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 IP based VPNs can be created over the top of the Internet or other VPN protocols, and can be implemented by Enterprise or Service Provider type networks. 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.

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 August 18, 2014.

Copyright Notice

Copyright (c) 2014 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 .................................................. 2
2. Definition of Terms ........................................... 3
3. Virtualizing LISP .............................................. 4
   3.1. The LISP IID in the Data Plane ............................ 4
   3.2. The LISP IID in the Control Plane ......................... 4
   3.3. Locator Network Segmentation ............................. 4
4. LISP VPN Network Elements ..................................... 5
5. Types of LISP VPNs ............................................. 5
6. Enterprise VPNs ................................................ 6
   6.1. Internet based Enterprise LISP VPN Example .............. 6
   6.2. MPLS-VPN based Enterprise LISP VPN Example ............. 6
7. Service Provider LISP VPNs .................................... 6
   7.1. MPLS VPNs and LISP CE based VPNs, from the SP perspective 6
   7.2. Service Provider Internet based LISP VPN Example ...... 7
   7.3. Service Provider MPLS-VPN based LISP VPN Example ..... 7
8. Security Considerations ........................................ 7
   8.1. LISP VPNs and IPSec ...................................... 8
9. Acknowledgments ............................................... 8
10. IANA Considerations ......................................... 9
11. References .................................................. 9
   11.1. Normative References .................................. 9
   11.2. Informative References ................................. 9
Authors’ Addresses .................................................. 10

1. Introduction

Network virtualization create multiple, logically separated topologies across one common physical infrastructure. Virtual Routing and Forwarding (VRF) containers are used to create multiple instances of Layer 3 routing tables virtualization (segmentation) at the device level. Data Plane Forwarding VRF table separation is maintained across network paths using either single-hop path segmentation (hop-by-hop) such as 802.1q VLANs or VPI/VCI PW. Traditional multi-hop mechanisms include MPLS and GRE tunnels. Control plane segmentation is key to allowing sites to use overlapping network prefixes in these logically separate topologies. MPLS+BGP (ref RFC 2547) is an example of this control plane segmentation.

LISP creates two namespaces - End-Site-Identifier (EID) namespace and the Routing Locators (RLOC) namespace. The LISP Mapping System maps
the EID to a RLOC. LISP can be used for virtual networking in both
name spaces, and the LISP Mapping System can be used to Map
Virtualized EID Networks to RLOC Networks. That is, either or both
namespace can be virtualized. When the EID namespace is segmented, a
LISP Instance-ID (IID) is encoded in both the data plane and in the
control plane to provide segmentation and to disambiguate overlapping
EID Prefixes. The allows multiple VRFs to ‘share’ a common Routing
Locator network while maintaining prefix segmentation.

This flexible approach to LISP virtualization, combined with LISP’s
innate capabilities of simple TE policy expression, address family
traversal, and mobility, have several implications for the use and
creation of Overlay Networks. An Enterprise using a LISP VPN it can
virtualize, under the same control plane, a coherent overlay network
in its campus, its branches, its Data Centers and its external
‘cloud’ based services.

A LISP VPN can be built with a partial mesh of Tunnel Routers that do
not have direct reachability to each other’s RLOCs. One example of
non globally reachable RLOC namespace is the IPv4 Internet and the
IPv6 Internet. Without some intervening mechanism, individual sites
connected to one, but not both of these two networks could not
directly communicate with each other. The same situation can occur
for Locator networks of the same address family, as in the case where
there are two separate MPLS VPNs acting as Locator Namespaces. When
data path security is needed, LISP virtualization can be combined
with IPSec to provide data path confidentiality, integrity, origin
authentication and anti-replay protection.

In general, LISP VPNs can be instantiated either by Enterprises or by
Service Providers. When implemented by Enterprise networks, the
functions of LISP Tunnel Routers (xTRs) and the LISP Mapping System
are enabled on Customer Edge (CE) devices use IP transport (either
the internet or a private IP network (e.g. an MPLS-BGP VPN), to
create a common underlay for the LISP Overlay to use. When LISP VPNs
are implemented by a Service Provider, the xTR function may be
enabled on either the Provider Edge (PE) or the CE devices, and the
LISP Mapping system may be enabled on either one of those devices or
dedicated to a devices somewhere in the Service Provider network with
IP connectivity to those data plane devices.

2. Definition of Terms

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

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.

VPNs must be allowed to have overlapping address space. We need to disambiguate this space in both the control and data plane. The LISP Instance ID (IID) is used to provide a VPN wide unique identifier.

The LISP Instance ID is a 24 bit unstructured namespace that identifies a LISP VPN. The tuple of EID Prefix and IID is referred to as an Extended EID (XEID) (ref DDT draft). The LISP IID is used in the data plane of the LISP header (ref RFC 6830), as well as in the LISP control plane (ref LCAF).

3.1. The LISP IID in the Data Plane

A LISP xTR will map, by configuration, the LISP Instance ID to a given VRF in its EID namespace. The purpose of the LISP IID in the LISP header is to allow an xTR to identify which VPN the packet belongs to when encapsulating or decapsulating LISP packets. The EID. For example, on receipt of a packet a LISP ETR will deliver the decapsulated data to the proper VRF. 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.

3.2. The LISP IID in the Control Plane

In the LISP Mapping Server, LISP sites are identified by a set of EID Prefixes, an authentication key, and an LISP IID.

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 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.
4. LISP VPN Network Elements

In general LISP VPNs are built from the network elements described in RFC 6830 and RFC 6832. This document describes a new way to use the Re-Encapsulating Tunnel Router in RFC 6830.

This LISP VPNs are comprised of the following major network elements:

CE routers acting as XTRs. Each customer site is deployed as one or more LISP xTR devices, and include single-home or multi-home designs, using any access media that provides Internet (IPv4 or IPv6) underlay connectivity. The site xTR configuration includes only the LISP EID space that the site is authoritative for and that it registers into the LISP Mapping System, and the RLOC addressing and ingress TE policy desired by the site. To reach other xTRs in the VPN, the xTR is only required to have simple, default routing to its next hop in the address family of the RLOC space.

A virtualized LISP Mapping System. The Mapping system is configured with per customer and per site information, including the IID of the VPN(s), the EID Prefixes allowed to be registered, and the authentication key(s) of the LISP sites, and optionally the specific Locators that are allowed to be registered.

Optionally, LISP Proxy Tunnel Routers. VPN services also need to be able to offer non-LISP to LISP interworking for Internet connectivity or for migration to the LISP VPN from other technologies.

Optionally, LISP Re-encapsulating Tunnel Routers. If LISP VPN services require LISP to LISP interworking across disconnected locator spaces, for example to connect LISP sites attached solely to the IPv4 Internet with those that are solely attached to the IPv6 Internet, then the SP also deploys a number of Re-encapsulating Tunnel Routers to act as a gateway in the data plane that joins these disjointed locator networks.

- IPSec infrastructure. (More text needed here)

5. Types of LISP VPNs

In general, LISP VPNs can be instantiated either by Enterprises or by Service Providers. When deployed by Enterprises, the functions of LISP Tunnel Routers (xTRs) and the LISP Mapping System are enabled on Customer Edge (CE) devices use IP transport (either the internet or a private IP network (e.g. an MPLS-VPN), to create a common underlay for the LISP Overlay to use. When LISP is used a Service Provider, the xTR function may be enabled on either the Provider Edge or the Customer Edge devices, and the LISP Mapping system may be enabled on
either one of these dedicated devices, or deployed elsewhere in the Service Provider network that shares IP connectivity with those data plane devices.

6. Enterprise VPNs

When implementing VPNs via LISP, enterprises create an Overlay which may be independent of their network Service Provider. These VPNs allow for edge virtualization to take place over a common core, as well as allow for simplified multihoming, address family traversal, ip multicast over unicast services, and support for other LISP use cases like Mobility.

6.1. Internet based Enterprise LISP VPN Example

Example of an Enterprise LISP VPN using internet underlay. (Example to be added)

6.2. MPLS-VPN based Enterprise LISP VPN Example

Example of an Enterprise LISP VPN using MPLS underlay (Example to be added)

7. Service Provider LISP VPNs

This section provides two examples of LISP VPNs being used by network Service Providers. These two are not exhaustive examples, and could themselves be combined by Service Providers wanting to deploy a unified Overlay VPN with multiple types (Internet, Mobile, or Private) of Underlay networks. The first example is a CE based VPN using the Internet as an underlay. The second example is a CE based VPN using an MPLS-BGP VPN as an underlay.

7.1. MPLS VPNs and LISP CE based VPNs, from the SP perspective

When LISP and MPLS VPNs are used in conjunction, there are some potential benefits to the services and scalability of the SPs MPLS VPN.

The Service provider would see a reduction in the number of routes on their PEs. When LISP runs as an overlay, all customer prefixes which are typically injected into eBGP and imported into the customer VRF are no longer required. The LISP Mapping system is instead used to provide the level of indirection resolution for end to end connectivity. The only prefixes that are required in the PE VRFs are the point-to-point PE-CE link prefixes connecting all customer sites to the MPLS core.
A reduction in the numbers of VRFs on their PEs. When LISP is run on the customer CE routers, sub-customer virtualization can be handled at the EID level and only a single MPLS VPN is required to segment traffic across the MPLS core. Thus, a global reduction in the number of PE VRFs can be achieved and allowing the SP to more efficiently operate the network.

Consistant network layer services across MPLS NNI networks. LISP VPNs can be used to provide, as an example, address family traversal over the top of an NNI VPN that does not support IPv6. The SP would deploy a LISP Proxy Tunnel Router at their ASBR to the partner, and then customer IPv6 traffic would be encapsulated into IPv4 at the primary provider’s edge into LISP and delivered to the IPv4 Locators of the partner provider’s CE.

7.2. Service Provider Internet based LISP VPN Example

This example describes an SP offering an Internet based VPN service offering using LISP VPNs.  (Example to be added)

7.3. Service Provider MPLS-VPN based LISP VPN Example

This example describes an MPLS VPN provider using LISP to create an Overlay to their MPLS VPN service offering.  (Example to be added)

8. 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 IPsec, with or without encryption depending on users’ confidentiality requirements (see below).

Re-encapsulating Tunnel Routers which bridge LISP-to-LISP domains that use disconnected locator spaces do have access to the LISP Mapping system and control plane components. Thus, RTRs should not need specialized security mechanism beyond those already in place for LISP VPNs.
8.1. LISP VPNs and IPSec

When LISP VPNs are created over the Public Internet, there may be a requirement for a VPN to provide data path confidentiality, integrity, origin authentication and anti-replay protection. When implementing IPSec in a LISP VPN, an operator has two broad choices. The operator can either apply the IPSec functions to the Routing Locator or the EID.

When applying IPSec to the routing locator header, the IPSec encryption policy is applied to the routing locator header of LISP, the order of operation is (1) LISP encapsulation, and then (2) IPSec encryption. In this case, the encryption policy must be designed to match LISP outer header source/destination attributes. It should be noted that this form of encapsulation provides confidentiality to the IID and the EID address space, that may be a security requirement for certain users.

When applying IPSec to the EID header, the IPSec encryption policy is applied to the EID header of LISP, the order of operation is (1) IPSec encryption, and then (2) LISP encapsulation. In this case, the encryption policy must be designed to match EID header source/destination attributes.

Various key exchange mechanisms can be used to provision the tunnel endpoints with appropriate key material. The use of group key management mechanisms such as GDOI [RFC6407] introduces a substantial simplification in terms of operation and use of encryption resources at the xTRs, given the role of a key server that "pushes" group key updates to the members of a VPN that share the same encryption key material. When GDOI encryption methods are used, positioning the Key Server infrastructure within its own EID network can provide substantial benefit. Architecturally, this allows the Key Server to be reachable via LISP from "all" CE devices (xTRs). This is advantageous from a security perspective, because the KS can be isolated from general routing, and is not reachable (and thus attackable) from any of the XTRs that constitute the VPN.

9. Acknowledgments

Thanks goes to Dino Farinacci, Dave Meyer, Vince Fuller, Isidor Kouvolus, Jesper Skrivner, Fabio Maino, Vina Ermagan, and other members of the community who have been working on implementing and deploying LISP VPNs.
10. IANA Considerations

This document creates no new requirements on IANA namespaces [RFC5226].

11. References

11.1. Normative References

[I-D.ietf-lisp-ddt]

[I-D.ietf-lisp-lcaf]


11.2. Informative References


Authors’ Addresses

Darrel Lewis
Cisco Systems, Inc.

Email: darlewis@cisco.com

Gregg Schudel
Cisco Systems, Inc.

Email: gschudel@cisco.com