Network Working Group
Internet-Draft
Intended status: Experimental
Expires: July 21, 2017

V. Moreno
Cisco Systems
D. Farinacci
lispers.net

January 17, 2017

LISP Virtual Private Networks (VPNs)
draft-moreno-lisp-vpn-00

Abstract

This document describes the use of the Locator/ID Separation Protocol (LISP) to create Virtual Private Networks (VPNs). LISP is used to provide segmentation in both the LISP data plane and control plane. These VPNs can be created over the top of the Internet or over private transport networks, and can be implemented by Enterprises or Service Providers. The goal of these VPNs is to leverage the characteristics of LISP - routing scalability, simply expressed Ingress site TE Policy, IP Address Family traversal, and mobility, in ways that provide value to network operators.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on July 21, 2017.

Copyright Notice

Copyright (c) 2017 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 Simplified BSD License.

Table of Contents

1. Introduction 3
2. Definition of Terms 3
3. LISP Virtual Private Networks (VPNs) 4
3.1. The LISP IID in the Control Plane 6
3.2. The LISP IID in the Data Plane 6
3.3. Locator Network Segmentation 7
3.4. Multicast in LISP VPN environments 8
4. LISP VPN Extranet 8
4.1. LISP Extranet VPN Control Plane 9
4.1.1. LISP Extranet VPN Map Register Procedures 9
4.1.2. LISP Extranet VPN Map Lookup Procedures 10
4.1.3. LISP Extranet VPN Home-IID encoding 10
4.2. LISP Extranet VPN Data Plane 11
4.3. LISP Extranet VPN Multicast Considerations 11
4.3.1. LISP Extranet VPN Multicast Control Plane 11
4.3.2. LISP Extranet VPN Multicast Data Plane 12
4.4. LISP Extranet SMR Considerations 12
4.5. LISP Extranet RLOC Probing Considerations 13
5. Security Considerations 13
5.1. LISP VPNs and LISP Crypto 13
6. IANA Considerations 14
7. Acknowledgements 14
8. References 14
8.1. Normative References 14
8.2. Informative References 14
Authors' Addresses 16

1. Introduction

Network virtualization creates multiple, logically separated topologies across one common physical infrastructure. These logically separated topologies are known as Virtual Private Networks (VPNs) and are generally used to create closed groups of end-points. Network reachability within a VPN is restricted to the addresses of the end-points that are members of the VPN. This level of segmentation is useful in providing fault isolation, enforcing access-control restrictions, enabling the use of a single network by multiple tenants and scoping network policy per VPN.

LISP creates two namespaces: The End-point Identifier (EID) namespace and the Routing Locator (RLOC) namespace. The LISP Mapping System maps EIDs to RLOCs. Either the EID space, the RLOC space or both may be segmented. The LISP Mapping System can be used to map a segmented EID address space to the RLOC space. When the EID namespace is segmented, a LISP Instance-ID (IID) is encoded in both the data plane and the control plane to provide segmentation and to disambiguate overlapping EID Prefixes. This allows multiple VRFs to 'share' a common Routing Locator network while maintaining EID prefix segmentation.

LISP VPNs must support Multicast traffic in the EID space and must also support the ability to provide controlled reachability across VPNs which is commonly known as extranet functionality. When data path security is needed, LISP virtualization can be combined with LISP Crypto to provide data path confidentiality, integrity, origin authentication and anti-replay protection.

2. Definition of Terms

LISP related terms, notably Map-Request, Map-Reply, Ingress Tunnel Router (ITR), Egress Tunnel Router (ETR), Map-Server (MS) and Map-Resolver (MR) are defined in the LISP specification [RFC6830].

Terms defining interactions with the LISP Mapping System are defined in [RFC6833].

Terms related to the procedures for signal free multicast are defined in [I-D.ietf-lisp-signal-free-multicast].

The following terms are here defined to facilitate the descriptions and discussions within this particular document.

Forwarding Context - Logical segment of a device's forwarding table and its associated interfaces. This is usually in the form of a VRF

for IP forwarding, may also be in the form of a Bridge Domain or VLAN for MAC forwarding.

Home-IID - In the context of cross VPN connectivity, a particular EID will be registered with multiple Instance-IDs, the Home-IID identifies the Instance-ID associated to the Forwarding Context (VRF) to which an EID is actually connected.

Extranet-VPN - In the context of cross VPN connectivity, a VPN that is reachable by all Extranet-Subscriber-VPNs and can reach all Extranet-Subscriber-VPNs.

Extranet-Subscriber-VPN - The VPNs that can reach the Extranet-Provider-VPN, but cannot reach each other.

Extranet Policy - The definition of which VPNs share reachability information with each other in the context of cross VPN connectivity. May be structured as a group of Extranet-Subscriber-VPNs that subscribe to an Extranet-VPN.

3. LISP Virtual Private Networks (VPNs)

A LISP VPN is a collection of LISP Sites building an Overlay Network. These sites share a common control plane, the LISP Mapping System. The members of this VPN also share common RLOC connectivity, whether it be the Internet or a private IP network.

Multiple LISP VPNs may run over a common RLOC space and many LISP VPNs may share one or more locations, requiring XTRs to service multiple VPNs simultaneously.

VPNs must be allowed to have overlapping address space. It is necessary to disambiguate the EID namespace in both the control and data plane as well as maintain forwarding segmentation within the XTRs. The LISP Instance ID (IID) is used to provide a VPN wide unique identifier that can be used both in the control and data planes.

The LISP Instance ID is a 32 bit unstructured namespace that identifies a LISP VPN. The tuple of EID Prefix and IID is referred to as an Extended EID (XEID) [I-D.ietf-lisp-ddt]. The LISP IID is used in the data plane of the LISP header [RFC6830], as well as in the LISP control plane [I-D.ietf-lisp-lcaf].

The operation of a LISP VPN is consistent with the operation of LISP in a non-VPN environment as defined in [RFC6830]. The operation of a LISP VPN is here described at a high level in terms of EID registrations, EID lookups and traffic forwarding:

EID registration: In a LISP VPN, XTRs that are members of the VPN should be configured with a forwarding context (e.g. VRF) and the associated IID for the VPN. Based on this configuration, the ETRs must register the EIDs within the forwarding context as Extended EIDs (IID+EID). The LISP mapping system consolidates the registrations from all the ETRs in the VPN and builds a mapping database for the VPN.

EID Lookup: ITRs that are members of the VPN will do forwarding lookups in the forwarding context where traffic was received. Upon a cache miss within the forwarding context, the ITR must issue a Map-Request for the destination EID and include the VPN's IID. This information must be encoded as an Extended EID (IID+EID) in the Map-Request issued. The IID to associate with the EID in this Map-request is derived from the configuration of the VPN's forwarding context (in which the traffic was received). The Mapping System should reply to the Map Request with a Mapping for the Extended EID (IID+EID), the IID of the Extended EID should be used to identify the forwarding context in which the Mapping received should be cached.

Traffic Forwarding: Once a Mapping has been cached in the VPN's forwarding context, the ITR will encapsulate the traffic towards the RLOC in the mapping. The IID corresponding to the VPN's forwarding context must be included in the Instance-ID field of the data plane header. When the encapsulated traffic is received at the ETR the encapsulation header is removed and the IID received in the header is used to identify the forwarding context to use to do a forwarding lookup for the decapsulated traffic.

A more formal description of the Control and Data Plane procedures for a LISP VPN is documented in the following sections.

In order to create VPNs, the following segmentation functions must be provided:

- Device Segmentation. The forwarding tables of the devices must be segmented so that independent forwarding decisions can be made for each virtual network. Virtual Routing and Forwarding (VRF) contexts may be used to create multiple instances of Layer 3 routing tables virtualization (segmentation) at the device level. If the EID space is in a Layer 2 address family (e.g. MAC addresses), then Layer 2 contexts such as VLANs or bridge domains may be used to segment the device. We generalize the concept of separate forwarding tables as forwarding contexts.

- Data Plane Segmentation. Data Plane Forwarding separation is necessary for the devices to maintain virtual network semantics at forwarding time. Data plane separation can be maintained across

network paths using either single-hop path segmentation (hop-by-hop) or multi-hop path segmentation. Single-hop path segmentation mechanisms include constructs such as 802.1q VLAN trunks, multi-hop mechanisms include MPLS, LISP, VXLAN and GRE tunnels.

- o Control Plane Segmentation. In order to correctly populate the multiple forwarding tables in the segmented network devices, the control plane needs to be segmented so that the different updates that are conveyed by the control plane contain the necessary virtual network semantics to discriminate between information relevant to one segment vs another. Control plane segmentation is key to allowing sites to use overlapping network prefixes in these logically separate topologies. BGP/MPLS VPNs (ref RFC 4364) are an example of this control plane segmentation.

3.1. The LISP IID in the Control Plane

In a LISP Mapping System supporting VPNs, EID Prefixes should be registered as Extended EID tuples of information that include the EID prefix as well as its corresponding Instance ID (IID) information.

In a segmented LISP network, whenever an EID is present in a LISP message, the EID must be encoded as an extended EID using the Instance ID LCAF type defined in [I-D.ietf-lisp-lcaf]. This includes all LISP messages pertinent to the EIDs in the segmented space, including, but not limited to, Map-Register, Map-Request, Map-Reply, Map-Notify, SMRs, etc.

On EID registration by an ETR, the Map-Register message sent by the ETR must contain the corresponding IID encoded as part of the EID using the Instance ID LCAF type.

On EID lookup, when an ITR issues a Map-Request, both the Map-Request message and the resulting Map-Reply must contain the IID for the EID encoded using the IID LCAF type. The IID to use for a Map-Request may be derived from the configuration of the ITR Ingress VRF. The mappings received by an ITR in a Map-Reply should be cached in the VRF corresponding (by configuration) to the IID included in the Map-Reply message.

The Mapping System must maintain the IID information that corresponds to any EIDs actively registered with the Mapping System.

3.2. The LISP IID in the Data Plane

A LISP xTR will map, by configuration, a LISP Instance ID to a given forwarding context in its EID namespace. The Instance-ID must be included in the data plane header to allow an xTR to identify which

VPN the packet belongs to when encapsulating or decapsulating LISP packets. The LISP header [RFC6830] as well as the VXLAN header [RFC7348] reserve a 24 bit field for the purposes of encoding the Instance-ID (referred to as VNID in the VXLAN specification).

LISP ITRs may receive non-encapsulated traffic on an interface that is associated with the forwarding context for a VPN (e.g. VRF). A LISP ITR should do Map-cache lookups for the destination EID within the forwarding context in which it received the traffic. The LISP ITR must encapsulate the traffic to the destination RLOC found in the map-cache and must include, in the header of the encapsulated packet, the IID associated with the forwarding context for the VPN. In the event of a map-cache miss, the LISP ITR must issue a Map-request with the IID associated with the ITR Ingress VRF as described in Section 3.1.

On receipt of an encapsulated LISP packet, a LISP ETR will deliver the decapsulated packets to the VRF associated with the IID received in the LISP header. Standard routing lookups will then take place within the context of the VRF for the forwarding of the decapsulated packet towards its destination.

The use of multiple IIDs on a single site xTR, each mapped to a different EID VRF allows for multiplexing of VPNs over a Locator network.

3.3. Locator Network Segmentation

This document has so far discussed virtualizing the LISP EID namespace, and communication between xTRs and the LISP Mapping System. Implicit in this communication requirement is a network between these devices. LISP VPNs do not require this underlay network connectivity to be in the "default" VRF, just that a a given LISP Site and its Mapping System be interconnected via a common VRF.

LISP xTRs may have connectivity to each other via multiple distinct VRFs, as in the case where the LISP VPN is being used to create an Overlay with multiple MPLS-VPN Service Providers being used as the transport. In other words, the RLOC space may also be segmented, the segmentation of the RLOC space is not done by LISP, but the segmentation of the RLOC space is delivered by the routing protocols and data plane used by the RLOC space. When the RLOC space is segmented, different EID segments may use different RLOC segments. An RLOC segment may service one or many EID segments, allowing a VPN in the RLOC space to service a subset of the VPNs created in the EID space.

3.4. Multicast in LISP VPN environments

Both Signaled and Signal Free Multicast within a VPN will operate without modification in VPN environments provided that all LISP control plane messages include the Instance ID for their VPN as specified in Section 3. Multicast Source (S) state as well as multicast Group (G) state are both scoped within a VPN and therefore the values for S and G may be reused in other VPNs.

4. LISP VPN Extranet

In a multi-tenant network the communication between a shared VPN and a multitude of otherwise isolated VPNs is generally known as extranet communication. Reachability is established between an shared Extranet-VPN and a multitude of Extranet-Subscriber-VPNs without enabling reachability between the different Extranet-Subscriber-VPNs. This section specifies the procedures and protocol encodings necessary to provide extranet functionality in a multi-instance LISP network. The mechanisms described require cross VPN lookups and therefore assume that the EID space across all VPNs involved does not overlap or has been translated to a normalized space that resolves any overlaps.

The operation of a LISP VPN Extranet is consistent with the operation of LISP VPNs as defined in Section 3. The operation of a LISP VPN Extranet is here described at a high level in terms of EID registrations, EID lookups and traffic forwarding:

EID Registration: EIDs in the Extranet-VPN should be registered in their Home-IID as well as in all other IIDs that are part of the Extranet scope. EIDs in the Extranet-Subscriber-VPNs should be registered in their Home-IID and the Extranet-VPN's IID. This makes the EIDs available for lookups in VPNs other than their Home-VPN. When an EID is registered in an IID that it does not belong to, the mapping should include a parameter containing the Home-IID for the EID. As a result any EID that should be reachable based on the Extranet configuration will be registered in every relevant VPN, if the EID is not native to that VPN, the mapping will have a parameter with the Home-IID for the EID.

EID Lookup: Map-requests will be issued within the IID of the requesting VPN as specified in Section 3. If the destination is across VPNs, the mapping for the destination EID should contain the EID's Home-IID as a parameter. The mapping, including the Home-IID parameter is returned in a Map-Reply and cached by the ITR in the Forwarding Context of the requesting VPN. The cache will include the destination's Home-IID as a parameter of the mapping.

Traffic Forwarding: An ITR will encapsulate traffic to a cross VPN destination using the destination's Home-IID in the data plane header. Upon decapsulation at the ETR, traffic is handed directly to the destination VPN's forwarding context based on the IID used in the header.

A more formal description of the Control and Data Plane procedures for a LISP VPN Extranet is documented in the following sections.

4.1. LISP Extranet VPN Control Plane

In order to achieve reachability across VPNs, EID mapping entries in the Extranet Provider VPN must be accessible for lookups initiated from an Extranet Subscriber VPN and vice-versa.

The definition of which VPNs share reachability information is governed by configurable Extranet Policy. The Extranet Policy will simply state which VPNs are extranet subscribers to a particular extranet provider VPN. There may be multiple provider VPNs in a LISP network and a VPN may subscribe to multiple provider VPNs. A subscriber VPN may act as a provider VPN to provide reachability across subscriber VPNs, this effectively merges the subscriber VPNs together, a scenario that is usually better achieved by creating a single subscriber VPN.

The Instance-ID (IID) for the VPN to which an EID is connected is referred to as the Home-IID of the EID. As cross VPN registrations and lookups take place, the Home-IID for an EID must be preserved and communicated in any pertinent LISP messages.

4.1.1. LISP Extranet VPN Map Register Procedures

An ETR may register EIDs in their Home-IID as well as in the other IIDs within the scope of the Extranet Policy. For example, an EID connected to the Extranet-VPN may be registered by its ETR in its Home-IID and also in all the IIDs corresponding to the Extranet-Subscriber-VPNs defined in the Extranet Policy. When Map-Register messages for an EID are issued in IIDs other than the EID's Home-IID, the Home-IID for the EID must be included in the Map-Register. The Home-IID must be encoded as described in Section 4.1.3.

When registering an EID in multiple IIDs, it is advisable to pack the multiple registrations in a single Map-Register message containing the multiple XEID records.

A Map-Server may be configured with the Extranet Policy. This may suffice for the Map-Server to be able to satisfy cross VPN lookups. In such implementations, ETRs may not be required to register an EID

across the entire scope of IIDs defined in the Extranet Policy, but may only require the registration of the EID in its Home-IID.

Which method of cross VPN mapping registration is used (initiated by the ETR or initiated by the Map-Server) should be a configurable option on the XTRs and Map-Server.

4.1.2. LISP Extranet VPN Map Lookup Procedures

Map-Request messages issued by an ITR, their structure and use do not change when a destination EID is outside of the Home-IID for the source EID.

When a Map-Request message is forwarded from the Map-Resolver to an authoritative Map-Server (either directly or by DDT delegation), the IID of the requesting EID must be preserved so that the Map-Reply is sent in the correct context.

Map-Reply messages must use the IID of the requesting EID and must also include the Home-IID of the destination EID. The Home-IID is a parameter of the destination EID, part of the mapping and must be encoded as described in Section 4.1.3. The mapping obtained in the Map-Reply must be cached in the forwarding context of the requesting EID, which is identified by the IID for the requesting EID. The mappings cached will contain the Home-IID of the destination EID whenever this destination EID is cached outside of its Home-IID.

4.1.3. LISP Extranet VPN Home-IID encoding

The Home-IID is an attribute of the EID-RLOC mapping. The Home-IID must be encoded as an additional RLOC within the record carried in Map-Register, Map-Reply or Map-Notify messages as defined in [RFC6830].

The additional RLOC containing the Home-IID should use AFI = 16387 (LCAF) with a List type as described in Section 4.1.3.1.

4.1.3.1. Home-IID encoded in LCAF List type

The Home-IID may be encoded as LCAF AFI of type Instance ID (Type 2). The IID LCAF AFI entry should be nested within a List Type LCAF (Type 1). The list type is used to include a distinguished name type that would provide the semantical information that identifies this field as a Home-IID to be used for the purposes of Extranet VPNs. Map-Servers and XTRs receiving the encoded messages would leverage the semantical information to parse the control plane message properly. The different LCAF types are documented in [I-D.ietf-lisp-lcaf]. The logical structure of the nested LCAF structure is depicted below:

```
AFI = LCAF(16387)
  Type = LIST(1)
    ITEM1
      AFI = Distinguished Name
      Value = "Home-IID"
    ITEM2
      AFI = LCAF(16387)
      Type = IID(2)
      Value = <Home-IID.value>
```

4.1.3.2. Home-IID encoded in dedicated LCAF Type

Alternatively, a new dedicated LCAF type could be used in order to include application semantics to the encoding of the IID in a purposely structured type. In the future, this document may be updated to provide details of the definition of structure and semantics for a dedicated LCAF type to be used in this application.

4.2. LISP Extranet VPN Data Plane

Traffic will be forwarded according to the procedures outlined in [RFC6830]. The map-cache will include the Home-IID for the destination EID as part of the mapping for the destination EID. In an ITR, unicast traffic will be encapsulated using the Home-IID for the destination EID as the Instance-ID in the encapsulation header. On de-capsulation, the Instance-ID in the header points to the destination VPN already so no further procedures are required.

4.3. LISP Extranet VPN Multicast Considerations

When Multicast traffic needs to be forwarded across VPNs, there are special considerations that are closely tied to the definition of the Extranet functionality. This specification will focus on the use of Signal Free Multicast [I-D.ietf-lisp-signal-free-multicast] for the delivery of a cross VPN multicast service.

4.3.1. LISP Extranet VPN Multicast Control Plane

The Receiver-site Registration procedures described in [I-D.ietf-lisp-signal-free-multicast] are expanded to allow the formation of a replication-list inclusive of Receivers detected in the different VPNs within the scope of the Extranet Policy.

Once the Receiver-ETRs detect the presence of Receivers at the Receiver-site, the Receiver-ETRs will issue Map-Register messages to include the Receiver-ETR RLOCs in the replication-list for the multicast-entry the Receivers joined.

The encodings for Map-Register messages and the EIDs and RLOCs within follow the guidelines defined in [I-D.ietf-lisp-signal-free-multicast].

For VPNs within the scope of the Extranet Policy the multicast receiver registrations will be used to build a common replication list across all VPNs in the Extranet Policy scope. This replication list is maintained within the scope of the VPN where the multicast source resides. When Receivers are in the Extranet-Subscriber-VPN, Multicast sources are assumed to be in the Extranet-VPN and viceversa.

The Instance-ID used to Register the Receiver-ETR RLOCs in the replication-list is the Instance-ID of the Extranet-VPN, i.e. the VPN where the Multicast Source resides. When listeners are detected in the Extranet-VPN, then multiple Registrations must be sent with the Instance-IDs of the Extranet-Subscriber-VPNs under the assumption that the Multicast sources could be in one or more of the Extranet-Subscriber-VPNs.

Source-ITRs will complete lookups for the replication-list of a particular multicast group destination as well as the forwarding of traffic to this multicast group following the procedures defined in [I-D.ietf-lisp-signal-free-multicast] without any change.

4.3.2. LISP Extranet VPN Multicast Data Plane

It is desirable to send a single copy of the Multicast traffic over the transit network and have the Receiver-ETRs locally replicate the traffic to all Receiver-VPNs necessary. This replication is governed by the Extranet Policy configured at the ETR. Thus, ITRs will encapsulate the traffic with the Instance-ID for the VPN where the Multicast Source resides. ETRs will receive traffic in the source IID and replicate it to the Receiver VPNs per the Extranet Policy.

4.4. LISP Extranet SMR Considerations

Data driven SMRs need to carry the IID for the VPNs of senders. Since the sender's VPN is not known, the ETR must send the SMR to the sending RLOC but replicated to all VPNs defined in the Extranet Policy. Multicast optimizations could be used to minimize the amount of traffic replicated when sending these SMRs and potentially replicate only at the ITR. An SMR traveling from an Extranet Subscriber VPN to an Extranet VPN will usually be less susceptible to being replicated many times than an SMR traveling in the opposite direction (provider to subscriber).

4.5. LISP Extranet RLOC Probing Considerations

RLOC Probes must be sent with the IID of the VPN originating the probe. The XTR receiving the probe must identify the VPN for the target EID. The XTR receiving the probe should run all verifications as specified in [RFC6830] within the forwarding context corresponding to the VPN where the target EID is connected. Once verifications are completed, the reply to the probe should be sent in the IID of the VPN that originated the probe.

5. Security Considerations

LISP [RFC 6830] incorporates many security mechanisms as part of the mapping database service when using control-plane procedures for obtaining EID-to-RLOC mappings. In general, data plane mechanisms are not of primary concern for general Internet use-case. However, when LISP VPNs are deployed, several additional security mechanisms and considerations must be addressed.

Data plane traffic uses the LISP instance-id (IID) header field for segmentation. in-flight modifications of this IID value could result in violations to the tenant segmentation provided by the IID. Protection against this attack can be achieved by using the integrity protection mechanisms afforded by LISP Crypto, with or without encryption depending on users' confidentiality requirements (see below).

5.1. LISP VPNs and LISP Crypto

The procedures for data plane confidentiality in LISP are documented in [I-D.ietf-lisp-crypto] and are primarily aimed at negotiating secret shared keys between ITR and ETR in map-request and map-reply messages. These secret shared keys are negotiated on a per RLOC basis and without regard for any VPN segmentation done in the EID space. Thus, multiple VPNs using a shared RLOC may also share a common secret key to encrypt communications of the multiple VPNs.

It is possible to negotiate secret shared keys on a per EID basis by applying the procedures described in [I-D.ietf-lisp-crypto] to RLOC probes. In a VPN environment, RLOC probes would be aimed at Extended EIDs that contain Instance-ID semantics, therefore resulting in the calculation of different secret shared keys for different XEID. Since the keys are calculated per XEID prefix rather than per VPN, there are scale considerations when implementing this level of key negotiation granularity.

6. IANA Considerations

This document has no IANA implications

7. Acknowledgements

The authors want to thank Marc Portoles, Vrushali Ashtaputre, Johnson Leong, Jesus Arango, Prakash Jain, Sanjay Hooda, Darrel Lewis and Greg Schudel for their insightful contribution to shaping the ideas in this document.

8. References

8.1. Normative References

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

[RFC3618] Fenner, B., Ed. and D. Meyer, Ed., "Multicast Source Discovery Protocol (MSDP)", RFC 3618, DOI 10.17487/RFC3618, October 2003, <http://www.rfc-editor.org/info/rfc3618>.

[RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, DOI 10.17487/RFC4601, August 2006, <http://www.rfc-editor.org/info/rfc4601>.

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

8.2. Informative References

[I-D.farinacci-lisp-crypto] Farinacci, D., "LISP Data-Plane Confidentiality", draft-farinacci-lisp-crypto-01 (work in progress), July 2014.

[I-D.farinacci-lisp-mr-signaling] Farinacci, D. and M. Napierala, "LISP Control-Plane Multicast Signaling", draft-farinacci-lisp-mr-signaling-06 (work in progress), February 2015.

[I-D.ietf-lisp-crypto]
Farinacci, D. and B. Weis, "LISP Data-Plane Confidentiality", draft-ietf-lisp-crypto-10 (work in progress), October 2016.

[I-D.ietf-lisp-ddt]
Fuller, V., Lewis, D., Ermagan, V., Jain, A., and A. Smirnov, "LISP Delegated Database Tree", draft-ietf-lisp-ddt-08 (work in progress), September 2016.

[I-D.ietf-lisp-lcaf]
Farinacci, D., Meyer, D., and J. Snijders, "LISP Canonical Address Format (LCAF)", draft-ietf-lisp-lcaf-22 (work in progress), November 2016.

[I-D.ietf-lisp-sec]
Maino, F., Ermagan, V., Cabellos-Aparicio, A., and D. Saucez, "LISP-Security (LISP-SEC)", draft-ietf-lisp-sec-12 (work in progress), November 2016.

[I-D.ietf-lisp-signal-free-multicast]
Moreno, V. and D. Farinacci, "Signal-Free LISP Multicast", draft-ietf-lisp-signal-free-multicast-02 (work in progress), October 2016.

[RFC6407] Weis, B., Rowles, S., and T. Hardjono, "The Group Domain of Interpretation", RFC 6407, DOI 10.17487/RFC6407, October 2011, <http://www.rfc-editor.org/info/rfc6407>.

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

[RFC6831] Farinacci, D., Meyer, D., Zwiebel, J., and S. Venaas, "The Locator/ID Separation Protocol (LISP) for Multicast Environments", RFC 6831, DOI 10.17487/RFC6831, January 2013, <http://www.rfc-editor.org/info/rfc6831>.

[RFC6833] Fuller, V. and D. Farinacci, "Locator/ID Separation Protocol (LISP) Map-Server Interface", RFC 6833, DOI 10.17487/RFC6833, January 2013, <http://www.rfc-editor.org/info/rfc6833>.

[RFC7348] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M., and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks", RFC 7348, DOI 10.17487/RFC7348, August 2014, <http://www.rfc-editor.org/info/rfc7348>.

Authors' Addresses

Victor Moreno
Cisco Systems
170 Tasman Drive
San Jose, California 95134
USA

Email: vimoreno@cisco.com

Dino Farinacci
lispers.net
San Jose, CA 95120
USA

Email: farinacci@gmail.com