Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 7, 2016

D. Saucez
INRIA
L. Iannone
Telecom ParisTech
A. Cabellos
F. Coras
Technical University of
Catalonia
October 5, 2015

LISP Impact
draft-ietf-lisp-impact-04.txt

Abstract

The Locator/Identifier Separation Protocol (LISP) aims at improving the Internet routing scalability properties by leveraging on three principles: address role separation, encapsulation, and mapping. In this document, based on implementation work, deployment experiences, and theoretical studies, we discuss the impact that the deployment of LISP can have on both the routing infrastructure and the end-user.

Table of Contents

1. Introduction

The Locator/Identifier Separation Protocol (LISP) relies on three principles to improve the scalability properties of Internet routing: address role separation, encapsulation, and mapping. The main goal of LISP is to make the routing infrastructure more scalable by reducing the number of prefixes announced in the Default Free Zone (DFZ). As LISP utilizes mapping and encapsulation technologies, it provides additional benefits beyond routing scalability. For example, LISP provides a mean for a LISP site to precisely control its inter-domain outgoing and incoming traffic, with the possibility to apply different policies to different domains exchanging traffic with it. LISP can also be used to ease the transition from IPv4 to IPv6 as it allows the transport of IPv4 over IPv6 or IPv6 over IPv4. Furthermore, LISP also supports inter-domain multicast.

This document discusses the impact of LISP's deployment on the Internet routing infrastructure and on end-users. LISP utilizes a tunnel-based data plane and a distributed control plane. LISP requires some new functionalities, such as RLOC reachability mechanisms. Being more than a simple encapsulation technology and as a new technology, until more deployment experience is gained, there will remain open questions related to LISP deployment and operations. As an encapsulation technology, there may be concerns on reduced Maximum Transmission Unit (MTU) size in some deployments. An important impact of LISP is on network operations related to resiliency and troubleshooting. As LISP relies on cached mappings and on encapsulation, resiliency during failures and troubleshooting may be more difficult. Also, the use of encapsulation may make failure detection and recovery slower and it will require more coordination than with a single, non-encapsulated, routing domain solution.

2. LISP in a nutshell

The Locator/Identifier Separation Protocol (LISP) relies on three principles: address role separation, encapsulation, and mapping.

Addresses are semantically separated in two: the Routing Locators (RLOCs) and the Endpoint Identifiers (EIDs). RLOCs are addresses typically assigned from the Provider (interdomain) Aggregatable (PA) address space. The EIDs are attributed to the nodes in the edge networks, by a block of contiguous addresses, which are typically Provider Independent (PI). To limit the scalability problem, LISP only requires the PA routes towards the RLOCs to be announced in the Provider infrastructure. Whereas, for non-LISP deployments the EIDs need as well to be propagated.

LISP routers are used at the boundary between the EID and the RLOC spaces. Routers used to exit the EID space (towards the Provider domain) are called Ingress Tunnel Router (ITRs) and those used to enter the EID space (from the Provider domain) are called the Egress Tunnel Routers (ETRs). When a host sends a packet to a remote destination, it sends it as in the non-LISP Internet. The packet arrives at the border of its site at an ITR. Because EIDs are not routable on the Internet, the packet is encapsulated with the source address set to the ITR RLOC and the destination address set to the ETR RLOC. The encapsulated packet is then forwarded in the Provider domain until it reaches the selected ETR. The ETR de-encapsulates the packet and forwards it to its final destination. The acronym xTR for Ingress/Egress tunnel router is used for a router playing these two roles.

The correspondence between EIDs and RLOCs is given by the mappings. When an ITR needs to find ETR RLOCs that serve an EID, it queries a mapping system. With the LISP Canonical Address Format (LCAF) [I-D.ietf-lisp-lcaf], LISP is not restricted to the Internet Protocol for the EID addresses. With LCAF, any address type can be used as EID (the address is only the key for the mapping lookup). LISP can transport, for example, Ethernet frames over the Internet.

An introduction to LISP can be found in [RFC7215]. The LISP specifications are given in [RFC6830], [RFC6833], [I-D.ietf-lisp-ddt], [RFC6836], [RFC6832], [RFC6834].

3. LISP for scaling the Internet Routing Architecture

The original goal of LISP was to improve the scalability properties of the Internet routing architecture. LISP utilizes traffic engineering and stub AS prefixes (not announced anymore in the DFZ), so that routing tables are smaller and more stable (i.e., they experience less churn). Furthermore, at the edge of the network, information necessary to forward packets (i.e., the mappings) is obtained on demand using a pull model (whereas the current Internet BGP model uses a push model). Therefore, the scalability of edge networks is less dependent on the Internet's size and more related to its traffic matrix. This scaling improvement has been proven by several studies. The research studies cited hereafter are based on the following assumptions:

- o EID-to-RLOC mappings follow the same prefix size as the current BGP routing infrastructure (current PI addresses only);

- o EIDs are used only at the stub ASes, not in the transit ASes;

o the RLOCs of an EID prefix are deployed at the edge between the stubs owning the EID prefix and the providers, allocating the RLOCs in a Provider Aggregetable (PA) mode.

The above assumptions are inline with [RFC7215] and current LISP deployments. It is recognized these assumptions may change in the longer term. [KIF13] and [CDLC] explore different EDI prefix space sizes, and still show results that are consistent and equivalent to the above assumptions.

Quoitin et al. [QIdLB07] show that the separation between locator and identifier roles at the network level improves the routing scalability by reducing the Routing Information Base (RIB) size (up to one order of magnitude) and increases path diversity and thus the traffic engineering capabilities. [IB07] and [KIF13] show, based on real Internet traffic traces, that the number of mapping entries that must be handled by an ITR of a network with up to 20,000 users is limited to few tens of thousands; that the signaling traffic (i.e., Map-Request/Map-Reply packets) is in the same order of magnitude similar to DNS requests/reply traffic; and that the encapsulation overhead, while not negligible, is very limited (in the order of few percentage points of the total traffic volume).

Previous studies consider the case of a timer-based cache eviction policy (i.e., mappings are deleted from the cache upon timeout), while [CDLC] has a more general approach based on the Least Recently Used (LRU) eviction policy, proposing an analytic model for the EID-to-RLOC cache size when prefix-level traffic has a stationary generating process. The model shows that miss rate can be accurately predicted from the EID-to-RLOC cache size and a small set of easily measurable traffic parameters. The model was validated using four one-day-long packet traces collected at egress points of a campus network and an academic exchange point considering EID-prefixes as being of the same size as BGP prefixes. Consequently, operators can provision the EID-to-RLOC cache of their ITRs according to the miss rate they want to achieve for their given traffic.

Results indicate that for a given target miss-ratio, the size of the cache depends only on the parameters of the popularity distribution, being independent of the number of users (the size of the LISP site) and the number of destinations (the size of the EID-prefix space). Assuming that the popularity distribution remains constant, this means that as the number of users and the number of destinations grow, the cache size needed to obtain a given miss rate remains constant O(1).

LISP usually populates its EID-to-RLOC cache in a pull mode which means that mappings are retrieved on demand by the ITR. The main

advantage of this mode is that the EID-to-RLOC cache size only depends on the traffic characteristics at the ITR and is independent of the size of the Provider domain. This benefit comes at the cost of some delay to transmit the packets that do not hit an entry in the cache (for which a mapping has to be learned). This delay is bound by the time necessary to retrieve the mapping from the mapping system. Moreover, similarly to a push model (e.g., BGP), the pull model induces signaling messages that correspond to the retrieval of mappings upon cache miss. The difference being that the signaling load only depends on the traffic at the ITR and is not triggered by external events such as in BGP. [CDLC] shows that the miss rate is a function of the EID-to-RLOC cache size and traffic generation process and [CDLC], [SDIB08], and [SDIB08] show from traffic traces that, in practice, the cache miss rate, and thus the signaling rate, remain low.

4. Beyond scaling the Internet Routing Architecture

LISP is more than just a scalability solution, it is also a tool to provide both incoming and outgoing traffic engineering ([S11], [I-D.farinacci-lisp-te]), it can be used as an IPv6 transition at the routing level, and it can be used for inter-domain multicast ([RFC6831], [I-D.coras-lisp-re]). Also, LISP has been identified for use to support devices' Internet mobility ([I-D.meyer-lisp-mn]) and to support virtual machines' mobility in data centers and multi-tenant VPNs. These last two uses are not discussed further as they are out of the scope of the current LISP Working Group charter.

A key advantage of the LISP architecture is that it facilitates routing in environments where there is little to no correlation between network endpoints and topological location. In service provider environments, this application is needed in a range of consumer use cases which require an inline anchor to deliver a service to a subscribers. Inline anchors provide one of three types of capabilities:

o enable mobility of subscriber end points

o enable chaining of middle-box functions and services

o enable seamless scale-out of functions

Without LISP, operators are forced to centralize service anchors in custom built boxes. This limits deployments as end-points only can move on the same mobile gateway, functions can be chained only if traffic traverses the same wire or the same DPI box, and capacity can scale out only if traffic fans out to/from a specific load balancer.

With LISP, service providers are able to distribute, virtualize, and instantiate subscriber-service anchors anywhere in the network. Typical use cases for virtualized inline anchors and network functions include: Distributed Mobility and Virtualized Evolved Packet Core (vEPC), Virtualized Customer Premise Equipment or vCPE, where functionality previously anchored at a customer premises is now dynamically allocated in-network, Virtualized SGi LAN, Virtual IMS and Virtual SBC, etc.

Current deployments by ConteXtream, using a pre-standards (designed 2006) LISP-based architecture, support a total of 100 million subscribers. And, a deployment at a tier-1 US Mobile operator with over 50 million subscribers provides a 39% download rate improvement over LTE.

4.1. Traffic engineering

In the current (non-LISP)routing infrastructure, addresses used by stub networks are globally routable and the routing system distributes the routes to reach these stubs. With LISP, the EID prefixes of a LISP site are not routable in the DFZ, mappings are needed in order to determine the list of LISP routers to contact to forward packets. This difference is significant for two reasons. First, packets are not forwarded to a site but to a specific router. Second, a site can control the entry points for its traffic by controlling its mappings.

For traffic engineering purposes, a mapping associates an EID prefix to a list of RLOCs. Each RLOC is annotated with a priority and a weight. When there are several RLOCs, the ITR selects the one with the highest priority and sends the encapsulated packet to this RLOC. If several such RLOCs exist, then the traffic is balanced proportionally to their weight among the RLOCs with the lowest priority value. Traffic engineering in LISP thus allows the mapping owner to have a fine-grained control on the primary and backup path for its incoming and outgoing packets use. In addition, it can share the load among its links. An example of the use of such a feature is described by Saucez et al. [SDIB08], showing how to use LISP to direct different types of traffic on different links having different capacity.

Traffic engineering in LISP goes one step further. As every Map-Request contains the Source EID Address of the packet that caused a cache miss and triggered the Map-Request. It is thus possible for a mapping owner to differentiate the answer (Map-Reply) it gives to Map-Requests based on the requester. This functionality is not available today with BGP because a domain cannot control exactly the routes that will be received by domains that are not in the direct

neighborhood.

4.2. LISP for IPv6 Co-existence

The LISP encapsulation mechanism is designed to support any combination of locators and identifiers address family. It is then possible to bind IPv6 EIDs with IPv4 RLOCs and vice-versa. This allows transporting IPv6 packets over an IPv4 network (or IPv4 packets over an IPv6 network), making LISP a valuable mechanism to ease the transition to IPv6.

An example is the case of the network infrastructure of a datacenter being IPv4-only while dual-stack front-end load balancers are used. In this scenario, LISP can be used to provide IPv6 access to servers even though the network and the servers only support IPv4. Assuming that the datacenter's ISP offers IPv6 connectivity, the datacenter only needs to deploy one (or more) xTR(s) at its border with the ISP and one (or more) xTR(s) directly connected to the load balancers. The xTR(s) at the ISP's border tunnels IPv6 packets over IPv4 to the xTR(s) directly attached to the load balancer. The load balancer's xTR de-encapsulates the packets and forwards them to the load balancer, which act as proxies, translating each IPv6 packet into an IPv4. IPv4 packets are then sent to the appropriate servers. Similarly, when the server's response arrives at the load balancer, the packet is translated back into an IPv6 packet and forwarded to its xTR(s), which in turn will tunnel it back, over the IPv4-only infrastructure, to an xTR connected to the ISP. The packet is then de-encapsulated and forwarded to the ISP natively in IPv6.

4.3. Inter-domain multicast

LISP has native support for multicast [RFC6831]. From the data-plane perspective, at a multicast enabled xTR, an EID sourced multicast packet is encapsulated in another multicast packet and subsequently forwarded in a RLOC-level distribution tree. Therefore, xTRs must participate in both EID and RLOC level distribution trees. Control-plane wise, since group addresses have no topological significance they need not to be mapped. It is worth noting that, to properly function, LISP-Multicast requires that inter-domain multicast be available.

LISP Replication Engineering (RE) ([I-D.coras-lisp-re], [CDM12]) leverage LISP messages ([I-D.farinacci-lisp-mr-signaling]) for multicast state distribution to construct xTR based inter-domain multicast distribution trees when inter-domain multicast support is not available. Simulations of three different management strategies for low latency content delivery show that such overlays can support thousands of member xTRs, hundreds of thousands of end-hosts and

deliver content at latencies close to unicast ones ([CDM12]). It was also observed that high client churn has a limited impact on performance and management overhead.

Similarly to LISP-RE, Signal-Free LISP Multicast ([I-D.farinacci-lisp-signal-free-multicast]) can be used when the core network does not provide multicast support. But instead of using signaling to build inter-domain multicast trees, signal-free exclusively leverages the map-server for multicast state storage and distribution. As a result, the source ITR generally performs head-end replication but it might be also used to emulate LISP-RE distribution trees.

5. Impact of LISP on operations and business models

Numerous implementation efforts ([IOSNXOS], [OpenLISP], [LISPmob], [LISPClick], [LISPcp], and [LISPfritz]) have been made to assess the specifications and, additionally, interoperability tests ([Was09]) have been successful. A world-wide large deployment in the international lisp4.net testbed, which is currently composed of nodes running at least three different implementations, will allow us to learn further operational aspects related to LISP.

The following sections distinguish the impact of LISP on LISP sites from the impact on non-LISP sites.

5.1. Impact on non-LISP traffic and sites

LISP has no impact on traffic which has neither LISP origin nor LISP destination. However, LISP can have a significant impact on traffic between a LISP site and a non-LISP site. Traffic between a non-LISP site and a LISP site are subject to the same issues as those observed for LISP-to-LISP traffic but also have issues specific to the transition mechanism that allows the LISP site to exchange packets with a non-LISP site ([RFC6832], [RFC7215]).

The transition requires setup of proxy tunnel routers (PxTRs). Proxies cause what is referred to as path stretch and make troubleshooting harder. There are still questions related to PxTRs that need to be answered:

- o Where to deploy PxTRs? The placement in the topology has an important impact on the path stretch.

- o How many PxTRs? The number of PxTR has a direct impact on the load and the impact of the failure of a PxTR on the traffic.

- What part of the EID space? Will all the PxTRs be proxies for the whole EID space or will it be segmented between different PxTRs?

- Who operates PxTRs? An important question to answer is related to the entities that will deploy PxTRs, how will they manage their additional CAPEX/OPEX costs associated with PxTRs? How will the traffic be carried with respect to security and privacy?

A PxTR will also normally advertise in BGP the EID prefix for which they are proxy. However, if proxies are managed by different entities, they will belong to different ASes. In this case, we need to be sure that this will not cause MOAS (Multi-Origin AS) issues that could negatively influence routing. Moreover, it is important to ensure that the way EID prefixes will be de-aggregated by the proxies will remain reasonable so as not to contribute to BGP scalability issues.

5.2. Impact on LISP traffic and sites

LISP is a protocol based on the map-and-encap paradigm which has the positive impacts that we have summarized in the above sections. However, LISP also has impacts on operations:

MTU issue: as LISP uses encapsulation, the MTU is reduced, this has implications on potentially all of the traffic. However, in practice, on the lisp4.net network, no major issue due to the MTU has been observed. This is probably due to the fact that current end-host stacks are well designed to deal with the problem of MTU.

Resiliency issue: the advantage of flexibility and control offered by the Locator/ID separation comes at the cost of increasing the complexity of the reachability detection. Indeed, identifiers are not directly routable and have to be mapped to locators but a locator may be unreachable while others are still reachable. This is an important problem for any tunnel-based solution. In the current Internet, packets are forwarded independently of the border router of the network meaning that, in case of the failure of a border router, another one can be used. With LISP, the destination RLOC specifically designates one particular ETR, hence if this ETR fails, the traffic is dropped, even though other ETRs are available for the destination site. Another resiliency issue is linked to the fact that mappings are learned on demand. When an ITR fails, all its traffic is redirected to other ITRs that might not have the mappings requested by the redirected traffic. Existing studies ([SKI12], [SD12]) show, based on measurements and traffic traces, that failure of ITRs and RLOC are infrequent

but that when such failure happens, a critical number of packets can be dropped. Unfortunately, the current techniques for LISP resiliency, based on monitoring or probing are not rapid enough (failure recovery on the order of a few seconds). To tackle this issue [I-D.bonaventure-lisp-preserve] and [I-D.saucez-lisp-itr-graceful] propose techniques based on local failure detection and recovery.

Middle boxes/filters: because of encapsulation, the middle boxes may not understand the traffic, which can cause a firewall to drop legitimate packets. In addition, LISP allows triangular or even rectangular routing, so it is difficult to maintain a correct state even if the middle box understands LISP. Finally, filtering may also have problems because they may think only one host is generating the traffic (the ITR), as long as it is not de-encapsulated. To deal with LISP encapsulation, LISP aware firewalls that inspect inner LISP packets are proposed [lispfirewall].

Troubleshooting/debugging: the major issue which LISP experimentation has shown is the difficulty of troubleshooting. When there is a problem in the network, it is hard to pin-point the reason as the operator only has a partial view of the network. The operator can see what is in its EID-to-RLOC cache/database, and can try to obtain what is potentially elsewhere by querying the Map Resolvers, but the knowledge remains partial. On top of that, ICMP packets only carry the first few tens of bytes of the original packet, which means that when an ICMP arrives at the ITR, it might not contain enough information to allow correct troubleshooting. Deployment in the beta network has shown that LISP+ALT ([RFC6836], [CCR13]) was not easy to maintain and control, which explains the migration to LISP-DDT [I-D.ietf-lisp-ddt].

Business/Operational-related: Iannone et al. [IL10] have shown that there are economical incentives to migrate to LISP, however, some questions remain. For example, how will the EIDs be allocated to allow aggregation and hence scalability of the mapping system? Who will operate the mapping system infrastructure and for what benefits?

Reachability: The overhead related to RLOC reachability mechanisms is not known.

6. IANA Considerations

This document makes no request to the IANA.

7. Security Considerations

Security and threats analysis of the LISP protocol is out of the scope of the present document. A thorough analysis of LISP security threats is detailed in [I-D.ietf-lisp-threats].

8. Acknowledgments

Thanks to Deborah Brungard and Wassim Haddad for their thorough reviews, comments, and suggestions.

The people that contributed to this document are Sharon Barkai, Vince Fuller, Joel Halpern, Terry Manderson, Gregg Schudel, Ron Bonica, Ross Callon.

The work of Luigi Iannone has been partially supported by the ANR-13-INFR-0009 LISP-Lab Project (www.lisp-lab.org).

9. References

9.1. Normative References

[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>.

[RFC6832] Lewis, D., Meyer, D., Farinacci, D., and V. Fuller, "Interworking between Locator/ID Separation Protocol (LISP) and Non-LISP Sites", RFC 6832, DOI 10.17487/RFC6832, January 2013, <http://www.rfc-editor.org/info/rfc6832>.

[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>.

[RFC6834] Iannone, L., Saucez, D., and O. Bonaventure, "Locator/ID Separation Protocol (LISP) Map-Versioning", RFC 6834, DOI 10.17487/RFC6834, January 2013, <http://www.rfc-editor.org/info/rfc6834>.

[RFC6836] Fuller, V., Farinacci, D., Meyer, D., and D. Lewis, "Locator/ID Separation Protocol Alternative Logical Topology (LISP+ALT)", RFC 6836, DOI 10.17487/RFC6836, January 2013, <http://www.rfc-editor.org/info/rfc6836>.

[RFC7215] Jakab, L., Cabellos-Aparicio, A., Coras, F., Domingo-Pascual, J., and D. Lewis, "Locator/Identifier Separation Protocol (LISP) Network Element Deployment Considerations", RFC 7215, DOI 10.17487/RFC7215, April 2014, <http://www.rfc-editor.org/info/rfc7215>.

9.2. Informative References

[CCR13] Saucez, D., Iannone, L., and B. Donnet, "A First Measurement Look at the Deployment and Evolution of the Locator/ID Separation Protocol", ACM SIGCOMM Computer Communication Review. Vol. 43, N. 2., April 2013.

[CDLC] Coras, F., Domingo, J., Lewis, D., and A. Cabellos, "An Analytical Model for Loc/ID Mappings Caches", IEEE Transactions on Networking, 2014.

[CDM12] Coras, F., Domingo-Pascual, J., Maino, F., Farinacci, D., and A. Cabellos-Aparicio, "Lcast: Software-defined Inter-Domain Multicast", Elsevier Computer Networks, July 2014.

[I-D.bonaventure-lisp-preserve]
Bonaventure, O., Francois, P., and D. Saucez, "Preserving the reachability of LISP ETRs in case of failures", draft-bonaventure-lisp-preserve-00 (work in progress), July 2009.

[I-D.coras-lisp-re]
Coras, F., Cabellos-Aparicio, A., Domingo-Pascual, J., Maino, F., and D. Farinacci, "LISP Replication Engineering", draft-coras-lisp-re-07 (work in progress), April 2015.

[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.farinacci-lisp-signal-free-multicast]
Moreno, V. and D. Farinacci, "Signal-Free LISP Multicast", draft-farinacci-lisp-signal-free-multicast-03 (work in progress), June 2015.

[I-D.farinacci-lisp-te]
Farinacci, D., Kowal, M., and P. Lahiri, "LISP Traffic Engineering Use-Cases", draft-farinacci-lisp-te-09 (work in progress), September 2015.

[I-D.ietf-lisp-ddt]
Fuller, V., Lewis, D., Ermagan, V., and A. Jain, "LISP Delegated Database Tree", draft-ietf-lisp-ddt-03 (work in progress), April 2015.

[I-D.ietf-lisp-lcaf]
Farinacci, D., Meyer, D., and J. Snijders, "LISP Canonical Address Format (LCAF)", draft-ietf-lisp-lcaf-11 (work in progress), September 2015.

[I-D.ietf-lisp-threats]
Saucez, D., Iannone, L., and O. Bonaventure, "LISP Threats Analysis", draft-ietf-lisp-threats-13 (work in progress), August 2015.

[I-D.meyer-lisp-mn]
Farinacci, D., Lewis, D., Meyer, D., and C. White, "LISP Mobile Node", draft-meyer-lisp-mn-13 (work in progress), July 2015.

[I-D.saucez-lisp-itr-graceful]
Saucez, D., Bonaventure, O., Iannone, L., and C. Filsfils, "LISP ITR Graceful Restart", draft-saucez-lisp-itr-graceful-03 (work in progress), December 2013.

[IB07] Iannone, L. and O. Bonaventure, "On the cost of caching locator/id mappings", In Proc. ACM CoNEXT 2007, December 2007.

[IL10] Iannone, L. and T. Leva, "Modeling the economics of Loc/ID Separation for the Future Internet", Book Chapter, Towards the Future Internet - Emerging Trends from the European Research, IOS Press, May 2010.

[IOSNXOS] Cisco Systems Inc., "Locator/ID Separation Protocol

(LISP)", http://lisp4.cisco.com, 2013.

[KIF13] Kim, J., Iannone, L., and A. Feldmann, "Caching Locator/ID Mappings: Scalability Analysis and Implications", Elsevier Computer Networks Journal, March 2013.

[LISPClick]
Saucez, D. and V. Nguyen, "LISP-Click: A Click implementation of the Locator/ID Separation Protocol", 1st Symposium on Click Modular Router, 2009, November 2009.

[LISPcp] "The lip6-lisp Project", https://github.com/lip6-lisp/, 2014.

[LISPfritz]
"Unsere FRITZ!Box-Produkte", http://avm.de/produkte/fritzbox/, 2014.

[LISPmob] "An open-source LISP implementation for Linux, Android and OpenWRT", http://lispmob.org, 2015.

[OpenLISP]
"The OpenLISP Project", http://www.openlisp.org, 2013.

[QIdLB07] Quoitin, B., Iannone, L., de Launois, C., and O. Bonaventure, "Evaluating the benefits of the locator/identifier separation", In Proc. ACM MobiArch 2007, May 2007.

[S11] Saucez, D., "Mechanisms for Interdomain Traffic Engineering with LISP", PhD Thesis, Universite catholique de Louvain, 2011, October 2011.

[SD12] Saucez, D. and B. Donnet, "On the Dynamics of Locators in LISP", In Proc. IFIP Networking 2012, May 2012.

[SDIB08] Saucez, D., Donnet, B., Iannone, L., and O. Bonaventure, "Interdomain Traffic Engineering in a Locator/Identifier Separation Context", In Proc. of Internet Network Management Workshop, 2008, October 2008.

[SKI12] Saucez, D., Kim, J., Iannone, L., Bonaventure, O., and C. Filsfils, "A Local Approach to Fast Failure Recovery of LISP Ingress Tunnel Routers", In Proc. IFIP Networking 2012, May 2012.

[Was09] Wasserman, M., "LISP Interoperability Testing", IETF 76,

LISP WG presentation, 2009., November 2009.

[lispfirewall]
"LISP and Zone-Based Firewalls Integration and Interoperability", http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/sec-data-zbf-xe-book/sec-zbf-lisp-inner-pac-insp.html, 2014.

Authors' Addresses

Damien Saucez
INRIA
2004 route des Lucioles BP 93
06902 Sophia Antipolis Cedex
France

Email: damien.saucez@inria.fr

Luigi Iannone
Telecom ParisTech
23, Avenue d'Italie, CS 51327
75214 PARIS Cedex 13
France

Email: ggx@gigix.net

Albert Cabellos
Technical University of Catalonia
C/Jordi Girona, s/n
08034 Barcelona
Spain

Email: acabello@ac.upc.edu

Florin Coras
Technical University of Catalonia
C/Jordi Girona, s/n
08034 Barcelona
Spain

Email: fcoras@ac.upc.edu