Impacts of mobility on wireless access to IPv6 networks

Christian Lazo R., Roland Glöckler
Universidad Austral de Chile, Instituto de Informática, General Lagos 2086, Casilla 567,Valdivia, Chile
{clazo,rolandglockler}@uach.cl

Fecha de recepción: 30-05-06 Fecha de selección: 30-10-06 Fecha de aceptación: 30-08-06

ABSTRACT

The project "AIRE 6 - Wireless Access to IPv6 Networks" generated a hot spot of wireless Internet access using Wi-Fi (IEEE 802.11 b/g) in a native IPv6 environment. The setup of the project enables end-to-end connectivity using global public addresses. By incorporating mobility mechanisms of Mobile IPv6 (MIPv6), it allows scenarios always-on with mobility functions. Client connections are managed with efficient AAA (Authentication, Authorization and Accounting) mechanisms that had to be developed for the project due to the absence of adequate solutions. Within the project administrable APs were enhanced with native IPv6 support. Among the results of the project is an analysis of the impacts on delay and data rates caused by client mobility in best effort environments. The results obtained will help to improve technical conditions for the use of mobile Internet with the full potential of IPv6.

KEYWORDS

IPv6, AAA, WiFi, Mobility, Route Optimization, Mipv6

RESUMEN

El proyecto "AIRE 6 – gíreles Access to IPv6 Networks" generó una serie de hot spots utilizando tecnología WiFi (IEEE 802.11b/g) en un ambiente IPv6 nativo. LA configuración del proyecto habilita la conectividad extremo a extremo utilizando direccionamiento público global. Con la incorporación de mecanismos de movilidad del IP móvil versión 6 (MIPv6), se pueden tener escenarios "always-on" con funciones de movilidad. Las conexiones de los clientes se manejan

con mecanismos eficientes de AAA (Authentication, Authorization and Accounting) que han sido desarrollados en el marco del proyecto debido a la ausencia de soluciones adecuadas. Dentro del proyecto, se mejoraron APs administrables con soporte IPv6 nativo. Entre los resultados expuestos en este trabajo, se encuentran el análisis del impacto en el retardo y las tasas de transmisión causados por la movilidad del cliente en ambientes de mejor esfuerzo (best effort).

PALABRAS CLAVE

MIPv6, AAA, WiFi, Movilidad, optimización de rutas.

Clasificación Colciencias: A

1. INTRODUCTION

In these days of ubiquitous wireless network access, various wireless technologies have reached great popularity, some even in spite of their maturity problems. The availability of this kind of technology is a great help in spreading Internet even more.

Setting up an access point (AP) in order to provide wireless network access to multiple clients is very easy and cheap nowadays. However, providing a secure access with valueadding features and controlling a group of access points, requires much more effort. Service providers create ever adapting business models around these technologies, and one of them for the use in public spaces are the so-called hot spots, which are zones covered by wireless access using a group of APs within a common administrative domain. Many of the techniques developed for those also have found their application in corporational or private networks, such as the AAA (Authentication, Authorization and Accounting) mechanisms to protect network resources and manage client connections.

Every innovation comes hand in hand with new challenges. Apart from the general limitations of any traffic concentrator, there are requirements from services, applications and end users that can hardly be fulfilled with the commonly used communication protocols.

First of all, there are many new types of applications such as Voice over IP (VoIP) or file transfer functioning in peer-to-peer (P2P) manner, requiring end-to-end (E2E) connectivity. It is common knowledge that IP addresses in the Internet Protocol version 4 (IPv4) are scarce and generally for public services dynamic addressing schemes or private addressing in combination with Network Address Translation (NAT) are used. The mixture of those methods with other features such as security leads to a lot of problems because of the multitude and complexity of protocols and systems that are needed to circumvent the limitations.

The use of wireless technologies creates the freedom to move around. If a client wants to maintain connectivity beyond the cover area of an individual access point, handover and mobility methods are needed. In order to maintain open IP based communication sessions, this means to maintain the communication 4-tuple of IP addresses and ports of the end points. In "Always-on" scenarios there shall be no interruption of service and everything has to happen transparently to the end user. There exist mobility extensions for IPv4, but they are not very efficient.

As can be seen, in such scenarios there is an agglomeration of difficulties mainly based on the shortcomings of IPv4. Examining the capabilities of IPv6 [1], the designated successor of IPv4, substantial progress in this area can be seen. Addresses are plenty in IPv6 and there is no need of dynamic assignment or private addressing. This way, everybody receives a globally unique address and features such as E2E connectivity are no problem. Mobility in IPv6 [2] is more efficient and less complex than in IPv4. In combination with the addressing advantage, "always-on" features can easily be provided.

The goal of the project "AIRE 6" [3] was to generate hot spots of wireless Internet access using Wi-Fi (IEEE 802.11 b/g) in a native IPv6 environment, i.e., no IPv4 address is used in the testbed. One of the paradigms was to use free software wherever possible. The setup of the project enables end-to-end connectivity using global public addresses. By incorporating mobility mechanisms of Mobile IPv6 (MIPv6), it allows scenarios always-on with mobility functions. During the project, an AAA mechanism based on a web portal and packet filtering was developed.

To provide wireless connectivity in an IPv6 only environment is basically no different than in IPv4, since all the wireless functionality resides in layer 2 of the OSI Reference Model, while IP resides in layer 3. However, any management and control of an access point uses upper layer protocols and thus needs IPv6 support. Due to the absence of commercially available APs with IPv6 support, it was also necessary to generate an AP supporting IPv6 management during the project.

2. TESTBED

2.1 Network layout

During the project, a complete native IPv6 network infrastructure was generated offering network access, routing, web, file transfer (FTP), mail, name resolution (DNS) and tunneling services. The also implemented RADIUS server was not used in the final solution. Figure 1 below shows the network layout of the testbed.

Figure 1. Testbed network layout.

2.2 Main network components

The following are the main components of the network:

The *Router Chile-6Bone* provides connectivity for the project networks and all other IPv6 networks in Chile to the IPv6 world. It is an integrated router with IPv6 functionality already incorporated. It provides the network prefix 3FFE:400F:E001::/64 to the network ipv6.cl in which reside the project servers.

The *WiFi access point*s using the wireless technology IEEE 802.11b/g were required to support management functions. Since there were no commercially available IPv6 capable products at the time, the multifunctional Linksys WRT54G was chosen, because it allows installing a Linux-based distribution. This way it gives the opportunity to add and modify modules such as IPv6 support. We chose the distribution OpenWRT for its modularity and flexibility.

The wireless clients may belong to any of the *subnetworks ALFA* (network prefix 3FFE:400F:EEEE:A::/64), *BETA* (network prefix 3FFE:400F:EEEE:B::/64) or *GAMMA* (network prefix 3FFE:400F:EEEE:C::/64).

For common network services, there are IPv6 native *DNS* and *FTP servers*.

The *Router AIRE6* plays a key role in the project networks. It was generated of a standard Linux PC (Fedora Core 2) and assumes various functionalities:

- For all three subnetworks it plays the role of *Home Agent* (HA).
- As a router it advertises the network prefixes, its own address and its capabilities, such as HA.
- For all successfully authenticated users, the *firewall* (packet filter) is opened for navigation. Traffic of other sources is restricted.

The *web portal* in combination with the *user database* manages the firewall.

The *mobile node (MN)* is a client of one of the subnetworks ALFA, BETA or GAMMA and uses the MIPv6 services offered by the HA while residing in other IPv6 networks.

2.3 MIPv6

When an IPv6 node connects to an IPv6 network, it receives a router advertisement (to accelerate the process, it also may request one). The information contained in that message allows the node to autoconfigure [4] a globally valid unicast address.

However, if that node has open connections in which it used a different address, upon changing the address it will lose connectivity in those sessions.

The Mobile IPv6 (MIPv6) protocol offers a mechanism that enables to transparently maintain those sessions and to be reachable for peers using both the current address and the original, so called "home address". This way, a user can move freely from network to network and doesn't have to bother about being reachable or losing connectivity. For the operating system Linux there is an implementation called "Mobile IPv6 for Linux" [5], which was used in the project.

In order to make the concept work, the node that is moving around needs that a router in its "home network", i.e., in the link that it considers its original location, provides it with sort of a proxy support. That router is called "Home Agent" (HA) and it receives all packets destined to the mobile node's (MN) "home address". It forwards them to the current address of the mobile node, the so-called "care-of-address", using a tunnel between the HA and the MN. Packets in backward direction also use the tunnel and they appear to come from the

home address of the MN. If the peer of the communication, the so called "Correspondent Node" (CN), also supports MIPv6, a route optimization can be used to communicate directly bypassing the HA and reducing the delay of the communication. The activation of this direct communication path is realized in parallel to the data communication through a correspondent registration procedure and thus delays in being setup.

The tunnel for indirect delivery has to be created and maintained using bidirectional communication between the HA and MN. The MN tells in a periodic manner in a message called "binding update" to the HA, to which network link it is attached currently. While this is outside the home network, the tunnel between home address and care-of-address has to be maintained active, otherwise it is not needed. The HA notifies in its answer "binding acknowledgement" of the update of its register.

While offering added value of transparent mobility, there is a cost in the delay of realizing the change of link, address auto-configuration, binding update, and tunnel modification. If the route optimization is not used, also each packet transmission has an increased delay due to the indirect delivery through the HA. The route optimization, in contrast, does allow efficient communication by using direct delivery, but needs some time to become effective.

2.4 AAA

In wireless networks, captive portals are the predominant implementation of Network Access Servers. However, at the time those functionalities were needed, there was no captive portal available with IPv6 support, and a simplified alternative solution was developed in the course of the project.

In the implemented solution, a non-captive web portal offers a form to enter username and password of a user. Upon clicking the "submit" button, a PHP script runs the mechanisms necessary to decide if the user will be granted access.

In order to make the decision, first the script controls if all necessary technical parameters are complied (access control). For instance, only clients using IPv6 may be granted access. The authentication is verified by comparing the values entered in the form to the values stored in the user database which contains the information of registered users. In case of successful comparison, the user database might indicate a certain level of access to resources (authorization). In our project networks, there is only one kind of access, navigation to any IPv6 address. In order to avoid duplicate session initiation, a final check verifies that the user has not an open session yet with the same address.

If all steps are passed successfully, the firewall is opened for the IPv6 address of the client and the session parameters are stored in a register. A new web page is loaded to show the user that he is granted access now and to offer him a button for the termination of his session.

If any of the described steps results in a denial of access, the user will be notified in a new web page that he was denied access indicating the reasons. In the case of wrong user cre-

dentials, he will be given the chance to try again.

An open session may be terminated by two ways. If the user clicks on the "logout" button, his session is terminated immediately. If he passes the time limit for his session, he is disconnected automatically. In both cases, the session register and the firewall settings are modified accordingly.

This authentication process is quite similar to the ones used nowadays in commercial hot spots of ISPs all around the world. The big difference is that it works with IPv6 addresses.

3. EXPERIMENTS

The goal of the experiments was to examine the impacts of the mobility mechanisms on the performance of user connections. The setup for the experiments as shown in the chapter 2 contemplated a remote mobile user located in Spain, which resulted in quite a distance and latency to the servers and testbed in Chile. The IPv6 native interconnection uses the advanced academic backbone networks of Chile and Spain. The QoS parameters of the connections were best effort, similar to standard Internet ISP politics, resulting obviously in variations of the measurement results.

All experiments save the last set were realized in two scenarios. The first measurement was taken without mobility mechanisms (indicated in red color in the graphs), the second measurement used mobility mechanisms (indicated in blue color in the graphs). In the last set, a third scenario using route optimization capabilities of MIPv6 was added (indicated in black color in the corresponding graph).

In the scenario without mobility, the autoconfiguration of the IPv6 address was enough to start generating traffic, so everything was automatic and transparent.

Before generating traffic in the mobility scenario, it was necessary to terminate the activation of MIPv6 capabilities, the autoconfiguration of a local address in the MN, its registration as CoA in the HA and the application of the AAA mechanisms of the testbed, since traffic was to be generated via the home network.

In the first series of measurements, the roundtrip time (RTT) of a ping with 256 bytes of payload was taken to a peer host (FTP server 3FFE:400F:E001::D) residing within the home network in Chile. Figure 2 shows the results. The red points correspond to the non-mobility scenario, the blue line to the mobility scenario.

As can be seen, there is only little difference in RTT between the direct delivery and the indirect one using the mobility tunneling via HA. The small delay comes from the encapsulation process necessary for the mobility application in the MN in order to use the tunnel and the stripping of the additional header in the HA.

A traceroute to the router AIRE6 (HA) for both cases leads to a similar result, but illustrates more clearly the path difference. The direct scenario uses 15 hops while the mobility scenario uses only one hop. However, the RTT is almost the same. Figure 3.

The next measurement consisted of an FTP file transfer between MN and the FTP server of the home network. The file size was 5 MB. In the results, shown in figure 4 and 5, the similari-

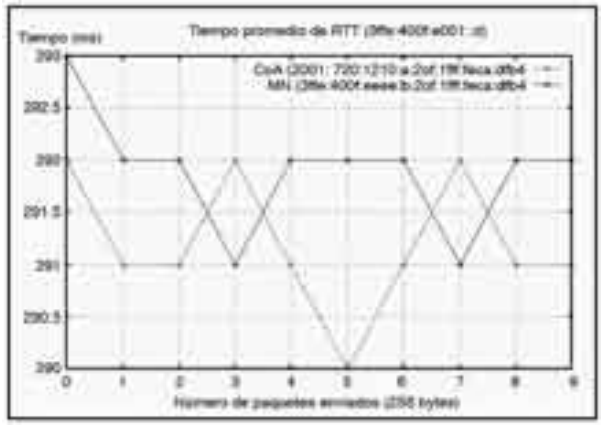

Figure 2. RTT measurements of ping to home network.

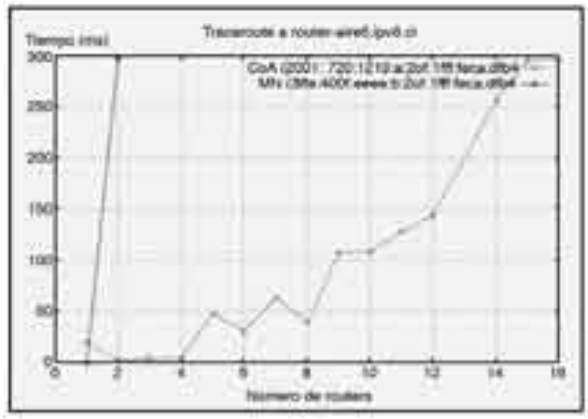

Figure 3. RTT measurements of traceroute to home network.

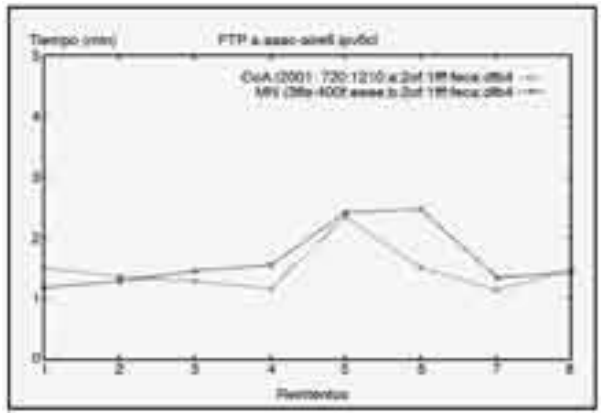

Figure 4. Transfer rate measurements of file transfer from home network.

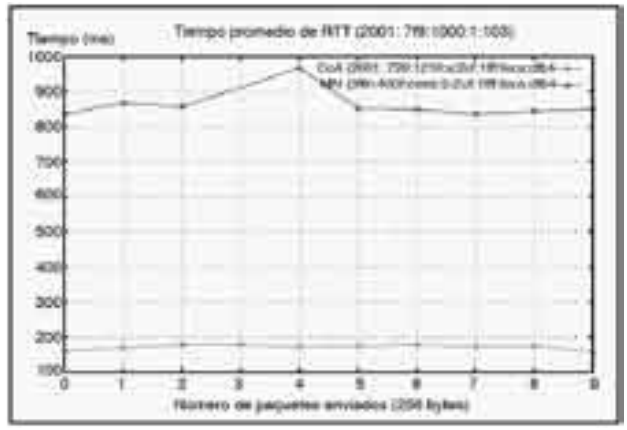

Figure. 5. Transfer time measurements of file transfer from home network.

ties to the case of ping and traceroute become obvious.

The transmission time and rate are quite constant and there is little difference between the two scenarios.

In a second set of measurements, the peer was located close to the current location of the MN, namely in Europe (www.euro6ix.com). The results are shown in Figure 6. In this case the difference between the scenarios is clearly visible. The explanation for the much longer duration of the mobility scenarios is the delay caused by the necessity to pass twice through transatlantic connections.

A similar result can be appreciated in the measurement of traceroute shown in Figure 6. The number of hops in the mobility case is much higher.

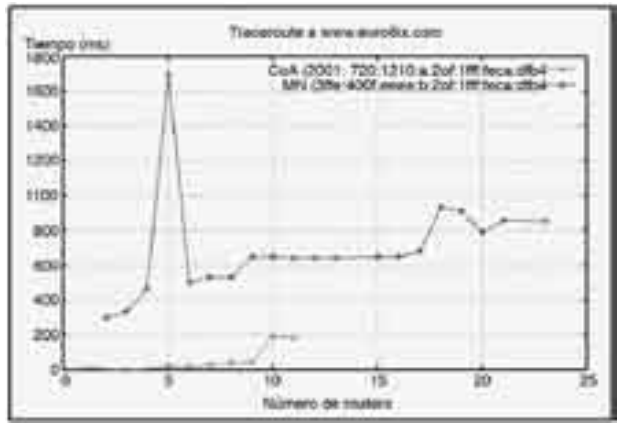

Figure. 6. RTT measurements of ping to network close to current link.

A third set of measurements used a connection to Japan (www.kame.net), which in regard of transmission time should lie more or less equidistant from the actual location of the MN in Spain and the tunnel end (HA) in Chile. In Figure 7, showing the corresponding ping results for this case, it can be appreciated that the RTT is relatively constant. The difference between the non-mobility and the mobility case is huge, as could be expected.

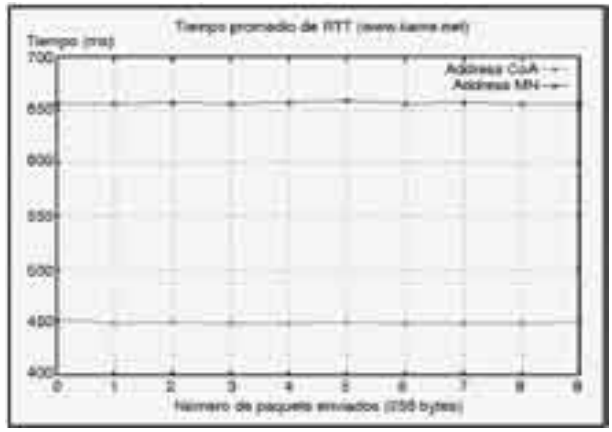

Figure 7. RTT measurements of ping to Japan.

In Figure 8, showing the corresponding traceroute results for this case, one can clearly identify the first hop (the tunnel) causing a great difference in the RTT.

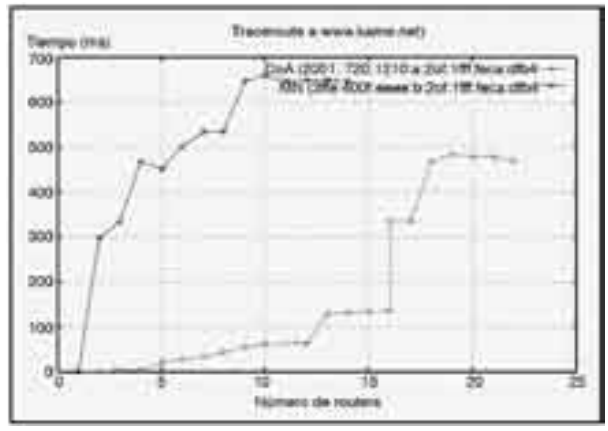

Figure 8. RTT measurements of traceroute to Japan.

The last set of measurements was realized with a peer that also supported the MIPv6 protocol and that was located close to the current network link. This way, the route optimization capabilities could be used.

In Figure 9 we can see in red and blue the results of the RTT of a series of pings representing the scenarios non-mobility and mobility without route optimization. Representing the third scenario, in which the route optimization capabilities were activated in both the MN and CN, the black points show that after some initial activation time the route optimization begins to work. The improvement is substantial; with route optimization one can obtain the same RTT results as in a direct connection.

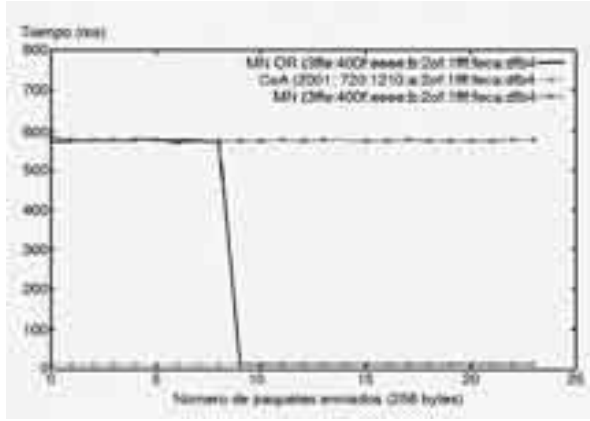

Figure 9. RTT measurements of ping to network close to current link using route optimization.

4. CONCLUSIONS

Both the second and the third set of measurements illustrated in this paper show clearly that the mobility mechanisms introduce a significant delay in the traffic. This can be mitigated by using Route Optimization features, which are only available if the correspondent node (CN) also supports the protocol MIPv6 and the MN allows for their use. Their necessity and effectiveness can be shown in the last set of measurements. However, the efficiency for shorttime connections has to be evaluated separately. In any case, without using route optimization, the only difference of MIPv6 to a manually setup IPv6-IPv6 tunnel between MN and HA is the automation and transparency of the process.

In summary, the efficiency of mobility depends largely on the support of the MIPv6 protocol by all communication partners thus allowing for Route Optimization. Its absence is a barrier in the adoption of mobility mechanisms.

On the other hand, the proposed user validation mechanism provides a simple and lightweight procedure that could be applied in commercial hot spots by ISP. It would allow them to implant IPv6 into their networks without having to change the external network architecture. The only changes necessary, as shown in

the development of this project, are the setup of a couple of machines in the administration core, realizing the mobility functions and the AAA mechanisms. The scheme could also perfectly be coupled to existing servers and databases in current networks using IPv6-IPv4 adaptation mechanisms and tunnels. This way it would generate new services and new business models and allow the faster adoption of the protocol IPv6.

Mobility is a hot theme nowadays and it causes a lot of discussion in scientific and engineering circles all around the world. It can be seen that still large discussion and testing procedures are necessary to mature the mechanisms and make them efficient. Maybe even political decisions could prove useful, for example to make mobility extensions obligatory, so one could rely on the optimization techniques available.

ACKNOWLEDGEMENTS

The authors would like to thank **FRIDA** (Fondo Regional para la Innovación Digital en América Latina y el Caribe) who has sponsored this research.

www.programafrida.net

BIBLIOGRAPHY

[1] S. Deering and R. Hinden, Internet Protocol, Version 6 (IPv6 Specification), IETF Request for Comments RFC 2460, December 1998; http://www.ietf.org/rfc/rfc2460.txt

[2] D. Johnson, C. Perkins and J. Arkko, Mobility Support in IPv6, IETF Request for Comments RFC 3775, June 2004; http://www.ietf.org/rfc/rfc3775.txt

[3] ProjectAIRE6; www.programafrida.net/sp/proyectos/arie6_acceso_i nalambrico_a_redes_ipv6.html

[4] S. Thomson and T. Narten, IPv6 Stateless Address Autoconfiguration, IETF Request for Comments RFC2462, December 1998; http://www.ietf.org/rfc/rfc2462.txt

[5] Mobile IPv6 for Linux; http://www.mipl.mediapoli.com/

CURRÌCULOS

Ing. Christian Lazo R. es profesor del área de redes del Instituto de Informática en la Universidad Austral de Chile. actualmente es candidato a Doctor en Ingeniería Telemática por la Universidad de Vigo en España, país donde reside. Su área de trabajo e investigación gira en torno al protocolo IPv6, redes móviles y la problemática de optimización de rutas e integración en redes heterogéneas.

Roland Glöckler es Ingeniero Electrónico Diplomado y Master of Science en Tecnología de Información. Actualmente trabaja en la Universidad Austral de Chile (UACh), donde su área de trabajo es la convergencia de redes de comunicaciones. Su actividad de investigación se concentra en el proyecto "VOI6E – Voz sobre IPv6 en entornos inalámbricos". También participó como co-investigador en el proyecto predecesor "Acceso Inalámbrico con Redes IPv6 (AIRE6)".