Workgroup: Network Working Group
Internet-Draft: draft-moreno-lisp-multi-as-00
Published: 29 July 2021
Intended Status: Experimental
Expires: 30 January 2022
Authors: V.M. Moreno
Cisco Systems

LISP Based Multi-AS Backbone Federation

Abstract

As multiple organizations interconnect their networks through peering agreements, it is desirable to preserve the services enabled by a LISP overlay over such interconnection of independent networks. This specification documents the requirements imposed by the deployment scenario in which multiple organizations federate their backbones with the objective of running a LISP overlay to enable services such as mobility or VPNs. The requirements for policies, enforcement and authoritative control of network assets are captured from the perspective of the operator.

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 30 January 2022.

Copyright Notice

Table of Contents

1. Introduction

Multiple organizations often collaborate and interconnect their networks in order to form a larger network that can provide broader coverage and connectivity. When these networks are interconnected the organizations enter peering agreements that specify the terms under which the connectivity is provided. Part of such peering agreements include the specification of the IP prefixes for which a

particular organization will agree to provide service. Traditionally these inter-organizational peerings have been implemented using BGP and constraining the distribution of routes between the Autonomous Systems of the different organizations in order to enforce the conditions set in the peering agreements. This is a tried and proven mechanism to integrate networks, but it is not easily extensible to include some of the services that overlay networks enable. One example of an overlay service that is not easily ported into the native IP routing stack is mobility. In order to support these services, a model for a multi-organizational federated overlay network is of interest. In such a model the multiple organizations will peer with each other to provide underlay connectivity and will participate in a common overlay network for which the control plane will be federated in order to allow the different organizations to define and enforce the policies necessary to conform to their peering agreements.

In this model, organizations will be in control of a set of xTRs, a series of Map Servers/Resolvers and a portion of the underlay topology. Organizations will be able to author and enforce policies governing the reachability of EID prefixes that are registered to their Map Servers, as well as the policies that govern when their underlay may be used as a transit network for traffic flows between end-points registered to other organizations. The policies enforced reflect the peering agreements that may exist between the different organizations.

An important aspect of the peering relationships is the use of network resources provided by the portions of the underlay topology that are in control of each organization. The federation mechanisms must therefore be aware of the underlay topology.

These types of networks are found primarily in operations involving multiple governments or service providers. Accountability, policy enforcement and autonomy are critical requirements for such organizations. There is a high interest in the creation of a federated network, yet the trust levels between organizations are low. Additionally, this federation must function strictly amongst peers, without the participation of an intermediary organization or any hierarchy amongst the peers.

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 [RFC8378].

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

Organization - An administrative domain which is part of the federation. An organization controls a series of xTRs, Map-Servers/ Resolvers (MS/MR), portions of the underlay topology, and is authoritative for the EIDs registered with its MS/MRs.

Underlay-AS - The autonomous system which includes all routers, control plane and RLOC prefixes for an organization. Underlay-AS will connect to each other at specific BGP peering points at which only underlay routing information is exchanged.

Federated Overlay - The overlay network established collaboratively between multiple organizations over a multitude of interconnected Underlay-ASs.

3. Problem statement and Requirements

The objective is the creation of a cross organizational overlay network that would leverage a multi-as underlay to provide a common backbone across the different organizations. The organizations should be able to define and enforce policies and agreements around the connectivity that will be provided for EID prefixes. These policies are relevant to the use of links and routers in the underlay within the boundaries of the different ASs, but are instantiated and enforced in the overlay, where the EIDs reside. Agreements around RLOC prefix reachability in the underlay should also be possible. All LISP services such as mobility, multi-homing, segmentation, Explicit Locator Paths, Signal Free Multicast, etc. should be available in this multi-AS backbone. At the same time, in order to maintain control and administrative delineation between the organizations, each organization will own and operate a set of MS/ MRs that participate in the multi-organization LISP Mapping System.

The following reference topology may be used to illustrate possible multi-AS underlay connectivity scenarios over which a LISP overlay is to be deployed as well as the types of policies, peering agreements and transit scenarios that may need to be supported.

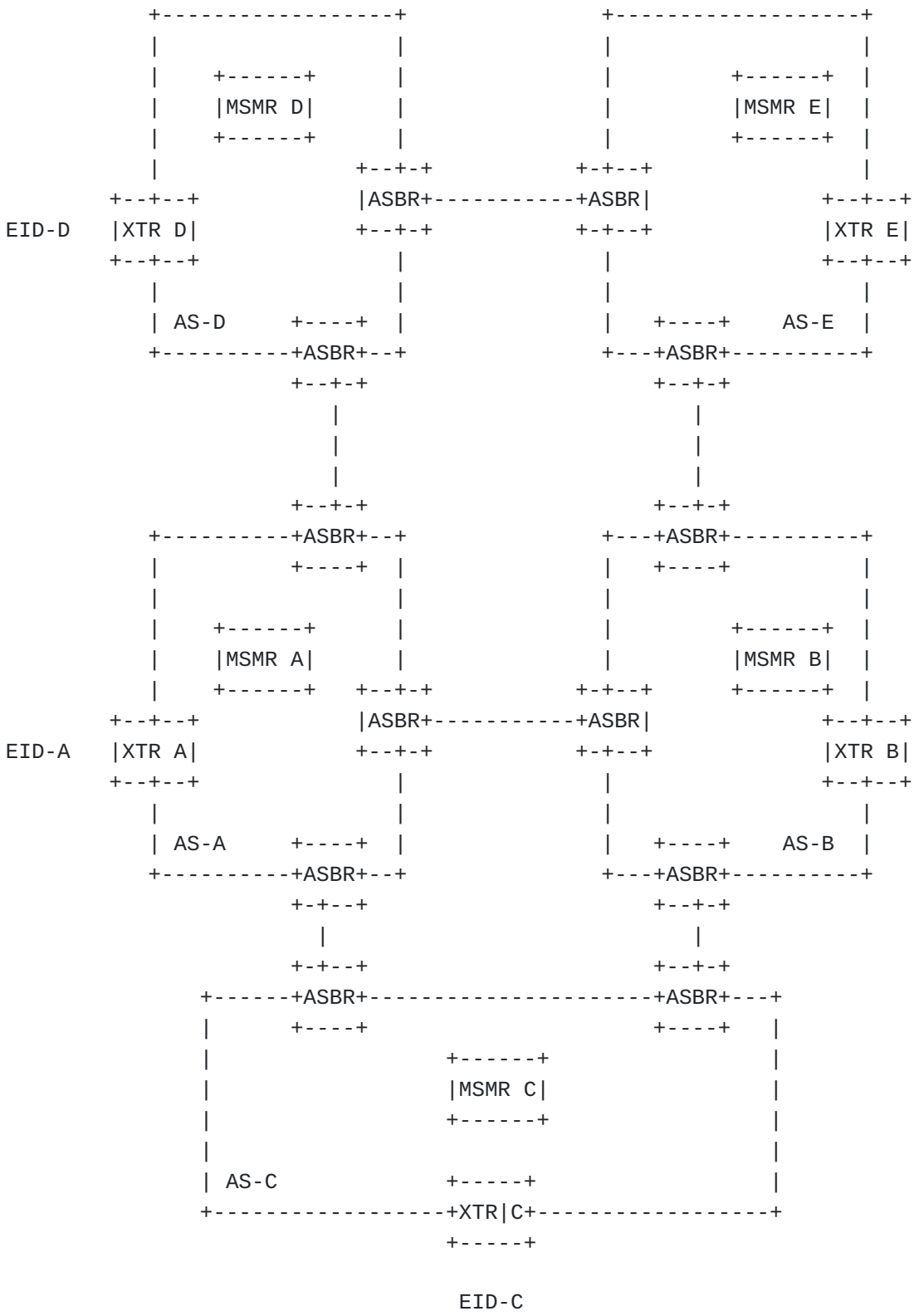

Figure 1. Multi-AS backbone with LISP overlay

Figure 1 shows 5 organizations with a partial connectivity mesh in the underlay. Each organization is represented by one AS. The AS-border routers are underlay routers interconnecting the ASs with EBGP and have no awareness of the overlay. From an overlay perspective, all organizations are actually part of the same overlay network, however the ownership and control of XTR and MS/MR resources is scoped by organization within the confines of each AS.

From the perspective of the connectivity that could be established between EID-A and EID-B in the topology of Figure 1, these are some of the possible scenarios that could be encountered:

* No transit: EID-B is allowed in AS-A and B, but not allowed in AS-C, D or E. The only possible path is the direct peering point between AS-A and B

* Single AS transit: EID-B is allowed in AS-A, B and C. EID-B is not allowed elsewhere. AS-C is a possible path for the flow between EID-A and EID-B, AS-C would serve as a transit AS for this connection. AS-A would have two possibe paths over which to establish the connection with EID-B, the decision on which path to use would be based on a local policy at AS-A that would factor the terms given to A to use the different ASs in the available paths.

* Multi-AS transit: EID-B is allowed in AS-A, B, D and E. The path that traverses AS-D and AS-E is a viable path for the session between EID-A and EID-B. A local ingress policy at AS-A may determine if this path is to be used vs. other paths such as the direct peering or going over AS-C. It is important to note that for the D,E path to be viable, both AS-D and AS-E must have an agreement in which they commit to transporting data for EID-B. If either one of these ASs does not have this agreement, the path would not be viable and should not be used.

The solution provided must allow the evaluation of the viability of different paths based on the peering agreements between organizations, which would allow or deny specific prefixes from being serviced by certain ASs.

When multiple viable paths are available, the solution should permit the definition and enforcement of policies that can be used by the ingress AS to select the preferred path for the forwarding of a certain flow. The terms of service over different paths may differ, leading to preferences in using the services of one AS over another.

EIDs must be able to move from one AS to another. All EIDs connected to an AS must be registered with the MSMR in that AS and fold under the authority of that AS's MSMR. This is required in order to

maintain accountability aligned with the AS providing service to a particular EID.

Each organization owns and controls fully all network elements in their AS, this includes XTRs, ASBRs, MSMRs as well as any underlay routers within the AS.

The following is a summary list of requirements pertinent to this environment:

* Organizations should be able to interconnect their backbone networks at agreed upon peering points and form a multi-AS federated underlay.

* Organizations should be able to participate in a common LISP overlay over the top of the multi-AS federated underlay.

* Ideally the organizations will be able to tunnel traffic directly between XTRs belonging to different organizations without requiring the deployment of RTRs at the boundaries of the domains.

* Peering agreements can be enforced in the underlay control plane to influence the multi-AS routing structure in the underlay RLOC space.

* It must be possible to define and enforce peering agreements and policies relevant to EID-prefixes.

* All peering and policy is to be negotiated in a federated manner. There should not be a need for an intermediary organization that brokers connectivity or policy between members of the federation.

* An organization should be able to restrict which flows use their network resources (underlay)

* Policies may allow or deny connectivity to specific prefixes over portions of the topology belonging to a particular organization.

* Policies may allow or deny transit services to specific prefixes over portions of the topology belonging to a particular organization.

* Organizations may structure their presence in the federation regionally. Thus an organization may have multiple instances participate in the federation. e.g. Org-A-East and Org-A-West.

* An organization is responsible, accountable and authoritative for any host connected to its network (XTRs). Thus, a roaming host

must register to the Mapping System for the organization it is connected to.

*A roaming host should be able to keep its EID constant as it roams.

*A host may connect to more than one AS. The host may use dedicated EIDs per interface or may use a single EID across all interfaces, both cases must be considered.

*An organization should own and control the XTRs in their network.

*An organization should own and control all routes in its Underlay-AS.

*Each organization should own and control their own set of MS/MRs.

*Each organization should be able to define and enforce reachability policies for the EIDs attached to it on the MS/MRs it owns/controls.

*An organization presented with multiple possible paths to reach a particular remote destination should be able to define a preference policy amongst the different paths.

The following sections discuss some of these requirements in more detail.

4. Multi-organizational federated LISP Overlay Network

In a multi-organizational network, the underlay is a collection of interconnected independent networks, each of which is owned and operated by a different organization. The different networks are interconnected at EBGP peering points. Given the use of Location-Identity separation, the peering policies enforced by EBGP at these peering points will be effective on the RLOCs used in the underlay only. All peering policies for the EID prefixes must be handled in the overlay control plane, which may be, in this case, a federation of MS/MRs.

Over the top of this underlay, an overlay network is deployed, to include XTRs and MS/MRs. Each organization will be in control of the XTRs that are directly connected to their underlay network. Furthermore, each organization will have its own set of MS/MRs that it will own and control. One could think of this as a single overlay network in which different portions of the network are owned and controlled by different organizations.

The MS/MRs of the different organizations will federate with each other without an intermediary and they will handle the resolution of

EID to RLOC mappings within and across organizations. The MS/MRs of each organization are authoritative for the EID-RLOC mapping information for EIDs directly connected to their network, but also for the enforcement of policies governing the handling of EID traffic that may use the organization's network as a transit network.

5. Policies and enforcement

The policies to be enforced will derive mainly from the peering agreements between organizations. These are the policies related to the handling of connectivity for EID prefixes and whether specific prefixes may be serviced by a specific AS or not. Although the EIDs are handled in the overlay control plane, the enforcement of the policies must correlate to the use of the resources in the underlay topology in the different ASs. For instance, if an AS does not permit forwarding of traffic for a specific EID prefix, any tunnels established to send traffic to that prefix may not traverse any links in the underlay that belong to the AS that does not permit the prefix.

5.1. Peering Agreement enforcement Policies

Based on their peering agreements, organizations may or may not allow the servicing of traffic for specific EID-prefixes. Traditionally this has been enforced by including or excluding the advertisment of routes into the specific ASs. In the demand model used in LISP, the equivalent would be to provide or withold a valid mapping for the destination from a map-response. Thus, the MS/MRs for all organizations in the possible underlay AS_Paths to be used must be involved in the process of responding to a Map Request. This is so that the policy can be enforced by the MS/MRs that are authoritative for the resources in each AS. Thus, if any of the ASs a tunnel would traverse does not permit the EID in question, the entire path is unusable. It is key to preserve information on richness of paths in the underlay. It may also be necessary to include mechanisms to correlate the AS_Path topology in the underlay to the resolution of mappings in the underlay.

5.1.1. RLOC alignment to AS_Paths

In order to share underlay information with the LISP control plane, XTRs could provide a dedicated RLOC for each peer-AS with which its underlay network AS has a peering relationship. Thus, if an AS has N peering points to N different ASs then there should be N RLOCs representing each XTR in the AS. Each distinct RLOC should only be advertised to the peer AS for which it was instantiated. These advertisements are managed by EBGP at the peering points between the different networks. This way, the different RLOCs are representative

of the different paths through which an AS may be reached, more importantly, each RLOC will be mapped unequivocaly to an AS_PATH as the RLOC is advertised across the different peering points. We refer to this notion of an RLOC that is only reachable via a particular AS as an "AS-aligned-RLOC". The AS-aligned-RLOC concept allows the forwarding over a specific AS_PATH by simply encapsulating traffic to a particular RLOC.

Sending traffic to an EID destination by encapsulating to a particular RLOC will result in the tunnel following a certain AS_PATH as the specific RLOC should only be allowed in specific ASs.

5.2. Sender/Ingress Policies

In a scenarion in which multiple AS_Paths may be followed to arrive at the ETR for a particular EID, a sender should be able to select a preferred path over which to send traffic for a specific location. The selection criteria is based on a subjective score given to each peer service based on negotiated peering agreements. For instance, a particular organization may have secured a better rate or preferential treatment for certain type of traffic over specific providers in the federation. When faced with multiple options to transport traffic to such destinations, there will be a preferred set of providers to use. Each provider is represented by an AS number and for each AS the operator sending the traffic may assign a preference score. Since the AS-PATH to the different RLOCs is registered in the LISP Mapping Database, it is possible to calculate a score of preference for different paths. The MS/MR sending the Map-Response to the requesting ITR will be able to set the LISP priorities and weights in the RLOC set of the mappings for these destinations and prioritize the use of paths with better negotiated terms over paths with a less beneficial agreement. The implementation of a preference score for the different ASs may open interesting applications such as the ability to calculate aggregate scores for the evaluation of composite paths to different destinations.

5.2.1. Application preference policies

In certain operations (e.g. ICAO ATN) application preferences may be expressed in which a certain application should use a particular CSP (AS). This is a clear example of an ingress policy in which the last AS in the path must be the provider with the radio service preferred for the application. As discussed in Section 6 the traffic will be identified with an extended-EID in the form of a tuple of a DSCP value and an IPv6 address, where the DSCP value represents the specific application and the IPv6 address would represent the aircraft. An alternative to this encoding is to simply provide a dedicated IPv6 address to each application on the aircraft. The

addressing could be structured hierarchically where the aircraft uses a covering prefix and the applications are represented by subnets of that covering prefix.

6. Multi-homing

A host may be connected to more than one AS. This is known as multi-homing. In the Civil Aviation use case, an aircraft will connect simultaneously to multiple radio services, each radio service ultimately connects the aircraft to a separate Conectivity Service Provider (CSP) backbone. Each CSP backbone is an Autonomous System in the reference model that we have provided.

The host will connect to different services using different interfaces, however it is expected that the host will use a single IP address for all interfaces. This results in an EID that is multi-homed. In the Civil Aviation use case, the EID is an IPv6 prefix that uniquely identifies the aircraft. It has been suggested that different addresses may be used on different interfaces. Nevertheless, the solution must accommodate both scenarios.

In a multi-homed scenario, the complete RLOC set for an EID is registered to different Map-Servers. Thus, the RLOC set is merged to a complete set upon resolution of the mapping.

In the Civil Aviation application different applications running on the aircraft may be identified with different DSCP values. There may be policy expressing a preference for the use of specific radio services for specific applications. Thus, a DSCP+IPv6 tuple would identify traffic for a particular application and this traffic should be routed to the AS of the preferred radio service.

7. Regionalization

An organization, or Connectivity Service Provider (CSP), may be organized in regions. Thus an organization may be in charge of multiple ASs, where each AS is a regional network. The solution should allow organizations to articulate intra and inter-regional policies in addition to any inter-organizational policies. Some examples of the types of connections expected to utilize these regional networks are included in Section 10.

8. Host Roaming and EID preservation

EIDs are expected to constantly roam and attach to different Connectivity Service Providers (CSPs). This behavior is combined with the multi-homing behavior described in Section 6, so these are multi-homed, roaming EIDs. When EIDs roam, they are expected to register with the Map Servers of the organization they are connecting to. Since these EIDs may be multi-homed, they may be

registered in multiple Map Servers at the time of roaming and the mobility updates may also need to be sent back to multiple map-servers.

In a single AS LISP network, EIDs would not move their registration from one Map Server to another, but the EIDs would remain under the authority of one Map Server. There are however a few factors driving the requirement for the EIDs to be re-homed to the Map-Server of the CSP they are connecting to. The following list enumerates some of those drivers:

* Resiliency and survivability. A problem in one CSP should not impact aircraft connected to other CSPs

* Latency. Minimize RTT of signaling

* Authority assignment. CSPs must be able to autonomously render and assure services, service levels and the enforcement of policies

* Accountability and Audit. CSPs are accountable for all communications of connected devices and must be able to show complete Audit logs

* Trust. Limited across CSPs, governments and other stakeholders

9. Uberlay Deployment

This set of requirements originally emerged in the context of an Uberlay based LISP design for the International Civil Aviation Organization (ICAO). The base proposal is to have a site-overlay deployed for each Connectivity Service Provider and interconnect all those site overlays via the Uberlay. The Uberlay would basically be an overlay network running over a multi-AS federated underlay. As the design progressed, the requirements for the enforcement of peering agreements that would have normally been implemented in BGP became evident. The need for the LISP enabled services remains key, but the requirement for the enforcement of peering agreements is also critical. As these requirements are satisfied, it is important that the solution proposed also works in the context of an Uberlay deployment. The federation of the underlay is applicable within and outside the scope of an Uberlay deployment.

10. ICAO use cases

These use cases are in reference to the solution described in the Ground Based LISP draft. Please refer to [I-D.haindl-lisp-gb-atn] for details and terminology.

10.1. Air Traffic Control

Air Traffic Control (ATC) communications are Regional, but cross-CSPs.

A dedicated IP address for ATC (ATC-EID) has been proposed.

Policy: maintain the ATC EIDs local to the region, all CSPs involved must be updated

10.2. Airline Operation Control

Airline Operation Control (AOC) communications may traverse CSPs, often an Airline will work with a single global CSP.

A dedicated IP address for AOC (AOC-EID) has been proposed.

Policy: Maintain authority @ connecting CSP's. This involves Mapping System Registrations, Access Control and Accountability.

Path preferences are expressed by aircraft and rendered by CSPs as described in Section 6.

10.3. Multi-link

Aircraft connects to more than one CSP.

Aircraft sends communication preferences to A/G-Rs (A/G Interface) per GB-LISP

Mappings are registered with matching Priorities and Weights

Aircraft signals whether it is leaving a link or adding new links

RTRs register the separate Aircraft mappings in the different Uberlay Map Servers

Federated MS must merge the mappings for the aircraft

10.4. Path Preference

Some policies may dictate path restrictions based on Aircraft or Airline preferences as well as CSP peering agreements. These (x)EID/ Application level policies must be enforceable in the Uberlay and will result in tunnels that traverse specific ASs.

11. Policy enforcement and Trust

11.1. Consensus mechanisms and enforceable evidence (data plane)

A malicious organization could override the Map-Reply information received from another organization and violate the restrictions that peering agreements may have imposed on certain flows. In order to avoid the possibility of such malicious behavior, a consensus mechanism involving the affected organization must be put in place. Furthermore, once consensus is achieved, there must be data plane mechanisms that would prevent unauthorized traffic from being sent over a particular underlay-AS. The means to achieve consensus and data plane verification are likely cryptographic. This is an area clearly open to contributions. The mechanisms we seek should provide the underlay/RLOC layer enforceable information relevant to the EID space. In other words, the model should enable the enforcement of EID centered policies in the underlay without the need for decapsulation of the traffic. In order to do so, one option is to create trusted metadata that can be used by the underlay to verify the validity of a flow. The metadata would be created cryptographically when consensus between the organizations is being calculated.

11.2. Topological enforcement (RTRs)

Another approach to enforcing the EID restrictions posed by peering agreements is to deploy RTRs at the AS Border-Routers and treat the overlay as an ELP. This would allow the decapsulation of traffic and the inspection of the EIDs in flight to check whether they are permitted by the peering agreement. Although this makes the enforcement of policy straightforward, it would require additional logic for the signaling across organizations. Future revisions of this document will explore this option should the workgroup not find adequate consensus mechanisms with enforceable data plane metadata.

12. Security Considerations

13. IANA Considerations

This document has no IANA implications

14. Acknowledgements

The authors want to thank the members of the ICAO mobility Workgroup for the countless hours of discussion around their requirements.

15. References

15.1. 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>.

[RFC3618] Fenner, B., Ed. and D. Meyer, Ed., "Multicast Source Discovery Protocol (MSDP)", RFC 3618, DOI 10.17487/RFC3618, October 2003, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc4607>.

15.2. Informative References

[I-D.haindl-lisp-gb-atn] Haindl, B., Lindner, M., Rahman, R., Comeras, M. P., Moreno, V., Maino, F., and B. Venkatachalapathy, "Ground-Based LISP for the Aeronautical Telecommunications Network", Work in Progress, Internet-Draft, draft-haindl-lisp-gb-atn-06, 6 March 2021, <https://www.ietf.org/archive/id/draft-haindl-lisp-gb-atn-06.txt>.

[RFC6407] Weis, B., Rowles, S., and T. Hardjono, "The Group Domain of Interpretation", RFC 6407, DOI 10.17487/RFC6407, October 2011, <https://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, <https://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, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc7348>.

[RFC8060] Farinacci, D., Meyer, D., and J. Snijders, "LISP Canonical Address Format (LCAF)", RFC 8060, DOI 10.17487/RFC8060, February 2017, <https://www.rfc-editor.org/info/rfc8060>.

[RFC8061] Farinacci, D. and B. Weis, "Locator/ID Separation Protocol (LISP) Data-Plane Confidentiality", RFC 8061, DOI 10.17487/RFC8061, February 2017, <https://www.rfc-editor.org/info/rfc8061>.

[RFC8111] Fuller, V., Lewis, D., Ermagan, V., Jain, A., and A. Smirnov, "Locator/ID Separation Protocol Delegated Database Tree (LISP-DDT)", RFC 8111, DOI 10.17487/RFC8111, May 2017, <https://www.rfc-editor.org/info/rfc8111>.

[RFC8378] Moreno, V. and D. Farinacci, "Signal-Free Locator/ID Separation Protocol (LISP) Multicast", RFC 8378, DOI 10.17487/RFC8378, May 2018, <https://www.rfc-editor.org/info/rfc8378>.

Author's Address

Victor Moreno
Cisco Systems
170 Tasman Drive
San Jose, California 95134
United States of America

Email: vimoreno@cisco.com