISP mobile node's Map-Server. This ensures that the LISP packets being decapsulated are from sources that have Map-Registered to the Map-Server. A LISP mobile node MAY install a default map-cache entry that points at a PETR for use with negative Map-Replies.

When a LISP mobile node roams, it continues to uses its configured PETR and Map-Server. This may add stretch to packets sent from a LISP mobile node to a non-LISP destination.

7.3. LISP Mobile Node to LISP Mobile Node

LISP mobile node to LISP mobile node communication is an instance of LISP-to-LISP communication with three sub-cases:

- Both LISP mobile nodes are stationary. This is covered in Section 7.1.
- Only one LISP mobile node is roaming. This is covered in Section 7.3.1.
- Both LISP mobile nodes are roaming. This is covered in Section 7.3.2

7.3.1. One Mobile Node is Roaming

In this case, the roaming mobile mode can find the stationary mobile node by sending Map-Request for its EID-prefix. After receiving a Map-Reply, the roaming node can encapsulate data packets directly to the non-roaming mobile node node.

The roaming mobile node, on the other hand, MUST update its Map-Server with the new mapping data as described in Section 7.1. It MAY also use the cache management techniques described in Section 7.1 to provide for timely updates of remote ITR caches. Once the roaming mobile node has updated its Map-Server, the non-roaming mobile node can retrieve the new mapping data (if it hasn't already received an updated mapping via one of the mechanisms described in Section 7.1) and the stationary mobile node can encapsulate data directly to the roaming mobile node.

7.3.2. Both Mobile Nodes are Roaming

When both mobile nodes are roaming, they both will both receive new RLOCs, and as a result both need register their new mappings to their Map Servers. However, because both mobile node's map-cache entries contain old RLOCs, neither can update the other using the data-plane techniques described in Section 7.1.

A mobile node can, however, force itself to issue Map-Requests by clearing its map-cache. These Map-Requests MAY contain the updated mapping information for the mobile node. Hence a LISP mobile node MUST clear its map-cache whenever it roams onto a new network (i.e., receives a new RLOC). This will cause the mobile node to issue a new Map-Request the next time it sends a data packet to the other mobile node. The Map-Request will follow the mapping infrastructure to the new location of the correspondent mobile node.

7.4. Non-LISP Site to a LISP Mobile Node

Hosts in non-LISP sites talk to other LISP hosts, whether mobile or stationary, using the PTR infrastructure. Because LISP mobile nodes always encapsulate packets, though subtle the behave differently than as described in [LISP-IW]. In particular, stationary ITRs do not encapsulate packets to a non-LISP host while LISP mobile node do. A PETR is required to decapsulated those packets that are destined from the LISP mobile node to a non-LISP host. Packets from the non-LISP site host return to the mobile node through a PTR, which non-LISP encapsulates packets to the mobile node. Inasmuch as all traffic forwarded through a PTR is unidirectional traffic, a mobile node should use the technique described in Section 7.1.1. In particular, a LISP mobile node SHOULD set the TTL on the mappings in its Map-Replies to be in 1-2 minute range.

7.5. LISP Site to LISP Mobile Node

When a mobile node roams onto a new network, it needs to update the caches in any ITRs that might have stale mappings. This is analogous to the case in that a stationary LISP site is renumbered; in that case ITRs that have cached the old mapping must be updated. This is done using the techniques described in Section 7.1.

When a LISP router in a stationary site is performing both ITR and ETR functions, a mobile node can update the stationary site's map-caches using techniques described in Section 7.1. However, when the LISP router in the stationary site is performing is only ITR functionality, these techniques can not be used because the ITR is not receiving data traffic from the mobile node. In this case, the mobile node should use the technique described in Section 7.1.1. In particular, a LISP mobile node SHOULD set the TTL on the mappings in its Map-Replies to be in 1-2 minute range.

8. Multicast and Mobility

Inasmuch as a mobile node performs both ITR and ETR functionality, it should also perform a lightweight version of multicast ITR/ETR functionality described in [LISP-MCAST]. When a mobile node originates a multicast packet, it will encapsulate the packet with a multicast header, where the source address in the outer header is one of it's RLOC addresses and the destination address in the outer header is the group address from the inner header. The interfaces in which the encapsulated packet is sent on is discussed below.

To not require PIM functionality in the LISP mobile node as documented in [LISP-MCAST], the LISP mobile node resorts to using

encapsulated IGMP for joining groups and for determining which interfaces are used for packet origination. When a LISP mobile node joins a group, it obtains the map-cache entry for the (S-EID,G) it is joining. It then builds a IGMP report encoding (S-EID,G) and then LISP encapsulates it with UDP port 4341. It selects an RLOC from the map-cache entry to send the encapsulated IGMP Report.

When other LISP mobile nodes are joining an (S-EID,G) entry where the S-EID is for a LISP mobile node, the encapsulated IGMP Report will be received by the mobile node multicast source. The mobile node multicast source will remember the interfaces the encapsulated IGMP Report is received on and build an outgoing interface list for it's own (S-EID,G) entry. If the list is greater than one, then the mobile node is doing replication on the source-based tree for which it is the root.

When other LISP routers are joining (S-EID,G), they are instructed to send PIM encapsulated Join-Prune messages. However, to keep the mobile node as simple as possible, the mobile node will not be able to process encapsulated PIM Join-Prune messages. Because the map-cache entry will have a MN-bit indicating the entry is for a mobile node, the LISP router will send IGMP encapsulated IGMP Reports instead.

When the mobile node is sending a multicast packet, it can operate in two modes, multicast-origination-mode or unicast-origination-mode. When in multicast-origination-mode, the mobile node multicast-source can encapsulate a multicast packet in another multicast packet, as described above. When in unicast-origination-mode, the mobile node multicast source encapsulates the multicast packet into a unicast packet and sends a packet to each encapsulated IGMP Report sender.

These modes are provided depending on whether or not the mobile node's network it is currently connected can support IP multicast.

9. RLOC Considerations

This section documents cases where the expected operation of the LISP-MN architecture may require special treatment.

9.1. Mobile Node's RLOC is not Globally Routable

When a mobile node receives a non-globally routable IPv4 [RFC1918] or IPv6 [RFC4193] address during a roaming event, it cannot advertise it globally (i.e., use it as an RLOC in a Map-Reply). This is because the scope of the private address is bounded by the current topological location where the mobile node resides. The use of

private address with LISP is detailed in [LISP-NAT].

9.2. Mobile Node's RLOC is an EID

When a LISP mobile node roams into a LISP site, the "RLOC" it is assigned may be an address taken from the site's EID-prefix. In this case, the mobile node will Map-Register a mapping from its statically assigned EID to the "RLOC" it received from the site. This scenario creates another level of indirection: the mapping from the mobile node's EID to a site assigned EID. The mapping from the mobile node's EID to the site assigned EID allow the mobile node to be reached by sending packets using the mapping for the EID; packets are delivered to site's EIDs use the same LISP infrastructure that all LISP hosts use to reach the site.

A packet egressing a LISP site destined for a LISP mobile node that resides in a LISP site will have three headers: an inner header that is built by the host and is used by transport connections, a middle header that is built by the site's ITR and is used by the destination's ETR to find the current topological location of the mobile node, and an outer header (also built by the site's ITR) that is used to forward packets between the sites.

Consider a site A with EID-prefix 1.0.0.0/8 and RLOC A and a site B with EID-prefix 2.0.0.0/8 and RLOC B. Suppose that a host S in site A with EID 1.0.0.1 wants to talk to a LISP mobile node MN that has registered a mapping from EID 240.0.0.1 to "RLOC" 2.0.0.2 (where 2.0.0.2 allocated from site B's EID prefix, 2.0.0.0/8 in this case). This situation is depicted in Figure 2.

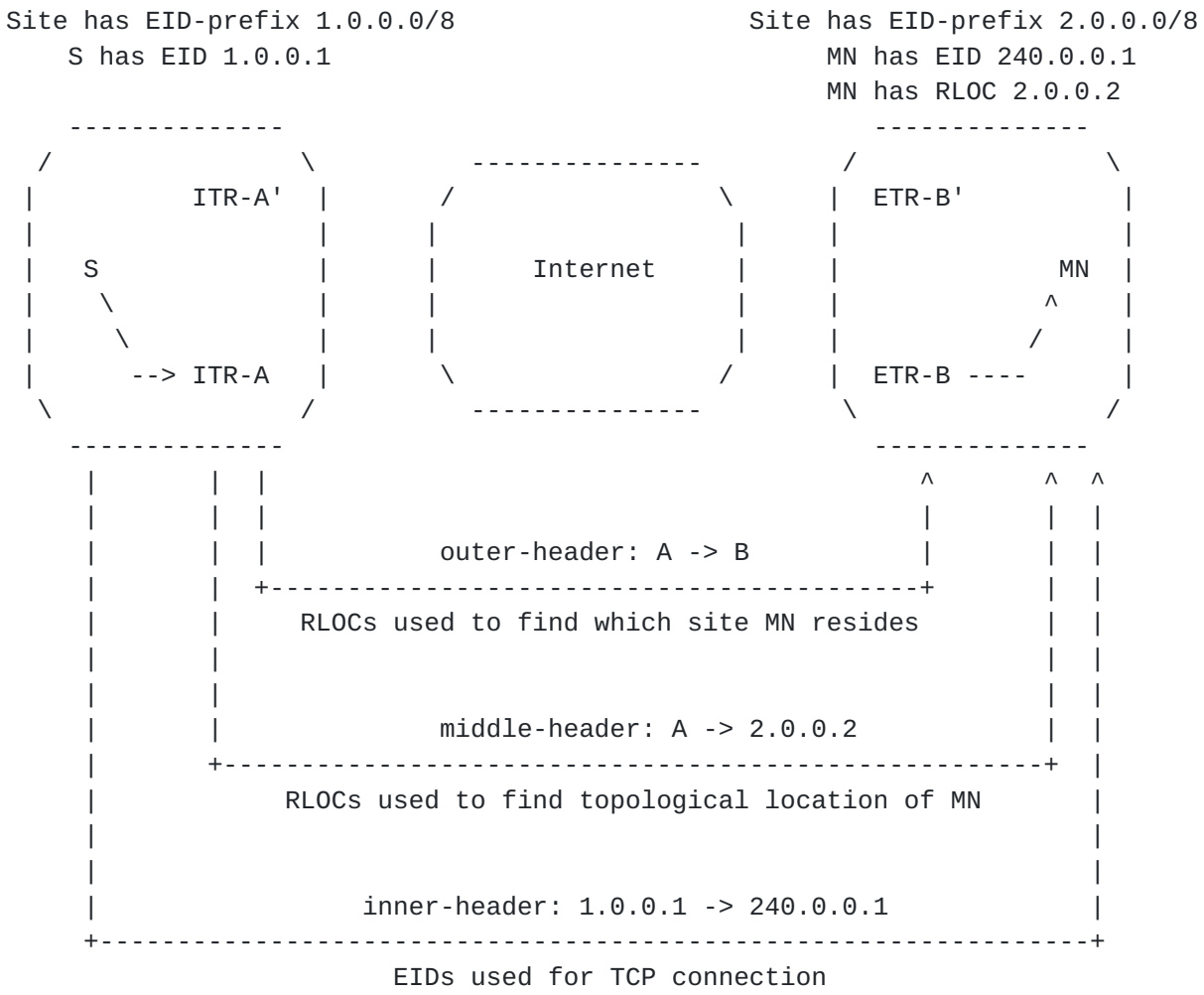


Figure 2: Mobile Node Roaming into a LISP Site

In this case, the inner header is used for transport connections, the middle header is used to find topological location of the LISP mobile node (the LISP mobile node Map-Registers the mapping 240.0.0.1 -> 2.0.0.2 when it roams into site B), and the outer header is used to move packets between sites (A and B in Figure 2).

10. Mobility Example

This section provides an example of how the LISP mobile node is integrated into the base LISP Architecture [LISP].

10.1. Provisioning

The LISP mobile node needs to be configured with the following information:

An EID, assigned to its loopback address

A key for map-registration

An IP address of a Map-Resolver (this could be learned dynamically)

An IP address of its Map-Server and Proxy ETR

10.2. Registration

After a LISP roams to a new network, it MUST immediately register its new mapping this new RLOC (and associated priority/weight data) with its Map-Server.

The LISP mobile node MAY chose to set the 'proxy' bit in the map-register to indicate that it desires its Map-Server to answer map-requests on its behalf.

11. LISP Implementation in a Mobile Node

This section will describe a possible approach for developing a lightweight LISP-MN implementation. A LISP mobile node will implement a LISP sub-layer inside of the IP layer of the protocol stack. The sub-layer resides between the IP layer and the link-layer.

For outgoing unicast packets, once the header that contains EIDs is built and right before an outgoing interface is chosen, a LISP header is prepended to the outgoing packet. The source address is set to the local RLOC address (obtained by DHCP perhaps) and the destination address is set to the RLOC associated with the destination EID from the IP layer. To obtain the RLOC for the EID, the mobile node maintains a map-cache for destination sites or destination mobile nodes to which it is currently talking. The map-cache lookup is performed by doing a longest match lookup on the destination address the IP layer put in the first IP header. Once the new header is prepended, a route table lookup is performed to find the interface in which to send the packet or the default router interface is used to send the packet.

When the map-cache does not exist for a destination, the mobile node

may queue or drop the packet while it sends a Map-Request to it's configured Map-Resolver. Once a Map-Reply is returned, the map-cache entry stores the EID-to-RLOC state. If the RLOC state is empty in the Map-Reply, the Map-Reply is known as a Negative Map-Reply in which case the map-cache entry is created with a single RLOC, the RLOC of the configured Map-Server for the mobile node. The Map-Server that serves the mobile node also acts as a Proxy ETR (PETR) so packets can get delivered to hosts in non-LISP sites to which the mobile node is sending.

For incoming unicast packets, LISP sub-layer in the mobile node simply decapsulates the packets and delivers to the IP layer. In addition, if the SMR-bit is set in the LISP header, the mobile node will schedule a timer to later send a Map-Request to the source address of the received encapsulated packet. Optionally, the loc-reach-bits can be processed by the LISP sub-layer. That is, the source EID from the packet is looked up in the map-cache and if the loc-reach-bits settings have changed, store the loc-reach-bits from the packet and note which RLOCs for the map-cache entry should not be used.

A background task that runs off a timer should be run so the mobile node can send periodic Map-Register messages to the Map-Server. The Map-Register message should also be triggered when the mobile node detects a change in IP address for a given interface. The mobile node should send Map-Registers to the same Map-Register out each of it's operational links. This will provide for robustness on radio links with which the mobile node is associated.

A mobile node receives a Map-Request when it has Map-Registered to a Map-Server with the Proxy-bit set to 0. That means, the mobile node wishes to send authoritative Map-Replies for Map-Requests that are targeted at the mobile node. If the Proxy-bit is set in Map-Registers, then the Map-Server will send non-authoritative Map-Replies on behalf of the mobile node. In this case, the Map-Server never encapsulates Map-Requests to the mobile node. The mobile node can save resources by not receiving Map-Requests.

To summarize, a LISP sub-layer should implement:

- Encapsulating and decapsulating data packets.
- Sending and receiving of Map-Request control messages.
- Receiving and optionally sending Map-Replies.
- Sending Map-Register messages periodically.

The key point about the LISP sub-layer is that no other components in the protocol stack need changing; just the insertion of this sub-layer between the IP layer and the interface layer-2 encapsulation/ decapsulation layer.

12. Security Considerations

Security for the LISP-MN architecture builds upon the security fundamentals found in LISP [LISP] for data-plane security and the LISP Map Server [LISP-MS] registration security. Security issues unique to the LISP-MN architecture are considered below.

12.1. Proxy ETR Hijacking

The Proxy ETR (or PETR) that a LISP mobile node uses as its destination for non-LISP traffic must use the security association used by the registration process outlined in Section 6.2 and explained in detail in the LISP-MS specification [LISP-MS]. These measures prevent third party injection of LISP encapsulated traffic into a Proxy ETR. Importantly, a PETR MUST NOT decapsulate packets from non-registered RLOCs.

12.2. LISP mobile node using an EID as its RLOC

For LISP packets to be sent to a LISP mobile node which has an EID assigned to it as an RLOC as described in Section 9.2), the LISP site must allow for incoming and outgoing LISP data packets. Firewalls and stateless packet filtering mechanisms must be configured to allow UDP port 4341 and UDP port 4342 packets.

13. Acknowledgments

Noel Chiappa, Andrew Partan, and John Zwiebel provided insightful comments on early versions of this document. A special thanks goes to Mary Nickum for her attention to detail and effort in editing early versions of this document.

14. IANA Considerations

This document creates no new requirements on IANA namespaces [RFC2434].

15. References

15.1. Normative References

[LIG] Farinacci, D. and D. Meyer, "LISP Internet Groper (LIG)", draft-ietf-lisp-lig-00.txt (work in progress), August 2010.

[LISP] Farinacci, D., Fuller, V., Lewis, D., and D. Meyer, "Locator/ID Separation Protocol (LISP)", draft-ietf-lisp-08.txt (work in progress), August 2010.

[LISP-ALT] Farinacci, D., Fuller, V., Lewis, D., and D. Meyer, "LISP Alternative Topology (LISP+ALT)", draft-ietf-lisp-alt-04.txt (work in progress), April 2010.

[LISP-IW] Lewis, D., Farinacci, D., Fuller, V., and D. Meyer, "Interworking LISP with IPv4 and IPv6", draft-ietf-lisp-interworking-00.txt (work in progress), May 2009.

[LISP-MCAST] Farinacci, D., Meyer, D., Venaas, S., and J. Zwiebel, "LISP for Multicast Environments", draft-ietf-lisp-multicast-03.txt (work in progress), April 2010.

[LISP-MS] Farinacci, D. and V. Fuller, "LISP MAP Server", draft-ietf-lisp-ms-05.txt (work in progress), April 2010.

[LISP-NAT] Farinacci, D., Fuller, V., Lewis, D., and D. Meyer, "NAT Traversal for the Locator/ID Separation Protocol (LISP)", draft-x-lisp-nat-traversal-00.txt (work in progress), April 2010.

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

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

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC3220] Perkins, C., "IP Mobility Support for IPv4", RFC 3220, January 2002.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

15.2. Informative References

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

Authors' Addresses

Dino Farinacci
Cisco Systems, Inc.
Tasman Drive
San Jose, CA 95134
USA

Email: dino@cisco.com

Vince Fuller
Cisco Systems, Inc.
Tasman Drive
San Jose, CA 95134
USA

Email: vaf@cisco.com

Darrel Lewis
Cisco Systems, Inc.
Tasman Drive
San Jose, CA 95134
USA

Email: darlewis@cisco.com

David Meyer
Cisco Systems, Inc.
Tasman Drive
San Jose, CA 95134
USA

Email: dmm@1-4-5.net