IPv6: Comparison of mobile environments in academic networks

Carlos Taffernaberry[1], Sebastián Tobar[1], Gustavo Mercado[1], Joel Noguera[1], Cristian Perez Monte[1], Raúl Moralejo[1], Santiago Perez[1]

[1] Grupo GridTICs – Departamento de Electrónica – Universidad Tecnológica Nacional - Facultad Regional Mendoza – Rodríguez 273, Ciudad Mendoza
CP (M5502AJE) República Argentina
{carlos.taffernaberry, sebastian.tobar, gustavo.mercado, joel.noguera, cristian.perez, raul.moralejo, santiago.perez}@gridtics.frm.utn.edu.ar

Abstract. The use of academic networks is generating important changes in research and education fields, providing new tools that bring us closer to other scientific and educational worldwide communities. Thus, investigations are carried out between work teams that are geographically distant. This allows better interaction and support between researchers, advanced scientific research collaboration, etc. In this paper, a comparison between two different IP mobility alternatives available in version 6 is presented. Standards evaluated are Mobility IPv6 (MIPv6) and Proxy Mobility IPv6 (PMIPv6). A comparison of performance, advantages, disadvantages, configuration, ease of handling and installation is made in the first instance. Afterwards the behavior of MIPv6 and PMIPv6 handover is evaluated for traditional and real time applications. Finally, comparisons and a conclusion are made.

Keywords: Mobile IP, IPv6, MIPv6, PMIPv6

1 Introducción

By the end of the twentieth century internet use became massive, which introduced changes in all areas of our lives. However, soon after its incorporation into everyday life, an emptiness and dissatisfaction in the scientific, academic and research community was felt. Advances in technology infrastructure were developed on academic networks to reinstall the hopes in these communities. That allowed the exclusive use of tools and applications to improve and increase their activities.

Nowadays these networks are known as advanced academic and research networks. Its main feature is to allow geographically distant research and scholars communities working together through collaborative mechanisms, sharing information and resources over a series of high speed interconnected networks.

With the emergence of mobile devices using different wireless technologies, the model of Internet connectivity changed. Currently when a user travels between

different networks (roaming), each of the new networks visited provides a different IP address, so the user cannot keep the session open for an application during his displacement. The goal of Mobile IP [1] is assign to the mobile user an unique address, regardless of the network where it is, allowing him to keep, for example, the session for applications.

After 30 years, the version 4 of the Internet Protocol (IP) can no longer provide scalability by the gradual depletion of available IP addresses, due to the current growth rate of nodes connected to the network [2].

The lifetime of IPv4 has been extended for a few years thanks to techniques such as address reuse with translation (NAT) [3] and classless routing (CIDR) [3]; IPv6 in this period grew and finally established as the successor to IPv4.

Some features of IPv6 [4] are: expanded addressing capability, quality of service (QoS), autoconfiguration (Neighbor Discovery), end to end connectivity, simplified header format and mobility support.

The conjunction between academic networks, mobility and IPv6 is a powerful tool to achieve the objective of start up collaborative research.

There are worldwide educational networks using IPv6, such as Internet 2 [5], GÉANT2 [6], Clara [7]. In our country there is a network called Innova Red [8], which provides national institutions access to global advanced networks through the Clara network.

Within the UTN the RUT2 [9] (Network Technology University) interconnect all the the Regional Faculties.

The ACyTNet initiative (Academic Network of Scientific and Technological Mendoza) is a network that joins, at this moment, CONICET Mendoza, INA National Institute for Water Resources and UTN GridTICS FRM pretending to be the Advanced Academic Network of metropolitan institutions in Mendoza.

1.1 IP Mobility

Network Mobility is a concept by whom a node is able to move from one network to another without losing it's current connection and this change should be transparent to the user.

The main entities involved in a mobile architecture [1] are:

- Mobile Node (MN): Device that moves frequently between different networks.
- Home Agent (HA): This device maintains information about the MN current location. It's a router, generally, located in the home network of the MN.
- Foreign Agent (FA): Device located in the foreign network that stores information about MNs. It coordinates, using messages, with the HA to provide mobility.
- Correspondent Node (CN): Any device, mobile or not, that communicates with the MN.

Additionally, IPv4 and IPv6 Mobility implementations have the following differences:

- IPv6 mobility does not need FA nodes. Self-address configuration and neighbor discovery are used, both unique features of IPv6 protocol.
- Mobility packets in IPv4 that travels from the HA to the MN must be encapsulated. This feature is not required in IPv6.
- IPv6 Mobility avoids triangular routing.

The rest of the paper is organized as follow: two approaches to mobility, with a brief explanation of them, are introduced in the section 2. The test environment used to conduct the experiment is described in the section 3. The way the experiment was conducted and results is found in Section 4. Finally, in the last Section are the conclusions reached.

2 Covered Approaches

There are two approaches related to mobile IPv6 networks management.

2.1 Traditional

The IPv6 mobility is managed by the participating nodes, by exchanging mobility messages between the MN and the HA. Therefore the kernel of both nodes must be prepared for it. The procedure is explained as follows:
A MN can have two addresses, a local HoA (Home-of-Address), and, in case of being in a foreign network, a dynamic CoA (Care-of-Address). If the MN is on its local network, packets will continue using conventional routing rules with its HoA. If it is in a foreign network, and a CN wish to communicate with it, it will initially use the HoA. These packets are intercepted by the HA, which manages a table with information linking HoAs with CoAs addresses, as well as tunnels from the local network of the HoAs to the foreign networks of the CoAs. The HA redirects these packets destined to the MN through a tunnel, carrying a new IP header with the CoA address, that permits encapsulate the original header with the HoA address. At the end of the tunnel, packets are decapsulated by the MN removing the IP header added before.

2.2 Mobility managed by the Network

This approach, known as NETLMM (Network-based Localized Mobility Management) [10], makes possible to implement mobility in IPv6 nodes without involve the MN and CN nodes in the exchanging mobility messages. It is an advantage over traditional mobility because does not require changes in the software behavior of these nodes. This is the case of the PMIPv6 protocol [11]. The main entities in the PMIPv6-NETLMM infrastructure are:

- Local Mobility Anchor (LMA): Is a HA with proxy properties. It's the responsible for the MN to be accessible. Topologically is the origin point (anchor point) for the origin network prefixes (home network prefix(s)) of the MN.
- Mobile Access Gateway (MAG): Usually is a router that manages the mobility in behalf of the MN, located in the local network of the MN. It is responsible of detecting the movements of the MN to and from the local network. It is involved in the MN registration in the LMA.

There may be multiple LMA in a Proxy Mobile domain, each giving service to different groups of MN.
From the perspective of each MN the entire PMIP domain seems like a single link. The network ensures that the MN does not detect any change with respect to the network layer, even if it changes its attachment point to the network.

3 Implementation

After a comparison between different free operating systems, GNU/Linux Distribution Fedora Core 14 was selected, mainly because the kernel in this distribution had the module MIP6 mobility [12] compiled. Also, it was necessary to run a MIP service in user mode to complete the IPv6 mobility support.

There are several alternatives for MIPv6 service implementations. UMIP [13] was selected due to a wide support and frequent improvement to his code.

For PMIPv6 service currently exists three options: OPMIP [14], OAI PMIPv6 [15] and UMIP [16] plus a patch to support PMIPv6. The first implementation is not very mature, has only two years of work. The second, OAI PMIPv6 is implemented over UMIP, and has specific hardware requirements that hinder and limit its implementation. That is why we decided to install UMIP and apply the necessary patches to give Proxy Mobile support.

3.1 MIPv6 deployment

In the ACyTNet network environment, a test bed was set up with five nodes, as shown in Figure 1. According to the detailed in Section 3, the GNU/Linux Distribution Fedora Core 14 Operating system was installed on all nodes.

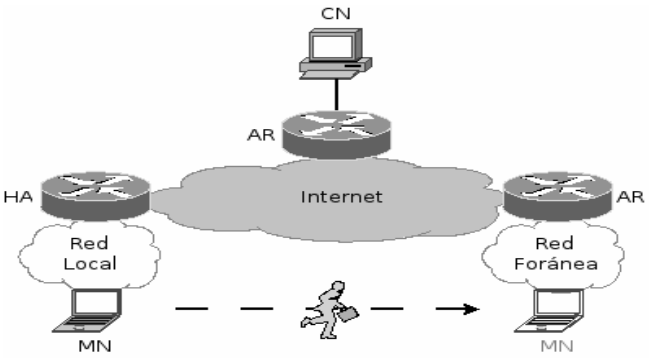

Fig. 1. Mipv6 scenario.

The UMIP service was installed in the MN and HA nodes, running in user space. This service was used to manage the tunnels and links of each node. The MN and HA kernels were responsible for handling IPv6 mobility specific extension headers. The UMIP service makes extensive use of XFRM [17] framework, manipulating the IPv6 headers.
Finally, IPSec [18] support was added, modifying the configuration, to protect the data flow. The MN and HA node settings were modified and also security associations were created in both operating systems.

3.2 PMIPv6 deployment

The test bed was reconfigured to deploy a PMIPv6 domain, as shown in Figure 2.
Due to PMIPv6 characteristics, the MN and CN operating systems version were not relevant. The chosen implementation, PMIPv6 UMIP version 0.4, needed a software patch to acquire PMIPv6 functionalities.
The node previously used as HA, assumed the LMA role, while the other routers assumed MAGs function. The MN and CN remained unchanged.

As well as in MIPv6, there was a single executable which meets PMIPv6 different roles; depending on the configuration file associated.

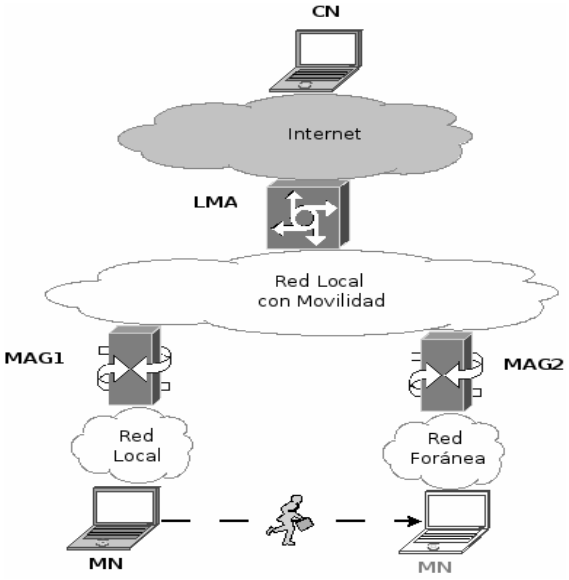

Fig. 2. Test environment used by PMIPv6

The LMA configuration for PMIPv6 was the same used for the MIPv6 HA. As said, in PMIPv6 the LMA is the MN topological anchor point.

4 Experimentation y Results

The test consisted of running applications on the MN node. Afterwards, while the applications were still running, the MN was moved from the home network to a foreign network. The MN handover was triggered by this change in the anchor point.
The applications under test were ping, FTP, SSH and real time traffic.
A topology without mobility was used as a reference scenario to compare the measurements.

4.1 Scenario without Mobility

The reference scenario was assembled at the GridTICs laboratory, in the UTN FRM, as part of the ACyTNet. The network architecture and addressing used is observed in Figure 3.

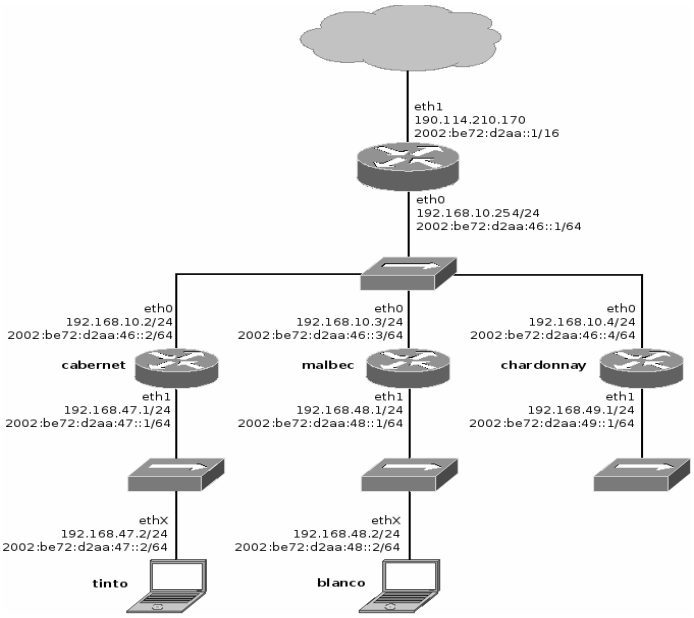

Fig. 3. Reference scenario

About MIPv6, as long as the MN was located at the home network, there was not any topological difference between the reference and the MIPv6 scenario. Once the MN was in a foreign network, a tunnel had to be created between the MN and the HA, adding one hop to the topology

The topology remained unmodified either when the MN was attached to the home or foreign network, when PMIPv6 was used. Also, there always existed a tunnel in this scenario.

4.2 Results

Basic functionality:

Both mobile protocols (MIPv6 and PMIPv6) worked as expected. During the handover, the MN conserved his IP address and established sessions.

Channel capacity:

A comparative of the bandwidth available for data transmission between MIPv6, PMIPv6 and reference scenario was carried out. This test, the Iperf [19] tool was used. The time configured to be used in the test was 10 seconds, while the number of concurrent clients was 1, 2 and 10 for full duplex communication. A graphic with these results can be seen in Figure 4.

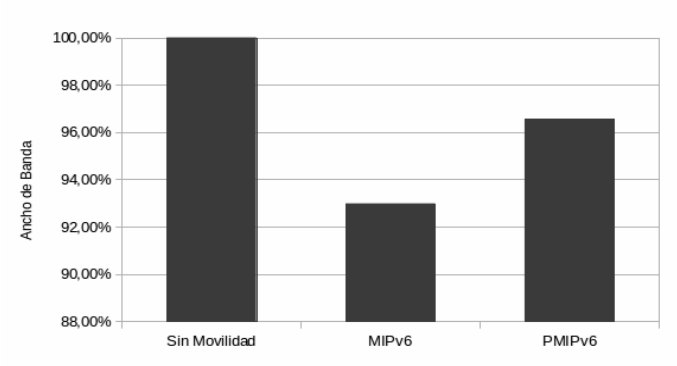

Fig. 4. Bandwidth comparison

RTT analysis. IPSec impact:
The ping tool was used to test the average round trip time between the MN and the CN. The packet size used was 56, 512 and 1024 bytes, along with flooding option (-f).

Obviously, the lowest RTT time was obtained using the reference scenario, without mobility. PMIPv6 took a slightly longer RTT, due to the overhead introduced by the tunnels used. With a considerably longer RTT time, caused by a triangular routing, appears MIPv6. Finally, MIPv6 with IPSec had the worst RTT, which was strongly affected by the processing overhead of the security algorithms. This benchmark can be seen in Figure 5.

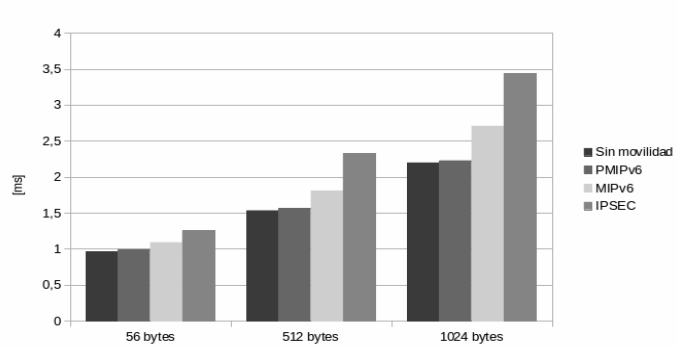

Fig. 5. RTT comparison

Handover Time:

Several considerations must be taken into account, regarding handover time measurements. This time depends on different variables not related to the mobility protocol under test [20][21].

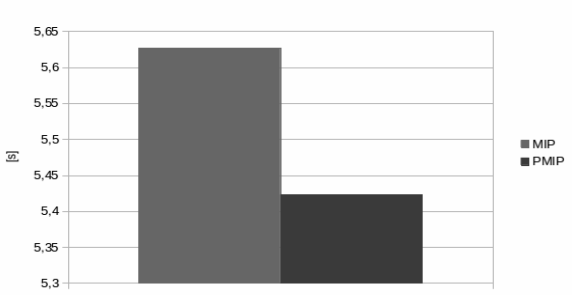

Fig. 6. Handover Comparison

The handover time in PMIPv6 and MIPv6 scenarios was evaluated in this comparison. As can be seen in Figure 6, this time is shorter for PMIPv6. This situation is related to the signaling driven by the LMA and MAGs instead of the CN or MN nodes.

5 Conclustions

It has been shown that the implementation of both protocols behaved properly in terms of functionality. Also, PMIPv6 allowed the use as MN of any IPv6 node without mobility extensions. This feature permitted a great diversity of mobile devices acting as MN; especially those that could not modify its operating system, such as smart phones, tablets, notebooks with proprietary software, etc.

The performance of MIPv6 was better than PMIPv6 while the MN was in the HN. It was because the data was always exchanged in “IPv6 in IPv6” tunnels for PMIPv6, causing overhead. If the MN was in a foreign network the performance was slightly higher for PMIPv6 protocol.

The security feature could not be compared because the PMIPv6 implementation did not have support to send encrypted signaling or data.

Handover measurements showed a shorter time for the PMIPv6 protocol when the MN moved from one network to another. In both protocols, the TCP session was not lost.

Finally, it's clear that both protocols were designed for distinct goals. MIPv6 ensures global reachability, sacrificing speed and requiring a modified MN. On the other hand, PMIPv6 offers a higher handover speed, limiting the MN mobility only to networks with such service.

References

1. James Solomon “Mobile IP: The Internet Unplugged” 1st. Edition. ISBN: 978-0138562465 (1997)
2. Informe LACNIC, “Distribuciones/Asignaciones IPv4, espacio disponible y pronósticos “ - http://www.lacnic.net/web/lacnic/reporte-direcciones-ipv4
3. Kevin Fall - Richard Stevens “TCP/IP Illustrated, Volume 1: The Protocols” 2nd. Edition. ISBN 978-0321336316 (2011)
4. Peter Loshin “IPv6: Theory, Protocol and Practice”, Morgan Kaufmann, Segunda Edición. ISBN 1-55860-810-9 (2004)
5. The Internet2 Net – http://www.internet2.edu
6. The high-bandwidth, academic Internet serving Europe’s research and education community - http://www.geant2.net
7. Cooperación Latinoamericana de Redes Avanzadas – http://www.redclara.net
8. Red Nacional de Investigación y Educacion Argentina – http://www.innova-red.net
9. Red Universitaria Tecnológica (RUT2) - http://www.utn.edu.ar/virtual/rut/index.html
10. RFC 4831 - J. Kempf, Ed. ”Goals for Network-Based Localized Mobility Management (NETLMM)”, August 2008 - http://tools.ietf.org/html/rfc4831
11. RFC 5213 - S. Gundavelli, Ed.” Proxy Mobile IPv6”, August 2008 - http://tools.ietf.org/html/rfc5213
12. Fedora Project: la evolución del código abierto. http://es.redhat.com/resourcelibrary/articles/the-fedora-project-open-source-evolved
13. “Umip Source Code” - http://git.umip.org/
14. OPMIP - http://helios.av.it.pt/projects/opmip
15. OAI - http://www.openairinterface.org/
16. "How to use our set of PMIPv6 patches" - http://www.umip.org/contrib/umip-pmipv6.html#config
17. “Framework XFRM” - http://git.kernel.org/cgit/linux/kernel/git/shemminger/iproute2.git/
18. RFC 4301 - S. Kent, K. Seo - “Security Architecture for the Internet Protocol”, Dicember 2005 - http://tools.ietf.org/html/rfc4301
19. Iperf - https://iperf.fr/
20. RFC 4861 - T. Narten, E. Nordmark, W. Simpson, H. Soliman, “Neighbor Discovery for IP version 6 (IPv6)” September 2007 - http://tools.ietf.org/html/rfc4861
21. DUNMORE, Martin; PAGTZIS, Theo; EDWARDS, Chris. Mobile IPv6 handovers: performance analysis and evaluation. 6NET Consortium, Deliverable D, 2005, vol. 4.