Noname manuscript No.
(will be inserted by the editor)

LISP-MN

Mobile Networking through LISP

Alberto Rodríguez Natal · Loránd Jakab · Marc Portolés · Vina Ermagan · Preethi Natarajan · Fabio Maino · David Meyer · Albert Cabellos Aparicio

Received: date / Accepted: date

Abstract The current Internet architecture was not designed to easily accommodate mobility because IP addresses are used both to identify and locate hosts. The Locator/Identifier Separation Protocol (LISP) decouples them by considering two types of addresses: EIDs that identify hosts, and RLOCs that identify network attachment points and are used as routing locators. LISP, with such separation in place, can also offer native mobility. LISP-MN is a particular case of LISP which specifies mobility. In this paper we provide a comprehensive tutorial on LISP-MN, showing its main features and how it compares to existing mobility protocols.

Keywords Future Internet · Location/Identity Separation · Mobility · Multihoming

This work has been partially supported by a Cisco Unsolicited Research Proposal Grant.

A. Rodríguez Natal · L. Jakab · A. Cabellos Aparicio
Universitat Politècnica de Catalunya
C/ Jordi Girona s/n
Barcelona, 08034
Spain
E-mail: {arnatal, ljakab, acabello}@ac.upc.edu

M. Portolés
Centre Tecnologic de Comunicacions de Catalunya Castelldefels (Barcelona)
Spain
E-mail: marc.portoles@cttc.cat

V. Ermagan · P. Natarajan · F. Maino · D. Meyer
Cisco Systems
170 Tasman Drive
San Jose, California 95134
USA
E-mail: {vermagan, prenatar, fmaino, dmm}@cisco.com

1 Introduction

The current Internet architecture was not designed to easily accommodate mobility because IP addresses are used both to identify and locate the hosts. The fact that separating identity from routing location is an important design principle of inter-domain networks was known even before the Internet was created [1], but unfortunately the current architecture does not implement it. Such separation would seamlessly provide mobility and multihoming, among other desirable features, to the Internet. As a result, this is still an important research topic, and many solutions centred around this idea have been proposed [2–4]. Besides this, mobility also requires a location management system that maintains bindings between the identity and the location of the mobile client.

The Location/ID Separation Protocol [7] has been recently proposed to provide an incrementally deployable solution to such separation in the Internet. LISP considers two different types of addresses: Endpoint Identifiers (EIDs) and Routing Locators (RLOCs). EIDs identify hosts, and are assigned independently of the network topology while RLOCs identify network attachment points, and are used for routing. This allows that the EID remains unchanged even if a topological change occurs, such as a handover. In transit, packets are encapsulated; the outer header contains RLOCs while the inner EIDs. LISP also introduces a Mapping-System [8], a distributed database that maps EIDs to RLOCs.

LISP, as architecture, provides two important features to the Internet. First it truly splits location from identity, which is a requirement to provide native mobility and multihoming. With LISP, mobile clients can be seamlessly equipped with multiple wireless interfaces, and handover from different points of attachment, or among interfaces. Secondly, it provides a new level of indirection. A hostname lookup in DNS returns an EID, a second lookup is required to the Mapping-System to find the associated RLOC. With LISP, this Mapping-System acts as a location management system. But unlike in traditional mobility protocols, such as Mobile IP [13], LISP's Mapping-System is distributed and federated. Mobile IP's location management system (the Home Agent) is deployed at the mobile client's service provider.

LISP, at the time of this writing, is being standardized at the IETF. There is an active community behind LISP and important research efforts are being devoted into its development and deployment. LISP is currently being deployed at a Beta-Network [5], this pilot network is a multi-company multi-vendor effort to research real-world behaviour of the LISP Protocol and includes a total of 156 LISP-enabled networks spread in 26 different countries.

Within the LISP architecture [7], LISP-MN [9] specifies the mobility functionality, and LISPmob [6] is an open-source and fully-featured implementation. In this paper we present the LISP-MN architecture and a comprehensive tutorial on how it works along with a comparison with traditional mobility solutions. Particularly, Section 2 presents an overview of LISP-MN as well as detailed explanations of its main components. At the end of the tutorial, in section 3, we provide an analysis of LISP-MN and a brief comparison with Mobile IP while section 4 concludes the paper.

2 How LISP-MN works

2.1 Overview

The Locator/ID Separation Protocol (LISP) [7] specifies an architecture for decoupling host identity from its location information in the current address scheme. This separation is achieved by replacing the addresses currently used in the Internet with two separate name spaces: Endpoint Identifiers (EIDs), and Routing Locators (RLOCs). Host applications bind to host's EID, which is used as the address for transport connections. RLOCs are IPv4 or IPv6 addresses used for routing through transit networks. In order to reach a host, identified by its EID, one must first find the current location (RLOC) of the host. LISP introduces a publicly accessible Mapping-System [8] that is designed to serve the EID-to-RLOC mapping information. Once the RLOC associated to an EID is discovered, packets with headers from the EID namespace are encapsulated in a second header from the RLOC space, and are routed to the destination, where the LISP header is removed before delivering packet to the destination host. LISP introduces special gateway routers called Tunnel Routers that perform the LISP encapsulation, and decapsulation at each sites ingress and egress points.

Separating the host identity (EID) from its locator (RLOC) enables seamless endpoint mobility by allowing the applications to bind to a permanent address, the host's EID. The location of the host can change many times during an ongoing connection. Each time, the LISP tunnel routers will encapsulate the packets to the new RLOC, preserving the connection session from breaking. LISP-MN [9] leverages this feature to build a mobility architecture and protocol based on LISP. In LISP-MN a mobile node (MN) is typically statically provisioned with an EID that it uses for all its connections. Each mobile node essentially behaves as a LISP site in accordance to the LISP architecture. Packets (except for management protocols such as DHCP) are LISP encapsulated by the mobile node, and routed based on the RLOCs to the destination site. In the event of a handover, MN receives a new RLOC and updates its EID-to-RLOC mapping in the associated Mapping-System to maintain reachability at its new location. The LISP-MN architecture leverages four existing LISP components: (i) A Mapping-System, (ii) the LISP-MN, (iii) LISP Internetworking components (iv) LISP NAT-traversal.

2.2 The LISP Mapping-System

The LISP Mapping-System [8] (figure 1) is a central aspect of the LISP-MN architecture and it is a publicly accessible service that publishes location information associated with EIDs (EID-to-RLOC mappings). Main elements of

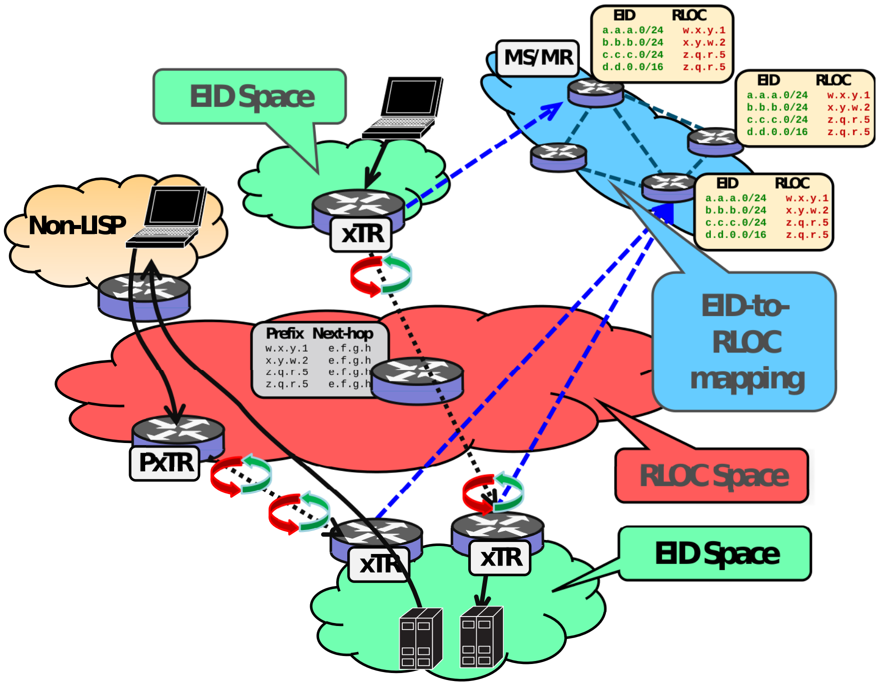

Fig. 1 An overview of the LISP architecture

LISP Mapping-System are Map-Servers (MS) and Map-Resolvers (MR) [10]. These are on the boarder of, and the interface to the Mapping-System. EID-to-RLOC mappings are stored in Map-Servers, and each Map-Server is associated with a partition of the EID name space, and stores the location information for those EID prefixes. Therefore, each LISP mobile node is associated with a specific Map-Server where it registers its EID-to-RLOC mapping, and updates it according to its movement. In this context, Map-Servers have assigned a set of prefixes (EIDs) and delegate them to either LISP tunnel routers or mobile nodes.

Map-Resolvers are used as an interface to the Mapping-System for looking up EID location information; they have a similar functionality as DNS resolvers have in today's Internet: LISP mobile nodes send EID lookup requests (Map-Request) to the Mapping-System through Map-Resolvers. LISP Mapping-System is designed to route EID lookup request from a Map-Resolver to the Map-Server responsible for that EID. At the time of this writing LISP has deployed a Mapping-System based on a BGP [8] at the LISP Pilot Network [5]. The system is an overlay that connects Map-Servers and Map-Resolvers. In this overlay, Map-Servers announce the EID prefixes that they serve through BGP. Map-Resolvers send EID requests onto the overlay, where they are routed according to the requested EID, and eventually reach the associated Map-Server that stores the EIDs location information.

A set of security mechanisms have been proposed in order to secure the mapping lookup process. Such mechanisms provide origin authentication, integrity and anti-reply protection to LISP's EID-to-RLOC mapping data. They also enable verification of authorization on EID-prefix claims in Map-Reply messages. For further information about these mechanisms we refer the interested reader to [12].

2.3 The LISP-MN

The lightweight tunnel router is the implementation of LISP-MN on the end-point or mobile node. Mobile node tunnel routers are used to encapsulate outgoing packets in a LISP header based on RLOCs before leaving the mobile node, and to remove the LISP header from incoming packets before sending them to upper layers ultimately reaching the destination application. The LISP-MN protocol is then, best understood, as the concatenation of three different phases: (i) Registering EID and obtaining an RLOC (ii) Signalling EID-to-RLOC bindings and transmitting data-packets (iii) Handover. In the following sections we review these phases in detail.

2.3.1 Registering EID and obtaining an RLOC

Each LISP-MN is configured with at least one EID. As we have discussed before, an EID is either a regular (/32) IPv4 or (/128) IPv6 address, that identifies the node uniquely and remains static independently of its location. If the node has also a DNS entry, this entry returns the EID. This address is typically assigned by the Map-Server provider and in LISPmob, it is configured in a static file.

In order to connect to the Internet, the LISP-MN also needs at least an RLOC. RLOCs are obtained by traditional mechanisms such as DHCP or configured manually and are location dependent. This means that as the mobile node roams across providers, it will obtain a different RLOC in each location.

For each new RLOC obtained by the LISP-MN, the node has to inform about the new EID-to-RLOC binding to its Map-Server. In order to do so LISP defines the Map-Register signalling message that includes the EID and the RLOC. The node may include multiple RLOCs if the node is multihomed and LISP supports any combination of IPv4 and IPv6 for EIDs and RLOCs. The LISP-MN and the Map-Server share a pre-configured key (again configured in a static file in LISPmob), this key is used to sign the Map-Register to ensure authentication. Once the Map-Server receives a valid Map-Register containing an EID-to-RLOC mapping it will it make it accessible throughout the Mapping-System.

Figure 2 shows a LISP-MN configured with the EID 3.0.0.3/32 and two RLOCs from two different providers (X and Y): 12.0.0.2 and 13.0.0.2. The MN registers these two bindings 3.0.0.3/32-12.0.0.2 and 3.0.0.3/32-13.0.0.2 into its Map-Server (identified with the address 66.2.2.2). The MN and a MS

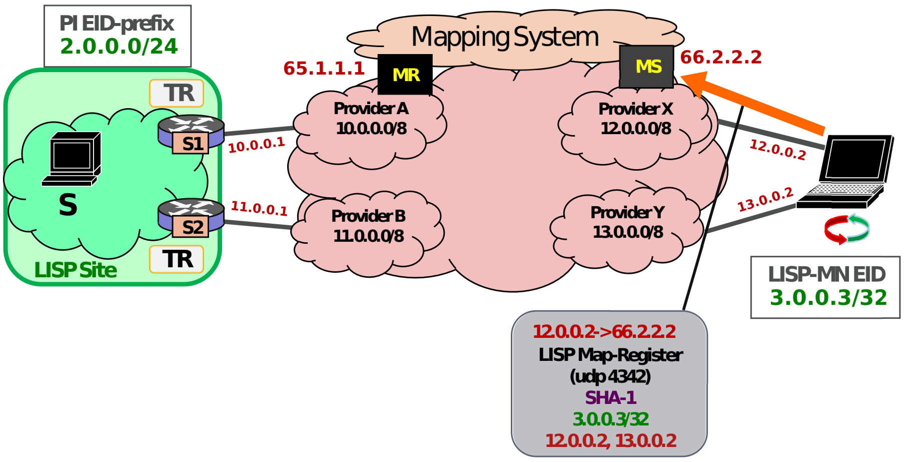

Fig. 2 Registering an EID-to-RLOC bindings

have a pre-configured key and this Map-Register message is signed and hence, authenticated.

2.3.2 Signalling EID-to-RLOC bindings and transmitting data-packets

Once a valid EID-to-RLOC has been registered into the Map-Server the mobile node can start sending and receiving data packets. In this section we describe how a static node located in a LISP site establishes a connection with a mobile node. Special cases like a MN within a LISP site and communication between two MNs are also covered. In section 2.4 we also present the case when the peering site is non-LISP.

As figure 3 shows, the static node first retrieves the EID of the node (3.0.0.3/32) by querying the DNS and then transmits a packet addressed to this EID just as in the plain Internet. The packet is routed until it reaches the LISP tunnel router. Upon reception, the tunnel router checks whether it knows the EID-to-RLOC binding or not. For this purpose each LISP node includes a data-structure called Map-Cache which stores such information.

If the tunnel router's Map-Cache does not contain the binding for the destination EID, it will trigger a Map-Request message. This message is used to query the Mapping-System for a particular binding. The Map-Request is sent to the Map-Resolver, which is typically co-located with the Map-Server. In turn, the Map-Resolver forwards the Map-Request message through the Mapping-System that routes it, according to the destination EID, until it reaches the Map-Server that provides mapping services to the MN.

The Map-Server then constructs a reply for the Map-Request using another LISP defined message, the Map-Reply. This message mainly contains the EID of the MN (3.0.0.0/32), the set of RLOCs that provide connectivity to the MN (12.0.0.2 and 13.0.0.2) and the priorities and weights of each locator, this is used for ingress load-balancing. Finally the Map-Reply also contains a

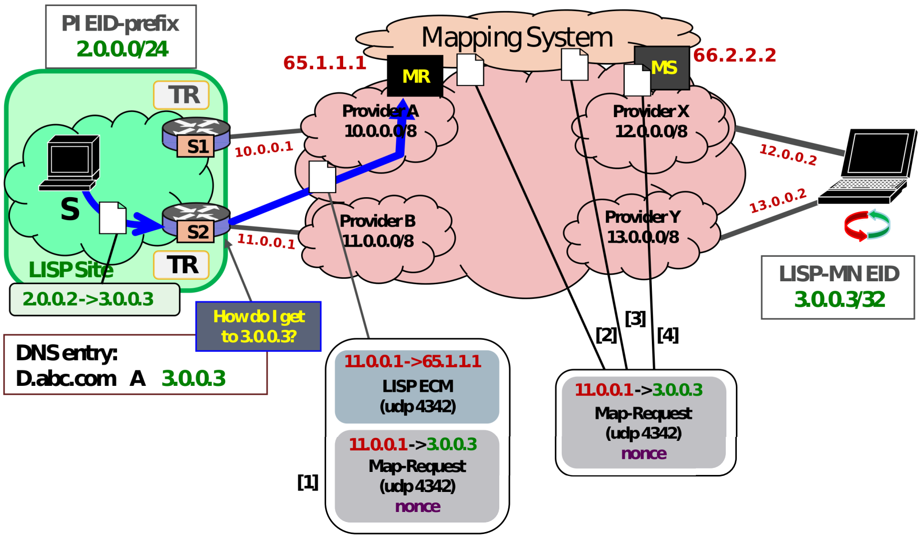

Fig. 3 Signaling an EID-to-RLOC binding (Map-Request)

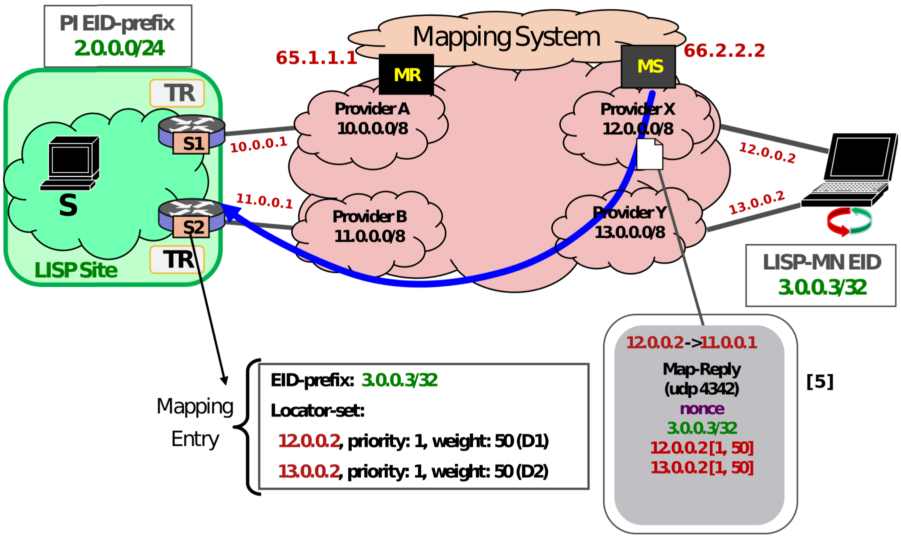

Fig. 4 Signaling an EID-to-RLOC binding (Map-Reply)

Time-To-Live (TTL) that defines the amount of time for which this particular mapping is valid, and a nonce to avoid unsolicited Map-Replies. The Map-Reply is sent directly to the tunnel router that will install this binding in its Map-Cache and will use it to encapsulate packets towards the MN until the TTL expires. At this point it will request a fresh binding. Typically, as in TCP, the node will reply with another data-packet addressed to the EID of the node (S).

Since the Map-Cache of the MN does not have the binding for such EID it will trigger a Map-Request querying for the RLOC of the LISP site (10.0.0.1 and 11.0.0.1). This Map-Request, as in the previous case, will be routed through the Mapping-System towards the Map-Server servicing the site that in turn, replies with a Map-Reply. The mobile node, upon reception of this message will install this binding in its Map-Cache and will start to encapsulate data packets directly to the locators of the LISP site according to whatever policies have been defined (weight and priorities). Such data-packets are decapsulated at the tunnel router and forwarded, as in the plain Internet, to the final destination S.

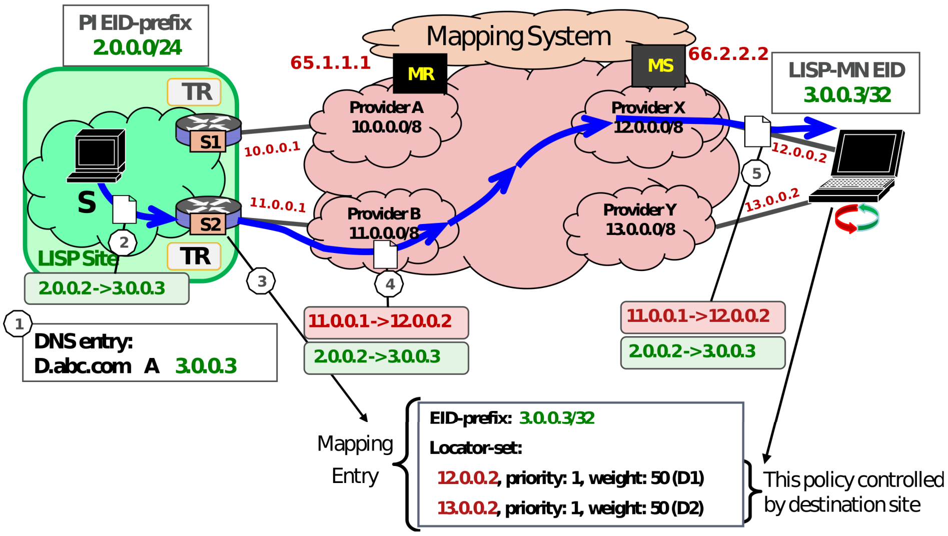

Fig. 5 Encapsulating and decapsulating data-packets

Figure 5 covers the common scenario where a MN communicates connected to the legacy Internet with a peer located in a LISP site. In the case of a MN behind a LISP site, double encapsulation is required. The RLOC of the MN is in fact an EID assigned by the xTR in charge of the LISP site. We refer to this EID as Location EID and to the permanently assigned MN's EID as Permanent EID. In this scenario, when the MN roams into a LISP site, the xTR assigns (by means of DHCP) the location EID. The MN registers this EID into the Mapping-System as its RLOC. The peer that wants to communicate with the MN queries the Mapping-System and receives the Location EID as the RLOC of the MN. The peer will then realize that the Location EID is not routable and will consequently query again the Mapping-System to obtain the RLOC, this is the IP address assigned to the xTR where the MN is attached. At this point the peer (typically an xTR, or another MN) will then double encapsulate the packets towards the MN. Upon reception, these packets will be first decapsulated by the xTR, and then by the MN.

2.3.3 Handover

In this section we describe the handover process in LISP-MN. When a MN changes its attachment it regains connectivity in a new subnetwork. It first obtains a new RLOC and, as described in section 2.3.1, it notifies the new EID-to-RLOC binding to its Map-Server. The MN has to update also all the bindings stored in the Map-Cache of the peers, either routers or nodes, with which it is communicating. In order to do it uses the special signalling message called Solicit-Map-Request (SMR). The reception of such message triggers a Map-Request to refresh the binding, it is important to note that such message is transmitted over the Mapping-System, and hence prevents the double-jump problem. Overall, the handover latency in LISP is 1.5 Round Trip Times. Research efforts to optimize such handover latency are already under development and take base on LISP-SEC [12].

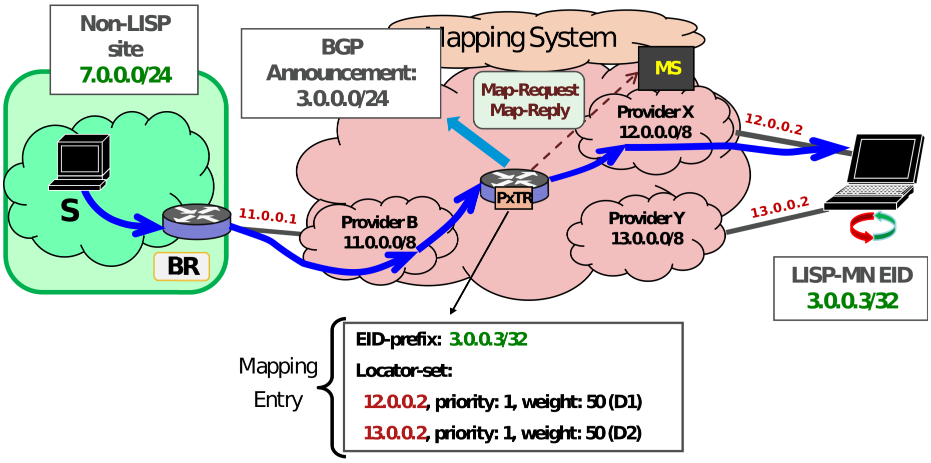

Fig. 6 Inter-networking with non-LISP sites

2.4 The LISP Inter-networking components

The LISP internetworking components are proxies that facilitate communication with legacy nodes that are not LISP enabled. Mainly, the PxTR is a LISP-enabled router that attracts traffic by announcing, by means of BGP, EID prefixes. Then it queries the Mapping-System to obtain the corresponding RLOC bindings and encapsulate the data-packets towards them. Additionally, PxTRs also decapsulate packets sent by LISP-enabled sites and nodes towards the non-LISP Internet. This is done to avoid ingress-filtering issues.

As shown in figure 6, the PxTR is announcing at the BGP DFZ an aggregated EID prefix that covers the one configured at the MN. In this scenario we are assuming that this entire prefix is used either by LISP sites or LISP-MNs. By means of this BGP announcement, PxTRs attracts traffic addressed to the EID of the MN (3.0.0.3/32) and, upon reception of a data-packet it queries the Mapping-System to obtain the locator set (12.0.0.2 and 13.0.0.2) and proceeds to encapsulate packets. In turn, the PxTR is also used to decapsulate data-packets addressed to non-LISP sites.

2.5 LISP NAT Traversal

LISP control and data messages are UDP encapsulated and they use the destination port 4342 and 4341 respectively. However, without prior configuration, NAT-boxes do not allow incoming packets addressed to these ports. In this section we describe how LISP-MNs perform NAT-traversal operations.

In order to avoid this issue LISP defines a new network element, the RTR (Re-encapsulating Tunnel Router). This entity acts as a proxy between the NAT box and the MN's incoming packets. The operations of a MN behind a NAT are as follows. First the MN must check weather its behind a NAT box. To obtain this information the MN sends a special signalling packet (NAT Info-Request) to its Map-Server. In turn, the Map-Server replies with a list of available RTRs and the actual source address and port of the MN. With this, MNs are aware that they are (or not) behind a NAT box. In this case, the MN sends a Data-Map-Register message to the RTR with source port 4341. This message is an encapsulated Map-Register which opens the port 4341 in the NAT table and it is used by the RTR to infer the translated RLOC and port of the MN. Then, the RTR forwards the Map-Register to the appropriate Map-Server. Please note that this Map-Register contains the RLOC of the RTR, not the one of the MN, so all MN's incoming packets are received by the RTR which, in turns, forwards them to the the translated RLOC and port of the MN. This way the RTR acts as a signalling and data-proxy for the MN.

Figure 7 shows an example of the packet flow when the MN is behind a NAT. The RTR register its RLOC (77.3.3.3) as the RLOC for the MN's EID (3.0.0.3). In its NAT table it stores the port (6789) and IP (12.0.0.2), since this is the real address and port received in the Data-Map-Register.

3 Analysis of LISP-MN

During the last decade we have witnessed huge progress in wireless access technologies. This has lead to a increase in the adoption of mobile devices and demand for mobile Internet. Consequently, a plethora of solutions and protocols have been proposed (see [15] and the references therein). Arguably, the most popular is the Mobile IP [13] family of protocols. LISP-MN has a set of features with respect to Mobile IP that makes it a real alternative. In the following we detail the main reasons that support such statement:

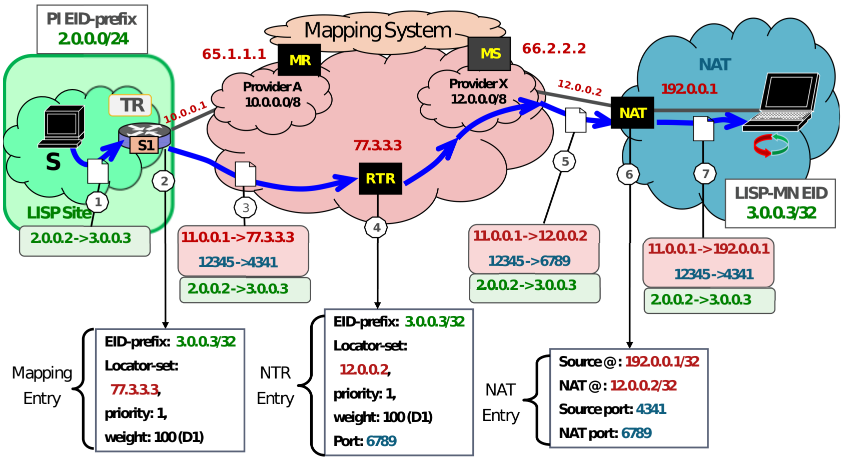

Fig. 7 MN behind a NAT box

- The Mobile IP family of protocols is a set of protocols that provides basic and advanced functionalities to mobile nodes. For instance there are two separate versions for IPv4 and IPv6, and additional protocols for network (prefix) mobility. Furthermore, advanced features such as fast handovers [16] or multihoming [17] are again defined in separate documents. As a result, a developer willing to adopt Mobile IP must read and implement different protocols defined in several documents. In LISP-MN all the features are defined in a single protocol, and thus only require a single implementation. Currently LISP-MN supports IPv4, IPv6, network mobility and multihoming natively. The benefits of the native multihoming of LISP are inhered by LISP-MN: each EID prefix can be mapped to more than one RLOC, and each RLOC can be assigned specific priority and weight. This simplifies adoption and reduces significantly capital expenditure costs.
- LISP-MN separates the control plane functionality from the data plane, allowing each to scale independently. Since LISP-MN does not require Home Agent or Foreign Agent network elements in the data plane, it avoids triangle routing at the data plane level, for both IPv4 and IPv6 address families, along with network mobility Data packets always follow the shortest path and hence, in this context LISP-MN incorporates native route optimization support. It is worth to note that when communicating with non-LISP sites, communications must be forwarded through a proxy.
- Separation of control plane from data plane in LISP-MN facilitates the decoupling of end-point identity from the mobility service provider. The sole functionality of the control plane is to locate a mobile node, much like DNS locating a service or a host name today. Similar to DNS, LISP control plane has a distributed and federated Mapping-System. Mobility becomes a native feature of the network architecture and avoids mobility provider lock-in. In this context, LISP-MNs can change their RLOC provider (typ-

ically an ISP) and are tight to their EID provider, however and unlike in Mobile IP, such EID provider may not be an ISP (i.e, the home of the mobile node) but rather a third-party company. EID providers do not operate in the data plane as Home Address providers in Mobile IP, but in the control plane, and represent new business opportunities.

4 Conclusions

In this paper we have presented the LISP-MN protocol which in short, is a lightweight implementation of the LISP protocol intended for mobile use. LISP-MN truly decouples identity from location by creating two separated namespaces glued by a control pane (Mapping-System) that provides bindings between both type of addresses. In a single protocol, and thereby in a single implementation, LISP-MN is a fully featured mobility protocol that supports both IPv4 and IPv6, including network mobility, with route optimization and native multihoming support. LISP-MN also supports interoperating with legacy nodes (by means of proxies using sub-optimal paths) and NAT-traversal. Given the amount of features that LISP-MN incorporates, and that it is already under deployment in the LISP Beta Network, this protocol represents a real alternative to provide mobility to the Internet.

References

1. J. F. Shoch, "Inter-Network Naming, Addressing, and Routing", in IEEE Proc. COMPCON Fall 1978, pp. 72-79. Also in Thurber, K. (ed.), Tutorial: Distributed Processor Communication Architecture, IEEE Publ. #EHO 152-9, pp. 280-287, 1979.
2. E. Nordmark, M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", RFC 5533, June 2009.
3. R. Moskowitz et al "Host Identity Protocol", RFC 5201, April 2008.
4. J. Pan, R. Jain, S. Paul, C. So-In, "MILSA: A New Evolutionary Architecture for Scalability, Mobility, and Multihoming in the Future Internet", in *IEEE Journal on Selected Areas in Communications (JSAC), Special issue on Routing Scalability*, 2010.
5. http://www.lisp4.net/
6. http://lispmob.org/
7. D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, "Locator/ID Separation Protocol (LISP)", draft-ietf-lisp-21, Internet Engineering Task Force, February 2012, work in progress.
8. Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "LISP Alternative Topology (LISP-ALT)", draft-ietf-lisp-alt-10, December 2011, work in progress.
9. D. Meyer, D. Lewis, D. Farinacci "LISP Mobile Node", draft-meyer-lisp-mn-06, Internet Engineering Task Force, October 2011, work in progress.
10. V. Fuller, D. Farinacci "LISP Map Server Interface", draft-ietf-lisp-ms-15, Internet Engineering Task Force, January 2012, work in progress.
11. D. Lewis, D. Meyer, D. Farinacci, V. Fuller, "Interworking LISP with IPv4 and IPv6", draft-ietf-lisp-interworking-03, Internet Engineering Task Force, February 2012, work in progress.
12. Maino, F., Ermagan, V., Cabellos, A., Sausez, D., and O. Bonaventure, "LISP-Security (LISP-SEC)", draft-ietf-lisp-sec-01, January 2012, work in progress.
13. C. Perkins, "IP Mobility Support" RFC 3344, August 2002.
14. D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

15. W. M. Eddy, ”At what layer does mobility belong?” in *IEEE Communications Magazine*, Number 42, Vol 10, 2004.
16. R. Koodli, ”Fast Handovers for Mobile IPv6 (FMIPv6)” RFC 4068, 2005
17. G. Tsirtsis et al. ”Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support”, RFC 5648, 2011