MOBILITY IN IP NETWORKS USING LISP AND OPENWRT

Cătălina Maria MĂLĂCEA, Dan Nicolae ROBU, Marian ALEXANDRU

Transilvania University of Brasov, Romania
(catalina.malacea@yahoo.com, dan.robu@unitbv.ro, marian.alexandru@unitbv.ro)

DOI: 10.19062/1842-9238.2018.16.3.10

Abstract: *Because the Internet was originally designed to interconnect several hundreds of networks and now has more than one billion hosts, scalability issues have started to appear. The current scalability of today's Internet architecture is mainly due to the use of a single IP address space, both for identifying host transport sessions, and for routing networks. Due to the large amount of information on the Internet, routing protocols have an important role. The size of the routing tables in the Default Free Zone (DFZ) is steadily increasing. The underlying reasons for this rapid growth are the independent addresses of suppliers and multihoming. In order to help solve these scalability problems associated with the said increase, the LISP (Locator Identifier Separation Protocol) was developed. It allows the separation of IP addresses into two different address spaces: the identity of the device, known as Endpoint Identifier (EID), and its location, known as the Routing Locator (RLOC), as opposed to the current routing architecture and IP addressing, which use a single addressing space, the IP address. The approach described in this paper demonstrates two advantages of the LISP Protocol: 1. It allows changing the connection of an ongoing call using the Circuit by Unify application, from a wireless network to a 3G network without losing the connection, based on the use of the open-source LISP implementation Open Overlay Router (OOR) as a platform and 2. A user can be addressed using the assigned IP address, irrespective of the network connection used.*

Keywords: *LISP, RLOC, EID, multihoming, OOR*

1. INTRODUCTION

The Locator/Identifier Separation Protocol (LISP) started as a research in the Routing Research Group, making its way to the Internet Engineering Task Force (IETF), and becoming a very attractive technology for Future Internet Architecture. LISP can be used to accommodate the need for Internet growth while facilitating the deployment of new services.

LISP was proposed for the first time by Cisco in the IRTF (Internet Research Task Force) and now is under development in the IETF. This protocol has been developed from its original design to adapt to the Internet constraints imposed by it, but at the same time offering solutions for the scalability issues.

2. LISP OVERVIEW

LISP is a network architecture and a set of protocols that implement a new semantic IP addressing. LISP creates two namespaces and uses two IP addresses: Endpoint identifiers (EIDs) that are assigned to end users and routing locators (RLOCs) that are assigned to devices (mainly routers) that make up the global routing system.

The Locator / ID Separation concept has been considered important for solving the scalability issues of the DFZ routing table. By dividing the identity of the device, its endpoint identifier (EID), and location of the device (RLOC) into two different namespaces, improving scalability of the routing system can be achieved by a greater aggregation of RLOCs.

In the figure below, the LISP architecture is presented. It includes the Endpoint Identifier (EID), which defines “who” the device is and the RLOC, which describes how a device is attached to the network. The Egress Tunnel Router (ETR) receives packages from the Internet, decapsulates them and sends them to the EID. The Ingress Tunnel Router (ITR) receives packages from hosts, encapsulates them and sends them to LISP sites or non-LISP sites.

An Alternative Logical Topology (ALT) can be built for managing EID-to-RLOC mappings for LISP and for accepting the prefixes provided by devices and informing an aggregated EID prefix which represents that distinct space to other parts of the ALT. The Map Resolver (MR) connects to the ALT and accepts the messages from the ITR encapsulated in Map-Request, decapsulates them and forwards them to the ETR responsible of the requested EID message.

The Map Server (MS) manages the mapping database by registering the ETRs from the LISP Site with the EID prefix and publishes them in a database. The Proxy ITR attracts non-LISP traffic designated to LISP sites by allowing non-LISP clients to connect to the LISP site and encapsulating this traffic to LISP sites. Proxy ETR is used for non-LISP sites that want to receive traffic from a LISP site but the LISP site is connected to a service provider network that does not accept non-routable EID packages.

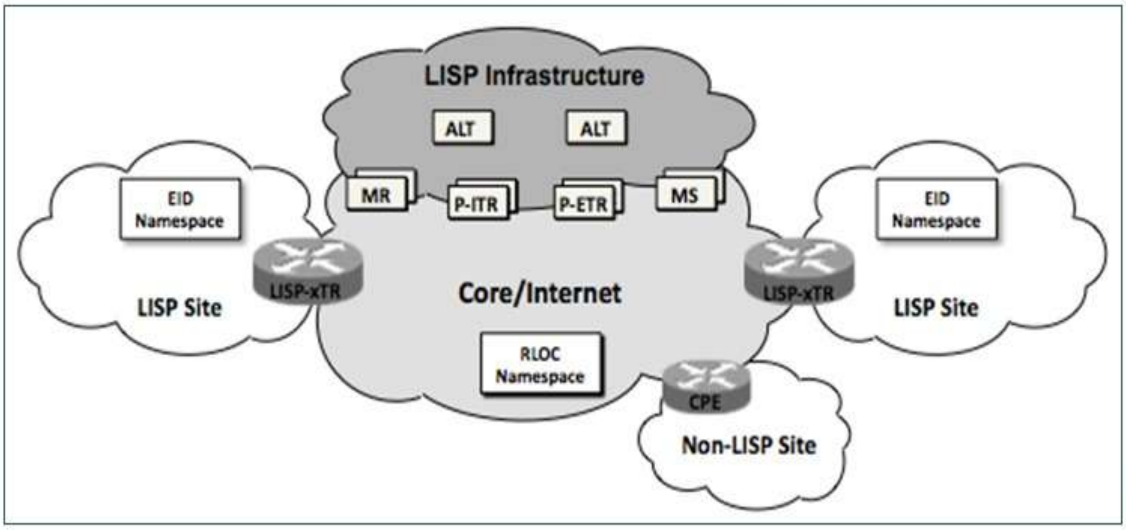

FIG.1 LISP architecture

2.1 Multihoming. Multihoming is a way to configure a PC that can have multiple network interfaces and multiple IP addresses. The multihomed PC is the host, which can be connected directly or indirectly to multiple networks, with the goal of increasing the network reliability.

The classic part is represented by a fixed network, being accessed via Wi-Fi, and the improvement brought is the multihoming mechanism with the 3G mobile network.

The multihoming is not new, but with LISP we get to keep our EID, so there is no change from the point of view of our partner.

3. PRACTICAL APPROACH

This section explains the structure of the network and the way in which the connection of an ongoing call can be changed using the Circuit by Unify application, from a wireless network to a 3G network without losing the connection.

The virtual machine OpenWrt - LEDE 17.01.1 x86 was installed in Oracle Virtual Box (which is a highly extensible GNU/Linux distribution for wireless routers [5]).

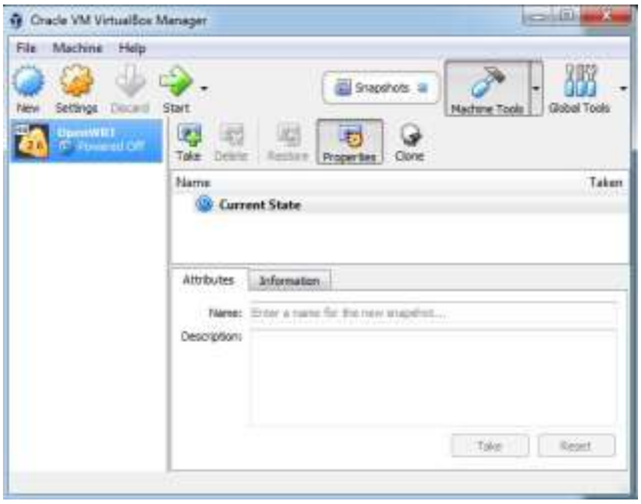

FIG.2 Installation of OpenWRT in Virtual Box

3.1 Network Settings for Virtual Box. The interface LAN 192.168.61.1, a host-only adapter on which the DHCP server was disabled in Virtual Box in order to retrieve the DHCP function from OpenWRT .

FIG.3 Host-Only Network Adapter

The Internet access was made through the NAT gateway, in order to download from the Internet the necessary packets for installing the Open Overlay Router (OOR). Network Address Translation (NAT) is the easiest way to access an external network from a virtual machine.

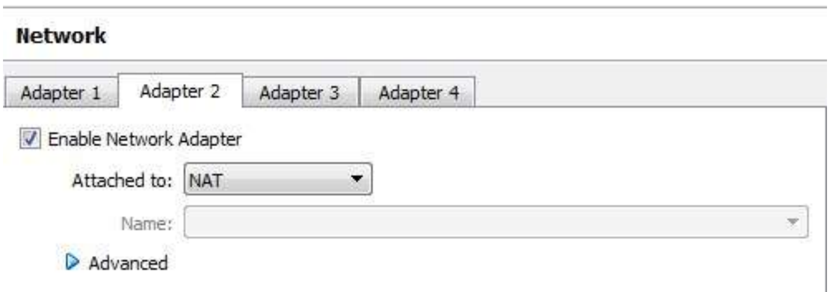

FIG.4 NAT Network Adapter

Further, the NAT network adapter was configured in Bridged mode, in order to access the Internet directly. With the help of Bridged network, Virtual Box uses a driver device on the host system, which filters data from the physical network adapter.

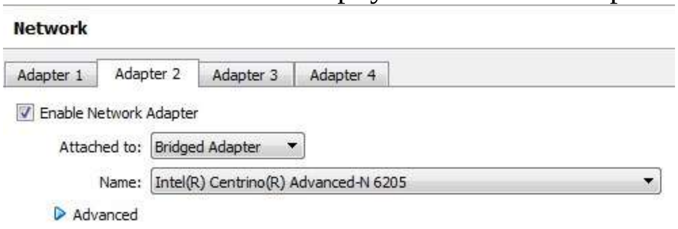

FIG.5 Bridged Network Adapter

3.2 Open Overlay Router (OOR). To configure the LISP protocol, an open-source modular solution was chosen: OpenOverlayRouter.

Open Overlay Router is an open-source application that can be used to create programmable overlaid networks. OOR is a complete implementation of the overlaid router, written in programming language C, available for OpenWRT, Android and Linux and being an open source under the Apache 2.0 license [7]. The OOR project is used to encapsulate packets in LISP-compliant packages and directs them over the basic physical infrastructure. In the current version, OOR uses the LISP control plan protocol (e.g., recovery and update mapping, etc.). Most of the OOR architecture revolves around the LISP protocol and its components. EIDs and RLOCs are impossible to identify from IPv4 and IPv6 addresses, allowing compatibility with the existing Internet architecture. A distributed database is responsible for maintaining associations between IDE and RLOC. Regarding the LISP devices implemented by OOR, it can now act as an xTR, MS / MR, RTR, or LISP-MN.

3.3 Installing the OOR mobile application. Open Overlay Router includes support for Android devices which work in a similar way to LISP-MN.

FIG.6 Open Overlay Router mobile application

3.4 Installing OOR on OpenWRT. The last version of the Open Overlay Router source code can be accessed at Github: *//github.com/OpenOverlayRouter/oor.git*. In order to build the code for Linux operating systems, the command *make* was executed in the top-level directory. For installing in /usr/local/sbin, the command *sudo make install* was executed. Once the code was installed successfully on the device, oor.conf.example was copied in /etc/oor.conf and edited with the corresponding values.

3.5 LISP Beta Network. The experimental LISP network used for tests is the LISP Beta network, which allows us to test the scenario in real terms. LISP is being deployed at a Beta-Network; this pilot network is a multi-company multi-vendor effort to research real-world behavior of the LISP Protocol which includes approx. 156 LISP-enabled networks spread in 26 different countries. The Beta Network contains elements such as Map-Servers, Map-Resolvers, Proxy Routers and xTR’s. Participants host one or more of these components [6].

3.6 Configuration. The configuration of the entire network is divided as follows:

LISP vlab.unitbv.ro is configured with a static IP to serve 2 LISP sites: LISP Site1 and LISP Site2.

Vlab.unitbv.ro is configured with a static university IP. Having a fixed IP, it constitutes an „anchor”, more precisely the RTR function. It takes over the traffic from the customers, from NAT networks and retransmits it to the LISP Beta network. Clients behind a NAT cannot be located by Map Server/Map Resolver and then the RTR becomes a „proxy” for them. A re-encapsulating tunnel router (RTR) provides communications support for LISP-to-LISP traffic between LISP sites that do not share common locator space. The functionality is that an RTR takes in LISP encapsulated packets from an ITR in one locator scope, decapsulates them, does a map-cache lookup, and then re-encapsulates them to an ETR in another locator scope. [8]

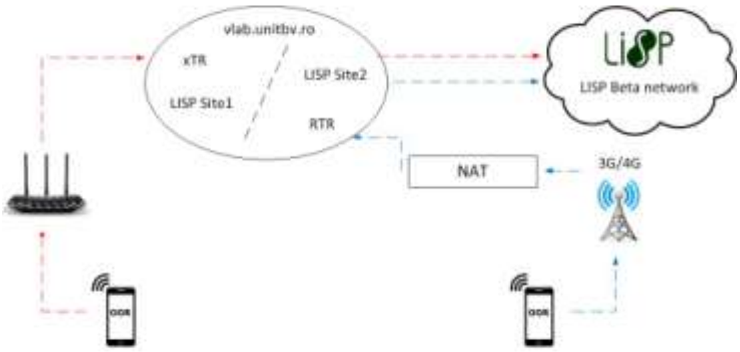

FIG.7 Network structure

In LISP Site1, the xTR is configured, providing both ITR and ETR functions and in LISP Site2 the RTR is configured, which is being required for the NAT Traversal function, as most 3G / 4G mobile operators use NAT. NAT changes a private IP address into a public IP address, in order to allow stations that use private addresses to access the Internet via a public one and hiding an unlimited number of devices under the same IP.

When NAT traversal feature is enabled, OOR is configured to send all data traffic through RTRs, even if the interface has a public address.

There are two possibilities when it comes to accessing the LISP Beta Network: access can be achieved through a Wireless Access Point, working as a bridge between vlab.unitbv.ro and the wireless network, which has direct connectivity to the network; or, through the 3G / 4G mobile network that has the application installed OOR, where the mobile is behind a NAT, being connected to an RTR that decapsulates the traffic received to re-encapsulate it again in the LISP Beta Network then on the Internet.

4. TESTING THE SCENARIO

For the test scenario, the Circuit application, connected to the Circuit Server, was started; after that, an audio call was made. Initially, the audio call was made on a wireless network, after which the mobile network (3G) was activated and the wireless network was disconnected, so that the call was automatically transferred without interruption.

When the xTR (in fact ITR) receives a LISP packet, it asks the MS for the RLOC of the destination, if not already available in the local table (on Wi-Fi). When it changes to 3G, the RTR receives the packets and sends them. Both xTR and RTR addresses are known as a destination for the MN so the packets will reach the MN.

CONCLUSIONS AND FUTURE WORK

Mobility is related to a situation where a device changes its attachment to the network, which can be produced due to a physical movement of the device. The problem of changing addresses due to mobility happens when a host moves to a different network, because in this case it can no longer be reached by other hosts on the previous address and its existing data flows are terminated. In the above-presented scenario we were able to demonstrate an easy way to use a separate IP. Even if the temporal connectivity is interrupted, the device uses the same IP, therefore when the LISP connectivity became available again, the session continued exactly from the same place where it was interrupted. An advantage can be the keeping of the same identity, as authentication should not be reinitialized every time, since identity never actually changes. Separation between location and identifier is considered and recognized as the optimal method for user/host mobility.

As a future work, we intend to improve the security level of this project and to show how LISP can be used for IPv6 transitions, network virtualization, and mobility.

REFERENCES

[1] *** ANR INFRA 2013 Project LISP-Lab, online resource accessed in April 24, 2018, at the address http://lisplab.openlisp.org/

[2] D. Saucez, L .Iannone, O. Bonaventure, D. Farinacci – *Designing a Deployable Future Internet: the Locator/Identifier Separation Protocol (LISP) case*, vol. 16, Issue: 6, Nov.-Dec. 2012, pages 14-21*;*

[3] T. Balan, D. Robu, and F. Sandu - *Multihoming for Mobile Internet of Multimedia Things*, vol. 2017, Article ID 6965028, 16 pages;

[4] A. R. Natal, L. Jakab, M. Portolés, V. Ermagan, P. Natarajan, F. Maino, D. Meyer, A. Cabellos Aparicio - *LISP-MN: mobile networking through LISP*, Wireless Personal Communications, vol. 70, no. 1, pp. 253-266, 2013.

[5] *** OpenWRT Project, online resources accessed in April 9, 2018, at the address https://openwrt.org/about

[6] *** LISP Beta Network, online resources accessed in May 3, 2018, at the address https://www.lisp4.net/beta-network/

[7] *** Open Overlay Router (OOR), online resources accessed in April 18, 2018, at the address http://www.openoverlayrouter.org

[8] *** Locator ID Separation Protocol (LISP) Overview, online resources accessed in April 20, 2018, at the address https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/15-mt/irl-15-mt-book/irl-lisp-support-for-disjoint-rloc-domains.html