LISP : a Novel Solution For The Transition From IPv4 to IPv6

Khalid EL KHADIRI, Najib EL KAMOUN, Ouidad LABOUIDYA, and Rachid HILAL

STIC Laboratory, Faculty of Sciences, Chouaib Doukkali University, El Jadida, Morocco

Summary
In order to connect to the Internet, each device needs an IP address. However, the number of IPv4 addresses is limited and insufficient to respond to the explosion of demand for new addresses for connected devices, including connected objects and smartphones. On February 2011, the IANA (Internet Assigned Numbers Authority) reported having exhausted the /8 blocks of IPv4 addresses intended for regional Internet registry (RIR). Gradually, the RIRs have exhausted their stock in turn. Consequently, it is necessary to deploy the new version of the Internet Protocol (IPv6), which considerably extends the address space. As IPv4 and IPv6 are incompatible (the headers are different from each other), the transition from the current version (IPv4) to the new version (IPv6) can't be done in a period of time, and this deployment has to be done gradually. In order to counter this issue, three solutions are possible: a) put a double stack on each device, b) translation or c) tunneling. Tunneling is the best solution possible. However, as each technology, tunneling is influenced by scalability. In this paper, we are proposing a solution for the IPv4/IPv6 transition, based on the LISP protocol (Locator/Identifier Separation Protocol), and we are studying its impact in relation to the IPv6 manual tunnel and the native IPv4/IPv6 networks. For this reason, we will perform an experimental study of the scalability under GNS3; by increasing the number of customers and varying the different technologies in order to deduce the best solution. For the performance measurements, we used VoIP traffic generated by IP SLA (Service Level Agreement). The evaluation criteria are the delay, jitter, MOS score, and loss rate. The results of this research will be important for the network administrators and various Internet service providers (ISP) for planning IPv6 migration networks.

Key words:
IPv4, IPv6, manual tunnel, LISP, GNS3, IP SLA, VoIP, Scability.

1. Introduction

The connection between the computer nodes requires a protocol so that each node is recognized and the source and the destination of each packet are known. IPv4, the version 4 of the protocol IP (Internet Protocol), is widely used today. IPv4 uses 32 bits and can only cover 4.3 billion nodes worldwide [1]. However, with the rapid growth of the size of the Internet (number of users, Internet of things, etc), IPv4 has become limited, and some Internet Service Providers (ISP) don't have enough IP addresses to respond to the customers demand. Consequently, it is necessary to deploy the new version of IP (IPv6) to maintain the rhythm of development of the Internet. IPv6, developed by the IETF (Internet Engineering Task Force), is considered more efficient than IPv4 in terms of scalability, reliability, speed, and security [2]. Moreover, the IPv6 address space is larger than that of IPv4 because IPv6 uses 128 bits instead of 32 bits for IPv4. With this addressing capacity, IPv6 can encompass all nodes and services that may require IP, both now and in the future.

IPv4 and IPv6 are two incompatible protocols (the size and format of the addresses are different). As a result, the transition from IPv4 to IPv6 can only be done gradually and step by step. For this reason, the IETF has put in place different mechanisms, most of them have different characteristics.

The LISP protocol was developed by Cisco in 2006 and adopted as a RFC 6830 standard until 2013, but its use in the transition from IPv4 to IPv6 is still new. According to our research, no scientific work has studied the LISP protocol as a solution for transition from IPv4 to IPv6, its deployment, its impact on network performance, on transported applications as well as on IPv6 tunneling, and on native IPv4/IPv6 networks. Only a few people, blogs, etc. specify it can be used in the IPv4/IPv6 transition.

Taking into account our remarks, in this research paper, we will implement and study the LISP protocol as a solution for transition from IPv4 to IPv6 in order to study its impact in relation to the IPv6 manual tunnel and the native IPv4/IPv6 networks. We will validate this work by an experimental study of the scalability under GNS3 in order to compare our proposed solution, based on the LISP protocol, with the manual IPv6 tunnel and the two native IPv4/IPv6 networks. We will perform this study over a test network infrastructure under GNS3 using IP SLA generated VoIP traffic by increasing the voice load in terms of the number of customers communicating VoIP and by varying the different technologies in order to determine the best solution. Regarding performance measurements, we will use the following parameters: the delay, jitter, MOS score, and loss rate.

The rest of the document is organized as follows. Section 2 will present an overview of the strategies of IPv4/IPv6 transition and their classification. Section 3 will describe our proposed solution (based on the LISP protocol), its architecture, its operating principle, its applications, and its advantages. Section 4 will discuss a non-exhaustive state of the art of the research work performed in this research field. Scenarios of the experimental study will be described

Manuscript received October 5, 2018
Manuscript revised October 20, 2018

in section 5. The results and the comparative analysis will be discussed in section 6. Section 7 will describe a global discussion of the results and the synthesis of the scalability of the studied technologies. Conclusions and perspectives will be presented in the final section of this paper.

2. Strategies of transition from IPv4 to IPv6

Transition strategies are methods that provide a mean of connection between hosts/sites using similar or different IP protocols because the two versions of IPv4 and IPv6 protocols can't communicate directly (IPv4 and IPv6 are incompatible). Therefore, in order to transfer data, a method is needed. These methods are classified into three strategies.

2.1 Dual Stack

Dual stack: is a method of cohabitation in which both IPv4 and IPv6 protocols operate simultaneously and side by side as shown in Figure 1 below. Regardless of the protocol used, the node is able to respond when a request or traffic is received [3]

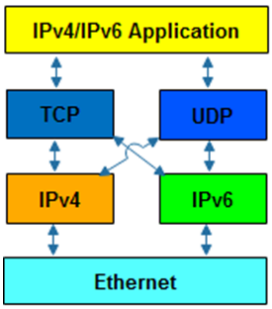

Fig. 1 Dual stack.

2.2 Tunneling

This strategy is used when two hosts/sites use the same IP version but are separated by another network with a different IP version [4]. Tunneling consists in establishing a virtual link [5] through networks by providing a connection in the middle of them. Tunneling techniques are classified into two categories: automatic tunnels and manual tunnels. Manual tunnels are manually configured, and tunnel endpoints are predefined, while automatic tunneling doesn't require manual configuration and endpoint specification. The operation of the tunneling mechanism is illustrated in Figure 2 below. Here are some tunneling techniques that can be used in order to transport IPv6 on IPv4.

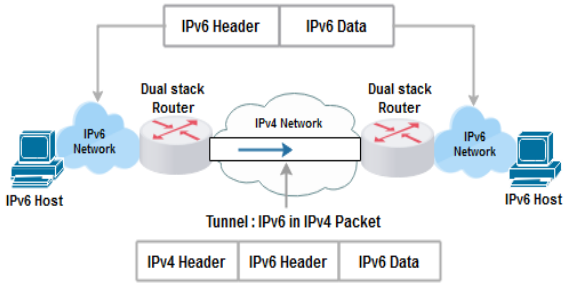

Fig. 2 Tunneling.

Manual tunnel

The manual tunnel provides a connection between IPv6 networks on the IPv4 network as a static point-to-point tunnel. Both ends of the tunnel are configured manually. This technique provides a secure connection between the two ends. [6].

ISATAP

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) is an automatic tunneling mechanism, designed for an Intra-Site (Intranet) scope allowing to connect IPv6 nodes on an IPv4 network [7] [8]. Unlike 6over4, it doesn't require an IPv4 infrastructure compatible with multicast.

6rd

6rd (IPv6 Rapid Deployment) is a transition mechanism used by some service providers to quickly deploy IPv6 to their customers who want to use IPv6 on an existing IPv4 infrastructure. 6rd has taken the operating principles of the 6to4 protocol while correcting its defects. Instead of using one and only one prefix (2002::/16 for 6to4), 6rd uses a different prefix for each ISP. Similarly, the 6to4 routers are replaced by 6rd routers and the relay router by a BR (Border Relay) router that is accessible by the IPv4 address anycast 10.1.1.1. Different tunneling techniques can be used such as 6to4 [9] [10], Teredo [11], Broker [12], etc.

2.3 Translation

This method is used to connect two hosts/sites using a different IP version. It is a device residing at the boundary of an IPv4/IPv6 network, allowing communication between IPv4 nodes residing in an IPv4 network and IPv6 nodes residing in an IPv6 network by translating the headers (IPv4 to IPv6 and vice versa) depending on the source and destination [13] as shown in Figure 3 below. Here are a few translation techniques.

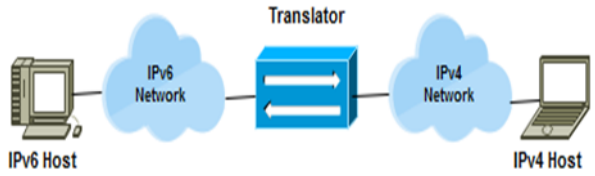

Fig. 3 IPv4/IPv6 Translator.

SIIT

SIIT (Stateless IP/ICMP Translator) [14] is a transition mechanism that uses a bidirectional translation algorithm to convert an incoming IPv4 header into an IPv6 header and an output IPv6 header into an IPv4 header. Translation also occurs between ICMPv6 and ICMPv4 messages. The translation mechanism doesn't affect the checksum values of the headers but ignores many IPv4 extension headers and options, resulting in loss of header information.

NAT-PT

NAT-PT (Network Address Translation-Protocol Translation) [15] is another translation mechanism that allows communication between IPv6 and IPv4 nodes. NAT-PT globally still has a range of routable IPv4 addresses and assigns IPv4 addresses to IPv6 nodes and vice versa. This is similar to the traditional NAT IPv4. NAT-PT can be combined with a DNS-PT. DNS-PT offers the automatic resolution of IPv4 names in IPv6 and vice versa.

TRT

The TRT mechanism (Transport Relay Translator) [16] operates on the transport layer of the TCP/IP model. It allows IPv6 hosts to exchange TCP traffic with IPv4 hosts by translating TCP over IPv6 to TCP over IPv4 and vice versa. The TRT mechanism operates the same way for UDP traffic. The TRT system can be located on a dual stack host or a router. Different translation techniques can be used such as NAT64 [17]/DNS64 [18], BIS [19], BIA [20], etc.

3. Overview of the LISP protocol

LISP (Locator/Identifier Separation Protocol) [21] is a protocol that uses a new approach for IP addressing. This is the separation of the components of the identification and location of IP addresses; this is not like the current architecture where the unique IP address expresses both functions: its identity and the way it is connected to the network. Indeed, LISP uses two namespaces:

- EIDs (Endpoint Identifiers), assigned to the end hosts (the machines)
- And RLOCs (Routing locators), mainly the routers that constitute the global routing system

3.1 LISP architecture and devices

Figure 4 below represents the LISP architecture. Three essential components exist in a LISP environment: LISP sites (EID namespace), non-LISP sites (namespace RLOC), and LISP mapping service (LISP infrastructure) [22].

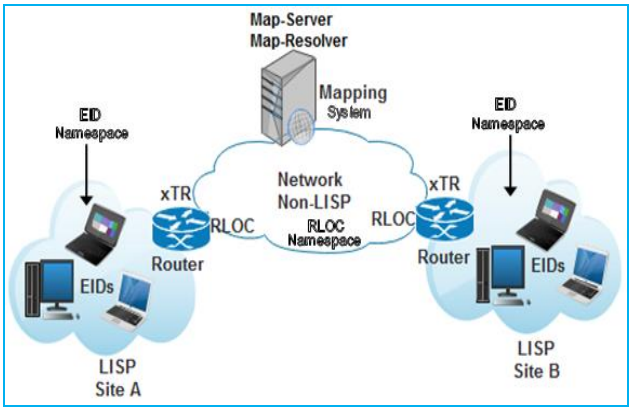

Fig. 4 LISP Architecture.

The LISP EID namespace represents the end sites of customers such as they are defined today. The only difference resides in the fact IP addresses used in these LISP sites are not advertised in the non-LISP, Internet (namespace RLOC). The LISP functionality of the final customer is exclusively deployed on the CE (Customers Edge) routers operating with LISP as ITR (Ingress Tunnel Router) and ETR (Egress Tunnel Router) devices. The ITR and ETR are abbreviated xTR in the figure.
To implement LISP with support for mapping services and Internet interworking, you may need to deploy additional LISP infrastructure components such as Map Server (MS), Map Resolver (MR), Proxy Ingress Tunnel Router (PITH), and Proxy Egress Tunnel Router (PETR).

Devices of the LISP site

The devices of the LISP site are as follows [21]:

- Ingress Tunnel Router (ITR): an ITR is the entry point of the tunnel. This device is deployed as an edge device of LISP sites. It receives packets from the interfaces in front of the site (internal hosts) and encapsulates them to a remote LISP site or natively to a non-LISP site.
- Egress Tunnel Router (ETR): an ETR is the exit point of the tunnel. This device is deployed as an edge device of LISP sites. It receives the packets

from the kernel-oriented interfaces (the Internet) in which the destination IP address is one of the IPs of an RLOC. Subsequently, it decapsulates and delivers them to local EIDs on the site.

LISP doesn't require either change in the final hosts or change in the infrastructure of existing databases. As a result, CE (Customer Edge) devices can play the functions ITR and ETR. This type of CE device is called the xTR. The LISP specification doesn't require any device to perform both functions (ITR and ETR).
For the two devices, the EID namespace is used inside sites for addresses of the end sites of hosts and routers. EIDs go into DNS records. The EID namespace isn't globally routed in the underlying Internet. The RLOC namespace is used in the kernel (the Internet). RLOCs are used as infrastructure addresses for LISP routers and ISP routers, and they are globally routed in the underlying infrastructure. Hosts don't know RLOCs, and RLOCs don't know hosts.

LISP infrastructure

The LISP infrastructure equipment is as follows:

- **Map Server (MS)** [23] [24]: receives LISP 'Mar-Register' messages from an ETR containing its RLOC and a list of its EID-prefixes. The Map-Server, for its part, records EID-RLOC mappings in the mapping database. Given that before sending a 'Map-Register' message, the ETR and Map-Server must be configured with a shared secret or other relevant authentication information, at the moment of the receiving of the 'Mag-Register' message from an ETR, the Map-Server checks the validity of the 'Map-Register' message and records it. Once the record was done, the Map-Server responds by a 'Map-Notify' notification message to confirm the operation.
- **Map-Resolver (MR)** [24] [25]: accepts requests by ITRs via LISP 'Map-Request' messages and responds by 'Map-Reply' by resolving EID-RLOC mappings by using a mapping database. If an ITR sends a 'Map-Request' request to a Map-Resolver to get back the RLOC from an EID and if the mapping is not found, the Map-Resolver on its side redirects that request to the Map-Server. The latter seeks in its local database corresponding to that EID and responds with 'Map_Reply' if it exists. Otherwise, it responds with Negative_Map_Reply.

Here are the format and the different kinds of messages of the LISP control plan mapping system [26], those essential for the LISP operations. They are:

- MAP-REGISTER: a message sent by an ETR to an MS to record one or several EID mappings to RLOC, including priority and RLOC weight parameters.
- MAP-REQUEST: a message sent by an ITR or relayed by an MS to an ETR to obtain the mapping of a given EID.
- MAP-REPLY: a message sent by an ETR in response to a Map-Request to provide the mapping information (EID/RLOC mapping and the site entry policy for the requested EID).
- ENCAPSULATED-CONTROL-MESSAGE (ECM): is used to encapsulate the control plan message between an xTR and the mapping system. Currently, only the Map-Request can be encapsulated and used to send messages between an ITR and an MR.
- SOLICIT-MAP-REQUEST (SMR): Map-Request message requesting a mapping update to an ITR. It will trigger the ITR's Map-Request to the requester, then a Map-Reply from the requester.

LISP interconnection devices

The LISP interconnection devices are as follows [22]:

- **Proxy ITR (PITR):** used for the interconnection between LISP and non-LISP sites. A PITR behaves as an ITR: it receives traffic from non-LISP sites and encapsulates it to LISP sites.
- **Proxy ETR (PETR):** used for the interconnection between LISP and non-LISP sites. A PETR behaves as an ETR, but it does it for LISP sites that send packets to non-LISP sites. Thus, it allows IPv6 LISP sites with RLOC IPv4 to reach IPv6 LISP sites that only have IPv6 RLOCs.

3.2 Operation principle of the LISP protocol

If a host of a LISP domain (EID Space a.a.a.0/24) wants to communicate with a server from another LISP domain (EID Space b.b.b.0/24), it will prepare its packet and send it by adding the destination EID address to the header. Once the packet has arrived at the ITR (entry point of the tunnel), the ITR for its part will look for the RLOC of the destination on its local cache. If it doesn't find it, it will send a 'Map-Request' message to the Map-Resolver to have the RLOC of the destination. If the RLOC is found, the ITR adds a LISP-specific extra header (Fig. 5 below) to the packet that is transmitted in UDP (port 4341) and whose source addresses and destinations are RLOC addresses of the two routers (ITR and ETR) (doing the two ends of the tunnel). Once the packet has arrived at the ETR

(the exit point of the tunnel), it decapsulates the packet, then transmits it to its destination [21].

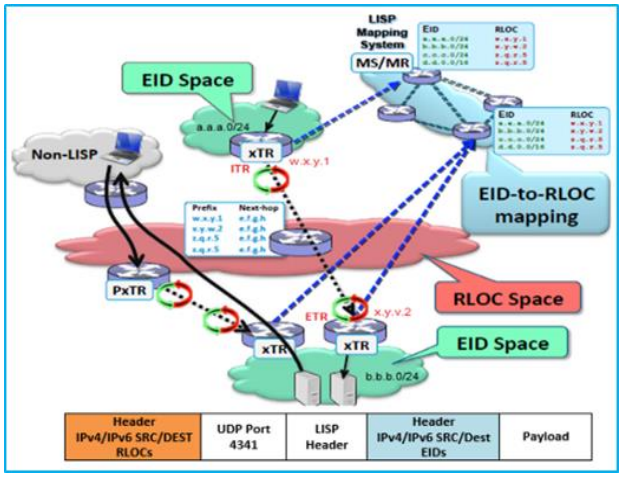

Fig. 5 Operation principle of the LISP protocol.

3.3 Applications and advantages of LISP

- Incrementally available for deployment (it isn't necessary for everyone to switch to LISP).
- Independent of the used IP address family (v4 or v6).
- Improvement of the routing system by reducing the size of the routing table in the DFZ (Default-Free-Zone) area by separating the components of the identification and location of the IP addresses.
- Multi-homing support for sites that are connected to different service providers (in which they can control their own flow policies)
- Operation as a solution of transition to IPv6
- Mobility: the portability of the IP address. Indeed, a station can move from one place to another without modifying its EID. Only the RLOC needs to be updated to MS/MR.
- Network virtualization

4. Related works

There is much research on IPv6, and several of these are about the transition to the IPv6 protocol. Here are some of them based on the comparison of different tunneling methods.

In [27], Aazam et al. compared two tunneling solutions, namely ISATAP and 6to4, on a test network based on two versions of Windows (XP and server 2003). To measure and compare the performance characteristics such as throughput, delay, jitter, and round-trip time (RTT), the authors used two kinds of traffic: UDP and ICMP. The final conclusion showed that the ISATAP tunnel is much more efficient. In addition, Sans and Gamess [28] performed a comparison of the IPv6 protocol performance with four tunneling methods, which are ISATAP, 6to4, 6rd, and Teredo on a test network built on Linux computers and different numbers of Cisco routers. Regarding performance measurements, the authors tested throughput and RTT on two kinds of traffic: UDP and TCP. Consequently, the authors concluded that IPv6 was the best choice, but if native IPv6 can't be used, ISATAP, 6to4, and 6rd are good solutions. Teredo has been presented as the worst solution, but it is the only choice when hosts to connect use private IPv4 addresses, and a NAT server helps them access the Internet.

The author El Khadiri et al., for their parts, have studied the performance of mechanisms of transition from IPv4 to IPv6. First, the authors discussed [29] in detail a comparative study of the mechanisms of transition from IPv4 to IPv6, in which the mechanisms were classified into three families: dual stack, tunneling, and translation, describing for each of them the concerned mechanisms, their operating principles, their fields of use, their advantages, and their disadvantages. In a second phase, they [30] [31] compared the performance of three IPv4/IPv6 transition mechanisms, namely the dual stack, the manual tunnel, and the 6to4 automatic tunnel, with two native IPv4 and IPv6 networks. The performance was measured on two real-time applications (VoIP and Video Conferencing) on five simulation parameters such as delay, delay variation, jitter, MOS, and packet loss. Consequently, the results showed that the dual-stack mechanism gave better performance than the tunneling mechanisms.

In [32], the author Hadiya et al. performed a performance evaluation of two transition mechanisms: configured tunnel and 6to4. The evaluation was performed on two versions of Windows (Windows server 2008 and 2012) using two kinds of traffic: TCP and UDP. The obtained results showed that the 6to4 transition mechanism gave better network performance than the configured tunnel. Another performance comparison was performed by the authors Albkerat and Isaac [33]. They compared three transition mechanisms, namely dual stack, 6to4, and manual tunnel, with two native IPv4 and IPv6 networks. The simulation was performed under OPNET Modeler using four measurement parameters such as throughput, processor (CPU) use, delay of queuing, and TCP delay. The found results showed that the processor use for manual applications and 6to4 is higher than IPv6, IPv4, and dual stack because the transition technology generates more encapsulation and decapsulation efforts. The dual stack found less delay with TCP, but with 6to4 and manual, the delay is longer because the packets are not directly

transferred. In terms of throughput, the results showed that the IPv6 throughput is higher than that of the other four.
Other research work compared the performance of transition mechanisms with native IPv4/IPv6 networks. First, the authors Shah and Parvez [34] compared the performance of the 6in4 transition mechanism with two native IPv4 and IPv6 networks. The study was performed under OPNET Modeler on the basis of three measurement parameters such as throughput, delay, and response time of different applications executed on the Internet, namely the database, the web browsing, video conferencing, voice communications, and remote login. Consequently, 6in4 produces a higher throughput than that of IPv4 and IPv6 networks. In terms of delay, 6in4 is subjected to a higher delay than that of IPv4 and IPv6 networks due to encapsulation and decapsulation that can have a significant effect on real-time applications. In a second phase, the authors compared [35] native IPv6 performance with the dual stack, 6in4, and 6to4. The simulations were performed with the OPNET Modeler tool on the basis of three measurement parameters such as TCP delay, throughput, and response time. Consequently, native IPv6 produced the best results while the second was 6to4.
According to our research, no scientific work has studied the LISP protocol as a solution for transition from IPv4 to IPv6, its deployment, its impact on network performance, on transported applications as well as on IPv6 tunneling, and on native IPv4/IPv6 networks. Only a few people, blogs, etc. specify it can be used in the IPv4/IPv6 transition. That made us want to study it as a solution for transition from IPv4 to IPv6. Our goal was to study its impact in relation to the manual IPv6 tunnel and the two native networks (IPv4 and IPv6). To do this, we carried out an experimental study of scalability under GNS3 by increasing the number of customers communicating VoIP and by varying the different technologies in order to deduce the best solution. Regarding performance measurements, we will use VoIP traffic generated by IP SLA. The evaluation criteria are the delay, jitter, MOS score, and loss rate.

5. Experiment scenarios

5.1 Network Testbed

In order to realize our study, we used the GNS3 tool (Graphical Network Simulator) [36] to create a project consistent with Figure 6 below. On the same network testbed, we have configured the 4 technologies: (IPv4, IPv6, manual IPv6 tunnel and our proposed solution based on the LISP protocol). As background traffic, we used VoIP traffic. To generate the traffic, in order to measure the quality of the link and applications, we used IP SLA [37], the Cisco method that generates test traffic between different network devices such as routers or switches. The advantage of this method is that it is not necessary to install additional equipment, and it doesn't require the development of new software or protocols.
Based on this project, we created 64 different scenarios. For each technology (IPv4, IPv6, manual IPv6 tunnel, and our proposed solution), we increased the number of customers communicating VoIP from 2 to 100 customers. GigabitEthernet technology (1.000 MB) is used in the provider backbone. The link between customer sites and providers boundaries is provided by the FastEthernet technology (10 MB).

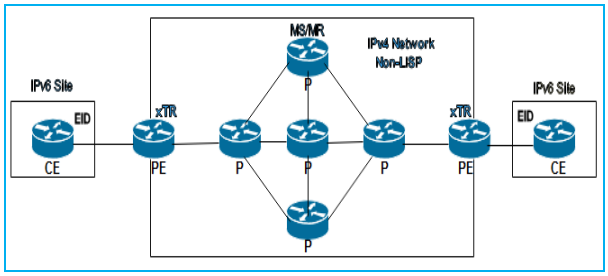

Fig. 6 Network Testbed

5.2 Traffic and measurement parameters

Table 1 describes the parameters of the VoIP traffic generated by the IP SLA tool.

Table 1: VoIP traffic settings

Used traffic	VoIP
Used codec	G729
Number of packets	1000 Packets
Interval between packets	20 Milliseconds

The parameters of performance measurements used in this study are:

- **Delay:** defines the end-to-end transmission delay that is measured between the moment when a packet is created and sent from a source until it is received at its destination
- **Jitter:** jitter is defined as the difference of end-to-end transmission delay between selected packets in the same packet stream, regardless of any lost packets. This parameter is important for a voice application because if the transmission delay varies during a VoIP conversation, the voice

quality will be degraded. The best jitter value is the closest to zero.

- **MOS score:** Meaning Opinion Score. This is an important indicator for assessing the quality of a voice application. It is a scale from 0 to 5 in which 5 indicates excellent quality, and 1 indicates poor quality. This score depends on the used codec; for the G.729 codec (our case), the MOS score is 4.06 (perfect case).
- **Packets loss rate:** this is a number in percent of lost packets related to the sent packets.

6. Obtained results and analysis

6.1 Delay

The results obtained in Figure 7 represent the delay values in milliseconds of the different technologies: IPv4, IPv6, manual tunnel, and our proposed solution based on the LISP protocol.

The obtained results show that when we increase the number of customers communicating VoIP, our proposed solution (based on the LISP protocol) remains the best related to the IPv6 manual tunnel. The difference is justified by the routing process on the tunnel and the encapsulation/decapsulation process of the tunneling mechanism while in LISP, there is no routing process on the tunnel. The comparison between the two protocols (IPv4 and IPv6) shows that the delay values are almost identical for a low or medium VoIP load (up to the 50-customers scenario). For a high VoIP load (after the 50-customers scenario), IPv6 became better than IPv4. This can be justified by the simplicity of the IPv6 header. It contains fewer fields (8 fields instead of 13 in IPv4), which allows for faster processing of data.

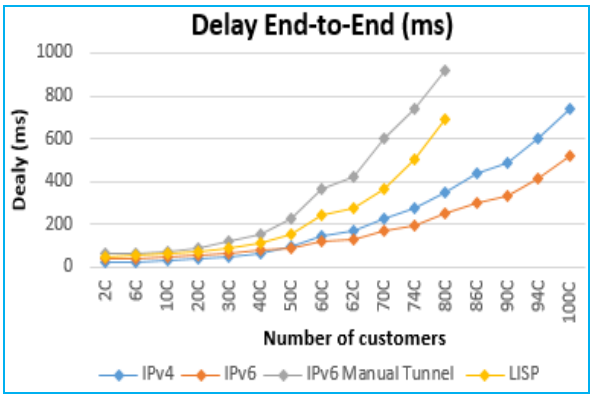

Fig. 7 End-to-end delay.

6.2 Jitter

Figure 8 presents the results of the jitter. According to a first reading, the variation of the jitter is similar to that of the delay but with different values. Indeed, by increasing the VoIP load (the number of customers communicating VoIP), the results show that our proposed solution is better than the manual tunneling mechanisms: it presents lower values in terms of jitter related to the tunneling mechanism. The comparison between IPv4 and IPv6 protocols related to the same criterion indicates that for a high load (after the 50-customers scenario), IPv6 became better than IPv4. This indicates that IPv6 offers a better voice quality related to IPv4 when we increase the VoIP load.

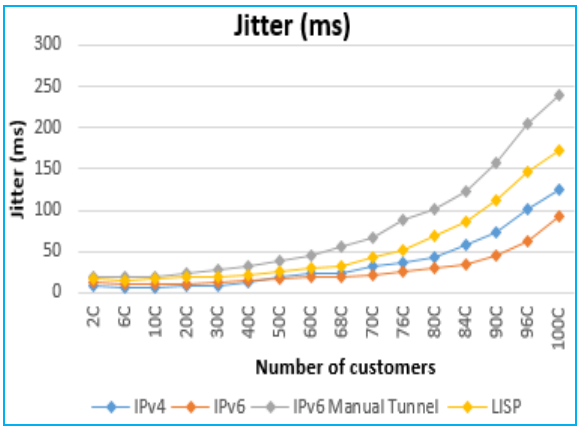

Fig. 8 Jitter.

6.3 Packets loss rate

Figure 9 below illustrates the results of packets loss rate. As shown in this figure, the results reveal that the loss rate of our proposed solution is lower than that of the tunneling mechanism when we increase the VoIP load. The difference is due to processes of encapsulation/decapsulation of IPv6 packets encapsulated in IPv4 packets by the tunneling mechanism and the routing of the tunnel. The comparison, which is between the two protocols, indicates that when we increase the VoIP load (after the 50-customers scenario), IPv6 presents a higher loss rate than that of IPv4, but in the case of a low or medium VoIP load (before the 50-customer scenario), this rate is zero.

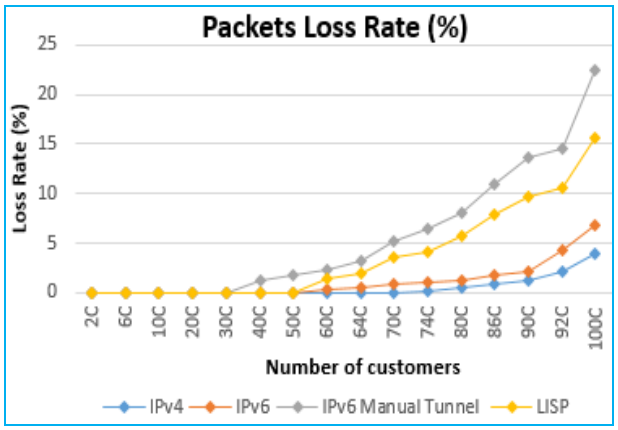

Fig. 9 Packets loss rate.

6.4 MOS score

The results obtained in Figure 10 below represent the values of the MOS score for the four studied technologies. The highest MOS value indicates better performance. As shown in this figure, the results indicate that our proposed solution provides a better voice quality than the manual tunneling mechanism. The comparison between the two protocols related to the same criterion indicates that IPv6 has a better voice quality than IPv4 when we increase the voice load (the number of customers communicating VoIP).

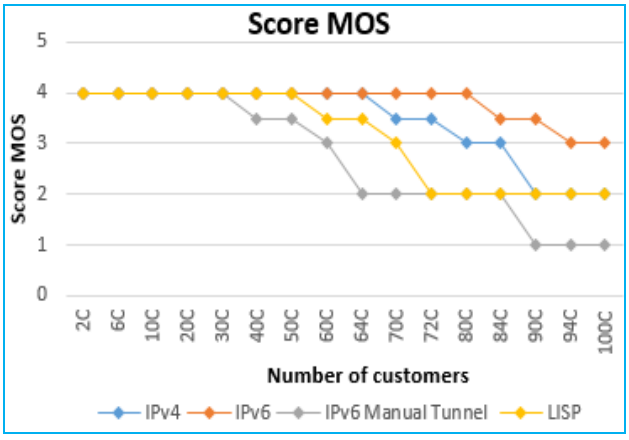

Fig. 10 MOS score.

7. Discussion

In this experimental study performed with GNS3 tool, we studied the scalability of four technologies, namely IPv4, IPv6, IPv6 manual tunnel, and our proposed solution based on the LISP protocol. For each technology, we created 64 scenarios, and we increased the number of customers communicating VoIP from 2 to 100 customers. Regarding performance measurements, we used VoIP traffic generated by IP SLA by using four measurement criteria such as delay, jitter, MOS score, and packets loss rate.

Based on our results, our proposed solution presents better performance than the manual tunneling mechanism with every measurement parameter when we increase the VoIP load in terms of the number of customers communicating VoIP. That is due to the routing process on the tunnel, as well as the process of encapsulation/decapsulation of IPv6 packets in IPv4 packets by the tunneling mechanism while in LISP, there is no routing process on the tunnel.

Related to the performance of IPv4 and IPv6 protocols, the results are almost identical when the VoIP load is low or medium (up to the 50-customers scenario). On the other hand, for a high load (after the 50-customer scenario), the results showed that IPv6 was more efficient than IPv4 with every measurement parameter (except the loss rate). The difference can be justified by the simplicity of the IPv6 header because it contains fewer fields (eight fields instead of thirteen in IPv4). That allows for faster data processing, which will be translated into increased performance.

To judge the scalability of the studied technologies, we must now take into account the tolerable thresholds of the delay (400 ms), the jitter (50 ms), and the loss rate (3%) at the same time.

We observe that:

- The IPv6 manual tunnel, even if it provides a tolerable loss rate in the 62-customers scenario, it reaches 418 ms of delay in the same scenario. Therefore, the manual tunnel can't route the VoIP from this scenario.
- Our proposed solution provides a tolerable delay up to the 70-customers scenario, but with a loss rate of 3.64% in the same scenario making the VoIP useless from this scenario.
- IPv4 reaches 57 ms of jitter in the 84-customers scenario, but with a tolerable loss rate in the same scenario. Therefore, the VoIP becomes unusable from this scenario.
- IPv6 can offer tolerable delay and jitter up to the 92-customers scenario, but the loss rate reaches 4.21% in the same scenario, making the VoIP useless from this scenario.

In summary, figure 11 below presents the degree of scalability of the studied technologies, namely IPv4, IPv6, IPv6 manual tunnel, and our proposed solution in terms of the number of customers communicating VoIP, taking into account the three following parameters: delay, jitter, and loss rate.

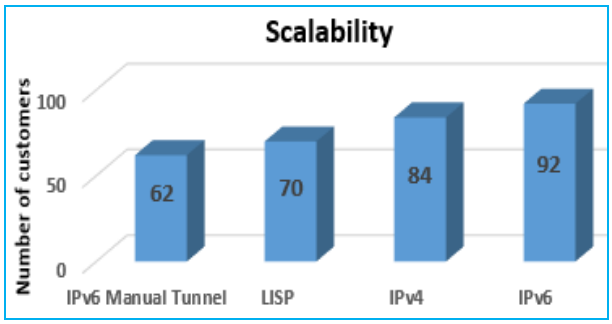

Fig. 11 Scalability.

From these results, it is clear that our proposed solution (based on LISP protocol) is more scalable than the manual tunneling mechanism. For the comparison between the two protocols IPv4 and IPv6 in terms of scalability, IPv6 is more scalable than IPv4.

8. Conclusion and perspective

In this paper, we have proposed a solution for transition from IPv4 to IPv6, based on the LISP protocol. We studied its impact in relation to the manual IPv6 tunnel and the native IPv4/IPv6 networks. We validated this work by an experimental study of the scalability under GNS3 by increasing the voice load in terms of the number of customers communicating VoIP on the basis of four measurement parameters such as the delay, jitter, MOS score, and the packet loss rate.

The results showed that our proposed solution, based on the LISP protocol, is more scalable than the manual tunneling mechanism. Thus, it gave better performance than the tunneling mechanism with every measurement parameter. This difference is justified by the routing process on the tunnel, as well as the encapsulation/decapsulation process of IPv6 packets in IPv4 packets by the tunneling mechanism while in LISP, there is no routing on the tunnel.

Regarding the two protocols (IPv4 and IPv6), the obtained results showed that IPv6 was better and more scalable than IPv4 when we increase the voice load in terms of the number of customers communicating VoIP. That is due to the simplicity of the IPv6 header, which has fewer fields than IPv4. That allows for faster data processing and consequently better performance. Our perspective targets a study of the security in the transition from IPv4 to IPv6.

References

[1] J. Postel, “Internet protocol,” RFC 791, Sep. 1981.
[2] S. Deering and R. Hinden, “Internet protocol, version 6 (IPv6) specification,” RFC 8200, 2017.
[3] P. Wu, Y. Cui, J. Wu, J. Liu, and C. Metz, “Transition from IPv4 to IPv6: A state-of-the-art survey,” IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1407–1424, 2013.
[4] M. Y. Arafat, F. Ahmed, and M. A. Sobhan, “On the Migration of a Large Scale Network from IPv4 to IPv6 Environment,” Int. J. Comput. Netw. Commun., vol. 6, no. 2, p. 111, 2014.
[5] Y. Wu and X. Zhou, “Research on the IPv6 performance analysis based on dual-protocol stack and tunnel transition,” in Computer Science & Education (ICCSE), 2011 6th International Conference on, 2011, pp. 1091–1093.
[6] Interface and Hardware Component Configuration Guide, Cisco IOS XE Release 3S. (2014). 1st ed. [ebook] San Jose: Cisco Systems, Inc., pp.18-26. Available at: http://www.cisco.com c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book.pdf [Accessed 10 May 2014]. .
[7] M. Talwar and D. Thaler, “Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) draft-ietf-ngtrans-isatap-24,” Jan. 2005.
[8] F. Templin, T. Gleeson, M. Talwar, and D. Thaler, “Intra-Site Automatic Tunnel Addressing Protocol (ISATAP),” RFC 5214, 2008.
[9] E. Nordmark and R. Gilligan, “Basic transition mechanisms for IPv6 hosts and routers,” RFC 4213, 2005.
[10] B. Carpenter and K. Moore, “Connection of IPv6 Domains via IPv4 Clouds,” RFC 3056, Feb. 2001.
[11] C. Huitema, “Tunneling IPv6 over UDP through NATs (Teredo), draft-huitema-v6ops-teredo-05,” Apr. 2005.
[12] A. Durand, P. Fasano, and D. Lento, “IPv6 Tunnel Broker,” RFC 3053, Jan. 2001.
[13] N. M. Ahmad and A. H. Yaacob, “IPSec over heterogeneous IPv4 and IPv6 Networks: Issues and implementation,” Int. J. Comput. Netw. Commun., vol. 4, no. 5, p. 57, 2012.
[14] E. Nordmark, “Stateless ip/icmp translation algorithm (SIIT),” RFC 2765, Feb. 2000.
[15] G. Tsirtsis and P. Srisuresh, “Network Address Translation - Protocol Translation (NAT-PT),” RFC 2766, Feb. 2000.
[16] J. Hagino and K. Yamamoto, “An IPv6-to-IPv4 transport relay translator,” RFC 3142, Jun. 2001.
[17] M. Bagnulo, P. Matthews, and I. van Beijnum, “Stateful NAT64: Network address and protocol translation from IPv6 clients to IPv4 servers,” RFC 6146, 2011.
[18] M. Bagnulo, A. Sullivan, P. Matthews, and I. Van Beijnum, “DNS64: DNS extensions for network address translation from IPv6 clients to IPv4 servers,” RFC 6147, 2011.
[19] K. Tsuchiya, H. Higuchi, and Y. Atarashi, “DualStack Hosts using the Bump-In-the-Stack Technique (BIS),” RFC 2767, Feb. 2000.
[20] S. Lee, M. K. Shin, Y. J. Kim, E. Nordmark, and A. Durand, “Dual stack hosts using" bump-in-the-API"(BIA),” RFC 3338, Oct. 2002.
[21] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, “The locator/ID separation protocol (LISP),” 2013.
[22] M. Hoefling, M. Menth, and M. Hartmann, “A survey of mapping systems for locator/identifier split internet routing,” IEEE Commun. Surv. Tutor., vol. 15, no. 4, pp. 1842–1858, 2013.
[23] M. Aiash, “A novel security protocol for resolving addresses in the location/ID split architecture,” in

International Conference on Network and System Security, 2013, pp. 68–79.
[24] A. Ksentini, T. Taleb, and F. Messaoudi, “A LISP-based implementation of follow me cloud,” IEEE Access, vol. 2, pp. 1340–1347, 2014.
[25] D. Saucez, L. Iannone, O. Bonaventure, and D. Farinacci, “Designing a deployable internet: The locator/identifier separation protocol,” IEEE Internet Comput., no. 6, pp. 14–21, 2012.
[26] D. P. Chi, S. Seed, G. Pujolle, P. Raad, and P. Gallard, “An open control-plane implementation for LISP networks,” in Network Infrastructure and Digital Content (IC-NIDC), 2012 3rd IEEE International Conference on, 2012, pp. 266–270.
[27] M. Aazam, A. M. Syed, S. A. H. Shah, I. Khan, and M. Alam, “Evaluation of 6to4 and ISATAP on a Test LAN,” in 2011 IEEE Symposium on Computers & Informatics, 2011, pp. 46–50.
[28] F. Sans and E. Gamess, “Analytical performance evaluation of native IPv6 and several tunneling technics using benchmarking tools,” in Computing Conference (CLEI), 2013 XXXIX Latin American, 2013, pp. 1–9.
[29] K. EL KHADIRI and O. LABOUIDYA, “Etude comparative des mécanismes de transition de l’IPv4 à l’IPv6,” Revue Méditerranéenne des Télécommunications, vol. 7, no. 1, 2017.
[30] K. EL KHADIRI, O. LABOUIDYA, N. ELKAMOUN, and R. HILAL, “Performance Analysis of Video Conferencing over Various IPv4/IPv6 Transition Mechanisms,” IJCSNS, vol. 18, no. 7, pp. 83–88, 2018.
[31] K. EL KHADIRI, O. LABOUIDYA, N. ELKAMOUN, and R. HILAL, “Performance Evaluation of IPv4/IPv6 Transition Mechanisms for Real-Time Applications using OPNET Modeler,” International Journal of Advanced Computer Science and Applications, vol. 9, no. 4, 2018.
[32] D. Hadiya, R. Save, and G. Geetu, “Network Performance Evaluation of 6to4 and Configured Tunnel Transition Mechanisms: An Empirical Test-Bed Analysis,” in 2013 6th International Conference on Emerging Trends in Engineering and Technology, Nagpur, India, 2013, pp. 56–60.
[33] A. Albkerat and B. Issac, “Analysis of ipv6 transition technologies,” ArXiv Prepr. ArXiv14102013, 2014.
[34] J. L. Shah and J. Parvez, “Performance evaluation of applications in manual 6in4 tunneling and native IPv6/IPv4 environments,” in Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on, 2014, pp. 782–786.
[35] J. L. Shah and J. Parvez, “An examination of next generation IP migration techniques: Constraints and evaluation,” in Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on, 2014, pp. 776–781.
[36] J. C. Neumann, The Book of GNS3: Build Virtual Network Labs Using Cisco, Juniper, and More. No Starch Press, 2015.
[37] D. Teare, B. Vachon, and R. Graziani, Implementing Cisco IP routing (ROUTE) foundation learning guide:(CCNP ROUTE 300-101). Cisco Press, 2014.

Khalid EL KHADIRI received the Master degrees, Network and telecommunication, from Faculty of sciences El Jadida in 2014. Professor of secondary education qualifying in public education, Actually a Ph.D Student on STIC Laboratory on Faculty Of sciences El Jadida, Network and Telecommunications team. His research interest are: IPv6, NGN, MPLS, Mobile learning, QoS of networks, wireless networks, networks and telecommunications.

Najib EL KAMOUN Ph.D, professor higher education degree at Faculty of sciences El Jadida.in the dept. of physics. Researcher member on STIC laboratory, header of Network and Telecommunications team. His research interest includes, NGN, MPLS, Networks, QoS on mobile networks, wireless networks, networks and telecommunications.

Ouidad LABOUIDYA has a Ph.D. in Information, Technologies and Communication. She is now Assistant Professor at the Faculty of Sciences, UCD El Jadida - Morocco. She is responsible for the research team "TICEF" in ICT laboratory and member of the ADMEE-Europe. Her research focuses on evaluation in higher education, self-training and ICT for education.

Rachid HILAL Ph.D, professor higher education degree at Chouaib Doukkali University. Actually a vice president of the Chouaib Doukkali University. Researcher member on STIC laboratory. His research interest includes, Hyperfrequency, amplifiers Antennas,