Workgroup: LISP Working Group
Internet-Draft: draft-haindl-lisp-gb-atn-09
Published: 27 March 2023
Intended Status: Informational
Expires: 28 September 2023
Authors: B. Haindl (Frequentis)
M. Lindner (Frequentis)
V. Moreno (Google)
M. Portoles (Cisco Systems)
F. Maino (Cisco Systems)
B. Venkatachalapathy (Cisco Systems)

# Ground-Based LISP for the Aeronautical Telecommunications Network

## Abstract

This document describes the use of the LISP architecture and protocols to address the requirements of the worldwide Aeronautical Telecommunications Network with Internet Protocol Services, as articulated by the International Civil Aviation Organization.

The ground-based LISP overlay provides mobility and multi-homing services to the IPv6 networks hosted on commercial aircrafts, to support Air Traffic Management communications with Air Traffic Controllers and Air Operation Controllers. The proposed architecture doesn't require support for LISP protocol in the airborne routers, and can be easily deployed over existing ground infrastructures.

## 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 https://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 28 September 2023.

## Copyright Notice



## Table of Contents

## 1. Introduction

This document describes the use of the LISP [RFC9300] architecture and protocols to address the requirements of the worldwide Aeronautical Telecommunications Network with Internet Protocol Services (ATN/IPS), as articulated by the International Civil Aviation Organization (ICAO).

ICAO is proposing to replace the existing aeronautical communication services with an IPv6 based infrastructure that supports Air Traffic Management (ATM) between commercial aircrafts, Air Traffic Controllers (ATC) and Air Operation Controllers (AOC).

This document describes how a LISP overlay can be used to offer mobility and multi-homing services to the IPv6 networks hosted on commercial aircrafts without requiring LISP support in the airborne routers. Use of the LISP protocol is limited to the ground-based routers, hence the name "ground-based LISP". The material for this document is derived from [GBL].

## 2. Definition of Terms

AOC: Airline Operational Control

ATN/IPS: Aeronautical Telecommunications Network with Internet Protocol Services

AC-R: Access Ground Router

A/G-R: Air/Ground Router

G/G-R: Ground/Ground Router

A-R: Airborne Router

A-E: Airborne Endsystem

ATS-E: ATS Endsystem

For definitions of other terms, notably Map-Register, Map-Request, Map-Reply, Routing Locator (RLOC), Solicit-Map-Request (SMR), Ingress Tunnel Router (ITR), Egress Tunnel Router (ETR), xTR (ITR or ETR), Map-Server (MS), and Map-Resolver (MR) please consult the LISP specification [RFC9300].

## 3. Design Overview

In the ATN/IPS architecture the airborne endsystems hosted on an aircraft are part of an IPV6 network connected to the ground network by one or more Airborne Routers (A-R). A-Rs have multiple radio

interfaces that connects them via various radios infrastructures (e.g. SATCOM, LDACS, AeroMACS) to a given radio region, also known as subnetwork, on the ground. Typically an A-R has a corresponding ground based Access Router (AC-R) that terminates the radio protocol with the A-R and provides access services to the ground based portion of the radio network infrastructure. Each radio region is interconnected with the ATN/IPS ground network via an Air-to-Ground router (AG-R).

Similarly, the Air Traffic Controllers and Air Operation Controllers Endsystems (ATS-E and AOC-E) are part of IPv6 networks reachable via one or more Ground-to-Ground Routers (G/G-Rs).

The ATN/IPS ground network infrastructure is the internetworking region located between the A/G routers and the G/G routers.

In the ground-based LISP architecture, a LISP overlay is laid over the ATN/IPS internetworking region (that is in the LISP RLOC space) and provides connectivity between endsystems (that are in the LISP EID space) hosted in the aircrafts and in the AOC/ATS regions. The A/G-Rs and the G/G-Rs assume the role of LISP xTRs supported by a LISP mapping system infrastructure.

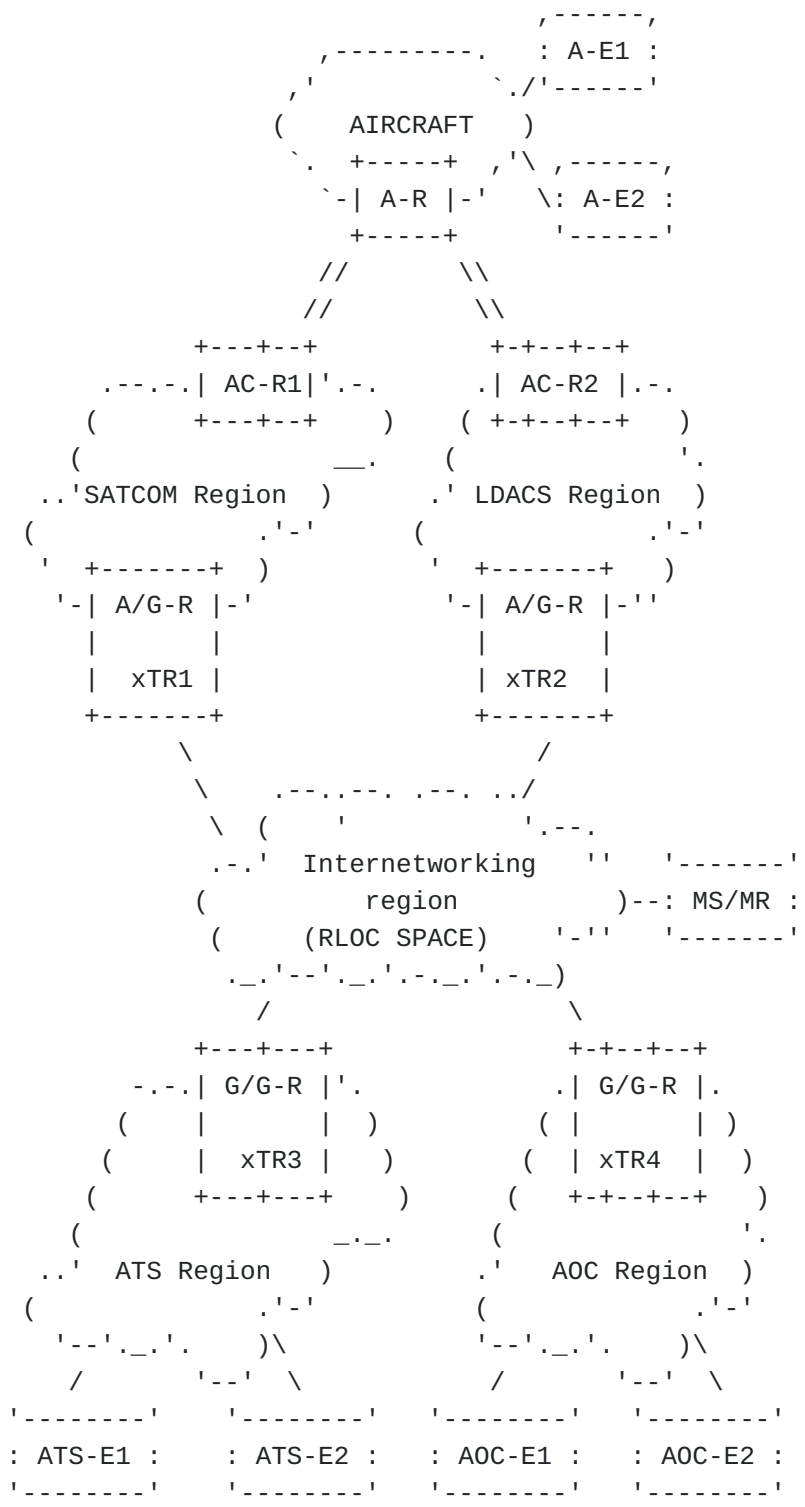


Figure 1: ATN/IPS and ground-based LISP overlay

Endsystems in the AOC/ATS regions are mapped in the LISP overlay by the G/G-Rs, that are responsible for the registration of the AOC/ATS endsystems to the LISP mapping system. Each G/G-R is basically an

xTR which has direct connections only to the terrestrial regions, i.e. no direct connection to the radio regions.

Aircrafts will attach to a specific radio region, via the radio interfaces of the A-Rs. How the radio attachment works is specific to each particular radio infrastructure, and out of the scope of this document, see [GBL].

Typically at the end of the attachment phase, the access router (AC-R) corresponding to the A-R, will announce the reachability of the EID prefixes corresponding to the attached aircraft (the announcement is specific to each particular radio infrastructure, and is out of the scope of this document). A/G-Rs in that particular radio region are responsible to detect those announcements, and, since they act as xTRs, register to the LISP mapping systems the corresponding IPv6 EID prefixes on behalf of the A-R, but with the RLOC of the A/G-R.

The EID prefixes registered by the A/G-Rs are then reachable by any of the AOC/ATS Endsystems that are part of the ground based LISP overlay.

The LISP infrastructure is used to support seamless aircraft mobility from one radio network to another, as well as multi-homing attachment of an aircraft to multiple radio networks with use of LISP weight and priorities to load balance traffic directed toward the aircraft.

The rest of this document provides further details on how ground-based LISP is used to address the requirements of the ATN/IPS use cases. The main design goals are:

* minimize added complexity on the aircraft
  - airborne routers can assume that any ground system is reachable via any A/G router. Static routing policies can be used on board
  - no need for routing/mobility protocols on board. Routing/ mobility is managed on the ground ATN/IPS network
  - on-board outgoing link selection can be done with simple static policy
* seamless support for aircraft mobility and multi-homing with minimal traffic overhead on the A/G datalink

*minimize complexity of ground deployment

-ground-based LISP can be easily deployed over existing ATN/IPS ground infrastructure

-it is based on COTS solutions

-can ease IPv4 to IPv6 transition issues

## 4. Basic Protocol Operation

Figure 1 provides the reference topology for a description of the basic operation. A more detailed description of the basic protocol operation is described in [GBL].

### 4.1. Endsystem Registration

The following are the steps via which airborne endsystem prefixes are registered with the LISP mapping system:

1. Each Airborne Endsystem (A-E) is assigned an IPv6 address that is the endsystem EID. Each EID includes a Network-ID prefix that comprises (1) an ICAO ID which uniquely identifies the aircraft, and possibly (2) an aircraft network identifier. Airborne devices are grouped in one (and possibly several) IPv6 EID prefixes. As an example an IPv6 EID prefix could be used for all ATC applications located in a safety critical domain of the aircraft network, another IPv6 EID prefix could be used for AOC applications located in a less safety critical domain.

2. After the Airborne Router (A-R) on an aircraft attaches to one radio region, the corresponding Access Router (AC-R) learns the IPv6 EID prefixes belonging to the aircraft. The AC-R also announces reachability of these prefixes in the radio region (subnetwork) e.g. by using an IGP protocol like OSPF. The attachment to a radio includes a preference parameter and a quality parameter, these parameters are used e.g. to calculate the IGP reachability advertisement metric.

3. The Air/Ground Router (A/G-R) in the subnetwork receives the radio region announcements which contain reachablity information for the IPv6 EID prefixes corresponding to the Airborne Endsystems. Since each A/G-R is also an xTR, the A/G-R registers the IPv6 EID prefixes with the LISP MS/MR on behalf of the A-R, but with the RLOC of the A/G-R. The included quality parameter (e.g. IGP metric) is converted to a LISP priority, so that a lower quality metric results in a lower LISP priority value.

Ground based endsystems are part of ground subnetworks where the Ground/Ground Router (G/G-R) is an xTR. Each G/G-R therefore registers the prefixes corresponding to the AOC endsystems and ATS endsystems with the LISP mapping system, as specified in [RFC9300].

### 4.2. Ground to Airborne Traffic Flow

Here is an example of how traffic flows from the ground to the airborne endsystems, when ATS endsystem 1 (ATS-E1) has traffic destined to airborne endsystem 1 (A-E1):

1. The default route in the ATS region takes the traffic to xTR3 which is also a Ground/Ground Router (G/G-R).

2. xTR3 sends a Map-Request message for the address of A-E1 to the LISP mapping system. xTR2 sends a Map-Reply to xTR3 with RLOC set to its address which is reachable from xTR3 via the internetworking region.

3. xTR3 encapsulates the traffic to xTR2 using the RLOC information in the Map-Reply message.

4. xTR2 decapsulates the traffic coming from xTR3. The destination address of the inner packet belongs to A-E1 which has been advertised by the AC-R in the same region. The traffic is therefore forwarded to AC-R2.

5. AC-R2 sends the traffic to the Airborne Router of the aircraft and the A-R sends it to the endsystem.

### 4.3. Airborne to Ground Traffic Flow

Here is an example of how traffic flows from the airborne endsystems to the ground when airborne endsystem 2 (A-E2) has traffic destined to ATS endsystem 2 (ATS-E2):

1. The default route in the aircraft points to the Airborne Router (A-R). The latter forwards the traffic over the radio link to AC-R2.

2. The default route on AC-R2 points to xTR2 (also an A/G-R), so the traffic is sent from AC-R2 to xTR2.

3. xTR2 sends a Map-Request message for the address of ATS-E2 to the LISP mapping system. xTR3 sends a Map-Reply to xTR2 with RLOC set to its address which is reachable from xTR2 via the internetworking region.

4. xTR2 encapsulates the traffic to xTR3 using the RLOC information in the Map-Reply message.

5. xTR3 decapsulates the traffic coming from xTR2, and forwards it to ATS-E2.

### 4.4. Default forwarding path

When an xTR is waiting for a Map-Reply for an EID, the xTR does not know how to forward the packets destined to that EID. This means that the first packets for ground-to-air traffic would get dropped until the Map-Reply is received and a map-cache entry is created. However if a device acting as RTR, see [I-D.ermagan-lisp-nat-traversal], has mappings for all EIDs, the xTR could use the RTR as default path for packets which have to be encapsulated. How the RTR gets all the mappings is outside the scope of this document but one example is the use of LISP pub-sub as specified in [I-D.ietf-lisp-pubsub]. Note that the RTR does not have to be a new device, the device which has the MS/MR role can also act as RTR. It is only the RTR which needs to subscribe to all the aircraft EIDs, the XTRs (i.e. the A/G-Rs and G/G-Rs) do not need to subscribe.

RTRs stitch two legs of a communication flow by acting as an ETR for the purposes of the first leg and as an ITR for the purposes of the second leg. As an ITR (second leg), the RTR will follow all standard procedures of an ITR (issue requests, cache mappings, subscribe to EIDs, etc). In the specific case of the first packet drop scenario, the RTR will subscribe to the entire EID space registered in the Mapping System and maintain a complete cache of all relevant destinations. Any changes to the registration state will be published promptly to the RTR using the pub/sub mechanisms. This ITR role can be made redundant by simply having each RTR in the redundancy group subscribe to the Mapping System. From an ETR perspective, the RTR will also follow all standard procedures for an ETR, but rather than registering specific prefixes, the RTRs will (optionally) register themselves as the “First Packet Handlers”. The ITRs sending traffic requiring first packet handling will be configured to forward traffic to the First Packet Handlers if there isn’t a mapping already cached for the destination.

The ITRs will know who the first packet handlers are by one of two mechanisms:

1. Configuration of the RLOCs of the first packet handlers on the ITR. This configuration would be done by a network management system.

2. Subscription of the ITR to the “First Packet Handler” EID. As First Packet Handler RLOCs are added or removed the subscribing ITRs are updated.

In both cases the resiliency mechanisms for the RLOCs are the same as for any other RLOC: Routing table reachability combined with optional data plane probes can be leveraged to accelerate failover. In the case in which subscriptions to the “First Packet Handler” EID are used, the RTR will also benefit from the updates in the publication to trigger failover processes.

### 4.5. Traffic symmetry

The requirements for traffic symmetry are still TBD.

## 5. Multi-Homing and Mobility

Multi-homing support builds on the procedures described in Section 4:

1. The Airborne Router (A-R) on an aircraft attaches to multiple radio regions. As an example, and referring to Figure 1, the A-R attaches to the LDACS and SATCOM regions, via AC-R2 and AC-R1 respectively.

2. Through the preference parameter sent to each region, the A-R has control over which path (i.e. radio region) ground to air traffic flows. For example, A-R would indicate preference of the LDACS region by choosing a better preference value for the LDACS region compared to the preference value sent to the SATCOM region.

3. Both xTR1 and xTR2 register the IPv6 EID prefixes with the LISP mapping system using merge semantic, as specified in section 4.6 of [RFC9301]. Since the priority used in the LISP registrations is derived from the preference and quality parameters, xTR2 would use a lower priority value than xTR1. In this way the LISP mapping system will favour xTR2 (A/G-R for the LDACS region) over xTR1 (A/G-R for the SATCOM region), as specified by the preference and quality parameters.

4. Upon registration the LISP MS/MR will send Map-Notify messages to both xTR1 and xTR2, to inform that they have reachability to the aircraft's IPv6 EID prefixes. Both xTRs are notified because they have both set the merge-request and want-map-notify bits in their respective Map-Register message.

5. Upstream and downstream traffic flows on the same path, i.e. both use the LDACS region.

With mobility, the aircraft could want to switch traffic from one radio link to another. For example while transiting from an area covered by LDACS to an area covered by SATCOM, the aircraft could desire to switch all traffic from LDACS to SATCOM. For air-to-ground

traffic, the A-R has complete control over which radio link to use, and will simply select the SATCOM outgoing interface. For ground-to-air traffic:

1. The A-R sends a radio advertisement to AC-R1 indicating a better preference for the SATCOM link.

2. This leads to AC-R1 lowering its quality parameter (e.g. IGP metric) for the IPv6 EID prefixes.

3. Upon receiving the better preference value, xTR1 registers the IPv6 EID prefixes with the MS/MR, using a lower priority value than what xTR2 had used. Both xTR1 and xTR2 receives Map-Notify messages signaling to xTR2 that xTR1 is now the preferred path toward the aircraft.

4. xTR3 has a map-cache which still points to xTR2, therefore xTR3 still sends traffic via xTR2. xTR2 sends Solicit-Map-Request (SMR) to xTR3 who queries the LISP mapping system again. This results in updating the map-cache on xTR3 which now points to XTR1 so ground-to-air traffic now flows on the SATCOM radio link.

The procedure for mobility is derived from [I-D.ietf-lisp-eid-mobility].

## 6. Convergence

When traffic is flowing on a radio link and that link goes down, the network has to converge rapidly on the other link available for that aircraft.

For air-to-ground traffic, once the A-R detects the failure it can switch immediatly to the other radio link.

For ground-to-air traffic, when a radio link fails, the corresponding AC-R sends a reachability update that the IPv6 EID prefixes are not reachable anymore. This leads to the A/G-R (also an xTR) in that region to unregister the IPv6 EID prefixes with the MS/MR. This indicates that the xTR in question has no reachability to the EID prefixes. The notification of the failure should reach all relevant xTRs as soon as possible. For example, if the LDACS radio link fails, xTR3 and xTR4 need to learn about the failure so that they stop sending traffic via xTR2 and use xTR1 instead.

In the sub-sections below, we the use of RLOC-probing, Solicit-Map-Request, and LISP pub-sub as alternative mechanisms for link failure notification.

### 6.1. Use of RLOC-probing

RLOC-probing is described in section 6.3.2 of [RFC9300].

At regular intervals xTR3 sends Map-Request to xTR2 for the aircraft's EID prefixes. When xTR3 detects via RLOC-probing that it can not use xTR2 anymore, it sends a Map-Request for the aircraft's EID prefixes. The corresponding Map-Reply indicates that xTR1 should now be used. The map-cache on xTR3 is updated and air-to-ground traffic now goes through xTR1 to use the SATCOM radio link to the aircraft.

The disadvantage of RLOC-probing is that fast detection becomes more difficult when the number of EID prefixes is large.

### 6.2. Use of Solicit-Map-Request

Solicit-Map-Request is used as described in Section 5:

1. xTR3 is still sending traffic to xTR2 since its map-cache has not been updated yet.

2. Upon detecting that the link is down, and receiving data plane traffic from the ground network, xTR2 sends an SMR to xTR3 that sends a Map-Request to update its map-cache. The corresponding Map-Reply indicates that xTR1 should now be used.

The disadvantage of this approach is that the traffic is delayed pending control-plane resolution. This method also depends on data traffic being continuous, in many cases data traffic may be sporadic, leading to very slow convergence.

### 6.3. Use of LISP pub-sub

As specified in [I-D.ietf-lisp-pubsub], ITRs can subscribe to changes in the LISP mapping system. So if all ITRs subscribe to the EID prefixes for which they have traffic, the ITRs will be notified when there is mapping change.

In the example where the LDACS radio link fails, when xTR2 unregisters the EID prefixes with the MS/MR, xTR3 would be notified via LISP pub-sub (assuming xTR3 has a map-cache entry for these EID prefixes).

This mechanism provides the fastest convergence at the cost of more state in the LISP mapping system.

## 7. Multi-domain structure of the ATN/IPS

The overlay on the ATN/IPS can be structured as a collection of independent administrative domains following the model defined in [I-D.moreno-lisp-uberlay]. In this model, the different administrative domains are interconnected by a transit area referred to as an uberlay. Each administrative domain is independent from the perspective of the control, data and administrative planes. Structuring the ATN/IPS in this manner allows the combination of different implementations and even different mobility methods in the ATN/IPS. The structure proposed also improves resiliency by isolating events and failures across the different administrative domains and improves the scale of the ATN/IPS by distributing the responsibility of maintaining granular aircraft state across the different administrative domains.

The uberlay may be a BGP network as defined in [I-D.templin-atn-bgp]. Following the definitions put forth in [I-D.templin-atn-bgp], the uberlay transit is the core autonomous system and the different administrative domains that conform the ATN/IPS are what [I-D.templin-atn-bgp] defines as stub autonomous systems.

## 8. Security Considerations

For LISP control-plane message security, please refer to [I-D.ietf-lisp-sec]. This addresses the control-plane threats that target EID-to-RLOC mappings, including manipulations of Map-Request and Map-Reply messages, and malicious ETR EID prefix overclaiming.

### 8.1. LISP Basic Security Mechanisms

The LISP specification, documented in [RFC6830bis] and [RFC6833bis], includes basic security mechanisms for the control plane. The base mechanisms are designed to prevent rogue unauthorized ETRs from registering mappings into the Mapping System and to protect ITRs from receiving unsolicited mapping information. To authenticate EID-to-RLOC mapping registrations and ensure that they are from an authorized ETR, LISP uses shared secret keys between ETRs and the Mapping System. Only ETRs that have the shared secret key are able to register EID-to-RLOC mappings to the Mapping System. Without the correct key, the authenticity of the map-register message cannot be verified, and the Mapping System must reject the map-register. The shared keys used to authenticate map-registers are distributed across ETRs and MS/MRs by the orchestration/configuration infrastructure. The shared keys need to be distributed between the xTR and the Mapping System. Since these components will be in the same administrative domain in GB-LISP, it would be feasible to implement a method for this key exchange (see Clause 6.5 in [LISP-

SEC]. In addition to authenticating EID registrations, it is recommended that the Mapping System restricts EID registrations to configured EID prefix ranges. Thus, an authorized ETR is allowed to register EID prefixes only within the EID prefix range configured in the Map-Server. The confidentiality of the LISP control plane messages can be ensured by protecting the transport of control messages with DTLS (over UDP) [RFC6347] or LISP-crypto [RFC8061]. DTLS is also proposed in Clause 6.7 of [LISP-SEC] for providing message privacy.

### 8.2. Control Plane overload protection

Data-plane gleaning [Clause 9 in RFC6830bis] might need to be turned off for avoiding potential attacks by forged data plane packets that could overload the control plane. Another approach is data fusion between multiple reachability verification mechanisms. Generic control plane protection mechanism, such as packet filtering and rate control, should be also deployed for GB-LISP nodes based on a risk assessment. This could mitigate such attacks that try to misuse the Map-Versioning mechanism in the data-plane for overloading the control-plane.

### 8.3. Protecting the LISP control plane from overclaim attacks

The Internet Draft [LISP-SEC] defines a set of security mechanisms (usually referred as LISP-SEC) to provide origin authentication, integrity, and antireplay protection to the EID-to-RLOC mapping data conveyed in the map-resolution process. It includes the usage of multiple one-time-keys (OTK) and hash based message authentication. LISP-SEC also enables authorization verification on EID-prefixes claims made by ETRs, preventing so-called “overclaiming attacks” in which an ETR attempts to claim EID-prefixes for which it is not authoritative. A LISP-SEC protected map-reply, in fact, includes metadata authenticated by the map-server that specify which

### 8.4. LISP Reliable Transport

The communication with the Mappin Systems is originally proposed based on UDP that is not a reliable transport. For a proper synchronization between the ETR and the Map-Servers periodic message transmission would be needed. Usually, Map-Register messages are retransmitted every minute by the ETR. The Map-Server removes the EID entries if they are not refreshed for three successive periods. In mobility solutions, typically a large number of EID entries needs to be registered. Because of packet size limitations these entries can be transported only by a significant number of Map-Register messages in each period. A new reliable transport option has been defined in [LISP-RELT] to solve these issues. Although this Internet Draft has been expired, the new method is used in the latest widely

deployed LISP solution for Software Defined Access (SDA) by Cisco Systems. The reliable transport is composed by new message formats and the support for other then UDP as a transport in the control plane. Both TCP and SCTP is addressed by the specification. The TCP implementation could be traced in the labs. The messages are based on a TLV format where a type filed support the future extensions of the protocol. A message end marker provides extra integrity check possibility for complex aggregated messages. Error notification messages are also specified for notifying situations when the receiver does not recognize or cannot parse message contents. The following message types are specified for the reliable transport mechanism: • Map-Register, • Registration acknowledgement, • Registration rejection, • Registration refresh, • Mapping notification, The session establishment has to be backward compatible. The Map Server authenticates the ETR first using UDP based messages. Once the ETR is authenticated, the Map Server performs a passive open by listening on TCP port 4342. TCP connections are accepted only from the already authenticated ETRs. The ETR has to open the TCP connection actively towards the Map Server one it has received the Map-Notify message on the UDP transport. If the TCP session goes down, the same UDP based procedure has to be repeated. The Map-Server will also revert to the expiration mechanism used for UDP transport until the TCP based session would be fully restored. A single TCP session is built up for all subsequent control plane messages. This applies even when multiple address families are used in the EID space. Once the reliable transport can be used, the periodic refresh is not needed anymore. Mapping information is sent only when there is new information to share. Time-out based removal of registrations are not used in this case. An explicit de-registration is needed by carrying a zero TTL. The reliable transport session should be authenticated. In the simpler case, it could be an RLOC spoofing mitigation. If this is not reliable, then the TCP Authentication Option [RFC5925], or the SCTP Authenticated Chunks [RFC4895] are recommended.

### 8.5. Reachability Control

The communication with the Mappin Systems is originally proposed based on UDP that is not a reliable transport. For a proper synchronization between the ETR and the Map-Servers periodic message transmission would be needed. Usually, Map-Register messages are retransmitted every minute by the ETR. The Map-Server removes the EID entries if they are not refreshed for three successive periods. In mobility solutions, typically a large number of EID entries needs to be registered. Because of packet size limitations these entries can be transported only by a significant number of Map-Register messages in each period. A new reliable transport option has been defined in [LISP-RELT] to solve these issues. Although this Internet

Draft has been expired, the new method is used in the latest widely deployed LISP solution for Software Defined Access (SDA) by Cisco Systems. The reliable transport is composed by new message formats and the support for other then UDP as a transport in the control plane. Both TCP and SCTP is addressed by the specification. The TCP implementation could be traced in the labs. The messages are based on a TLV format where a type filed support the future extensions of the protocol. A message end marker provides extra integrity check possibility for complex aggregated messages. Error notification messages are also specified for notifying situations when the receiver does not recognize or cannot parse message contents. The following message types are specified for the reliable transport mechanism: • Map-Register, • Registration acknowledgement, • Registration rejection, • Registration refresh, • Mapping notification, The session establishment has to be backward compatible. The Map Server authenticates the ETR first using UDP based messages. Once the ETR is authenticated, the Map Server performs a passive open by listening on TCP port 4342. TCP connections are accepted only from the already authenticated ETRs. The ETR has to open the TCP connection actively towards the Map Server one it has received the Map-Notify message on the UDP transport. If the TCP session goes down, the same UDP based procedure has to be repeated. The Map-Server will also revert to the expiration mechanism used for UDP transport until the TCP based session would be fully restored. A single TCP session is built up for all subsequent control plane messages. This applies even when multiple address families are used in the EID space. Once the reliable transport can be used, the periodic refresh is not needed anymore. Mapping information is sent only when there is new information to share. Time-out based removal of registrations are not used in this case. An explicit de-registration is needed by carrying a zero TTL. The reliable transport session should be authenticated. In the simpler case, it could be an RLOC spoofing mitigation. If this is not reliable, then the TCP Authentication Option [RFC5925], or the SCTP Authenticated Chunks [RFC4895] are recommended.

### 8.6. Data Plane Security

#### 8.6.1. Segmentation

LISP inherently delivers segmentation by using extended endpoint identifiers (EIDs) and Instance-IDs to partition the EID space, segment the map-caches, and color the control and data plane messages to create virtual networks. These virtual networks are a seamless extension of the way EIDs are normally handled in LISP and therefore enjoy all the benefits of scale, mobility, and address family independence that LISP provides.

### 8.6.2. Automated RLOC Filtering

The communication on between the xTRs and Map-Servers use the RLOC space data plane. Only those communications attempts shall be accepted that are coming from valid RLOC addresses. Manual configuration of such access lists would be too difficult to manage. An automated RLOC membership mechanism is proposed in [LISP-RFIL]. Although this Internet Draft has been expired, it is still included in some LISP implementations. The Map-Server can authenticate each xTR that wants to communicate. It will build up a list of xTRs that are valid members of this LISP administrative domain. An xTR can specifically subscribe to this membership information. Membership can be maintained by address family and instance ID (VPN). This allows an easy management of both RLOC and EID space segmentation by VPNs. It also supports gateway functions between separated RLOC spaces. Only valid xTR members can apply for notifications of membership information. The xTR receiving the membership information might use it for building internal access control lists automatically. Proxy xTR information is not included in the membership list, so communication with such nodes need to be configured manually. A membership message format is defined in [LISP-RFIL]. The following message type are specified: • Membership subscribe, • Membership subscribe acknowledgement, • Membership subscribe negative acknowledgement, • Membership unsubscribe, • Membership element add, • Membership element delete, • Membership refresh request, • Membership refresh begin, • Membership refresh end. The membership information could be used by the xTR for other future functions, too. Automated RLOC filtering is just one example.

### 8.6.3. Confidentiality, Integrity and Anti-replay protection

In those sections of the ATN/IPS network where data plane confidentiality, integrity and anti-replay protection may be required, the LISP data plane can be secured as any other IP traffic by leveraging IPsec. The provisioning of an IPsec VPN to secure IP encapsulated LISP frames is orthogonal to deployment of LISP and can be done using well known IPsec key negotiation mechanisms such as IKEv2 [RFC7296].

IKEv2 uses X.509 certificates for authentication. A PKI is needed for managing the certificates. The certificates are used for generating the exchanged symmetric encryption keys.

## 9. IANA Considerations

No IANA considerations.

## 10. Acknowledgements

The original authors would like to thank Dino Farinacci and Bela Varkonyi for their review of the document and deep insights.

The following people have contributed, over time, to the autorship of this document: Bernhard Haindl, Manfred Lindner, Reshad Rahman, Marc Portoles-Comeras, Victor Moreno, Fabio Maino, Balaji Venkatachalapathy.

## 11. References

### 11.1. 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, <https://www.rfc-editor.org/info/rfc2119>.

**[RFC9300]** Farinacci, D., Fuller, V., Meyer, D., Lewis, D., and A. Cabellos, Ed., "The Locator/ID Separation Protocol (LISP)", RFC 9300, DOI 10.17487/RFC9300, October 2022, <https://www.rfc-editor.org/info/rfc9300>.

**[RFC9301]** Farinacci, D., Maino, F., Fuller, V., and A. Cabellos, Ed., "Locator/ID Separation Protocol (LISP) Control Plane", RFC 9301, DOI 10.17487/RFC9301, October 2022, <https://www.rfc-editor.org/info/rfc9301>.

### 11.2. Informative References

**[GBL]** Frequentis, "Ground Based LISP for Multilink Operation, https://www.icao.int/safety/acp/ACPWGF/CP WG-I 19/WP06 Ground_Based_LISP 2016-01-14.pdf", January 2016.

**[I-D.ermagan-lisp-nat-traversal]** Ermagan, V., Farinacci, D., Lewis, D., Maino, F., Portoles-Comeras, M., Skriver, J., White, C., Brescó, A. L., and A. Cabellos-Aparicio, "NAT traversal for LISP", Work in Progress, Internet-Draft, draft-ermagan-lisp-nat-traversal-19, 7 May 2021, <https://datatracker.ietf.org/doc/html/draft-ermagan-lisp-nat-traversal-19>.

**[I-D.ietf-lisp-eid-mobility]** Portoles-Comeras, M., Ashtaputre, V., Maino, F., Moreno, V., and D. Farinacci, "LISP L2/L3 EID Mobility Using a Unified Control Plane", Work in Progress, Internet-Draft, draft-ietf-lisp-eid-mobility-11, 10 January 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-lisp-eid-mobility-11>.

**[I-D.ietf-lisp-pubsub]**
Rodriguez-Natal, A., Ermagan, V., Cabellos-Aparicio, A., Barkai, S., and M. Boucadair, "Publish/Subscribe Functionality for the Locator/ID Separation Protocol (LISP)", Work in Progress, Internet-Draft, draft-ietf-lisp-pubsub-15, 28 February 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-lisp-pubsub-15>.

**[I-D.ietf-lisp-sec]** Maino, F., Ermagan, V., Cabellos-Aparicio, A., and D. Saucez, "Locator/ID Separation Protocol Security (LISP-SEC)", Work in Progress, Internet-Draft, draft-ietf-lisp-sec-29, 7 July 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-lisp-sec-29>.

**[I-D.moreno-lisp-uberlay]**
Moreno, V., Farinacci, D., Rodriguez-Natal, A., Portoles-Comeras, M., Maino, F., and S. Hooda, "Uberlay Interconnection of Multiple LISP overlays", Work in Progress, Internet-Draft, draft-moreno-lisp-uberlay-06, 28 September 2022, <https://datatracker.ietf.org/doc/html/draft-moreno-lisp-uberlay-06>.

**[I-D.templin-atn-bgp]** Templin, F., Saccone, G., Dawra, G., Lindem, A., and V. Moreno, "A Simple BGP-based Mobile Routing System for the Aeronautical Telecommunications Network", Work in Progress, Internet-Draft, draft-templin-atn-bgp-08, 16 August 2018, <https://datatracker.ietf.org/doc/html/draft-templin-atn-bgp-08>.

## Authors' Addresses

Bernhard Haindl
Frequentis

Email: bernhard.haindl@frequentis.com

Manfred Lindner
Frequentis

Email: manfred.lindner@frequentis.com

Victor Moreno
Google

Email: vimoreno@google.com

Marc Portoles Comeras
Cisco Systems

Email: mportole@cisco.com

Fabio Maino
Cisco Systems

Email: fmaino@cisco.com

Balaji Venkatachalapathy
Cisco Systems

Email: bvenkata@cisco.com