Automatic and Dynamic Connection of Next Generation Personal Area Networks to the Internet

Sérgio Nuno Queirós Pinto Lopes

Dissertation under the Master's Degree in Electrical and Computers Engineering of the Faculdade de Engenharia da Universidade do Porto, supervised by Prof. Manuel Ricardo and by Eng. Rui Campos

_____

President of the Jury

Faculdade de Engenharia da Universidade do Porto
Departamento de Engenharia Electrotécnica e de Computadores
Rua Roberto Frias, s/n, 4200-465 Porto, Portugal

March 2008

Resumo (Português)

A próxima geração de redes pessoais trará mudanças relativas ao paradigma de comunicações pessoais. Actualmente, um utilizador transporta consigo múltiplos dispositivos pessoais que, no entanto, operam de forma isolada. Num cenário futuro, esses mesmos dispositivos formarão uma rede pessoal em torno do utilizador, constituindo uma esfera de comunicação que se move com ele e se adapta quer às suas preferências, quer ao contexto de comunicação em cada momento, nomeadamente no que respeita à ligação à rede global (Internet) para o suporte de várias aplicações – *Voice over IP* (*VoIP)*, s*treaming* de vídeo, *e-mail*, *web browsing*. A heterogeneidade dos dispositivos (*Personal Digital Assistants* (PDAs), Telemóveis, *Laptops*, *Desktops*, Câmaras Digitais, Leitores MP3/MP4), das tecnologias de comunicação que formarão a rede pessoal (Bluetooth, Wi-Fi, Ultra Wide Band (UWB), Ethernet) e dos múltiplos mecanismos de autoconfiguração de redes, bem como a coexistência de dois protocolos IP (Internet Protocol) na Internet, apresentam-se como aspectos determinantes e com os quais é necessário lidar através de novas soluções.

As tecnologias actuais apenas permitem a criação de redes pessoais incipientes, focam-se numa única tecnologia de comunicação, por exemplo, Bluetooth ou Wi-Fi (Wireless Fidelity) e necessitam de configuração manual para diferentes cenários de acesso à Internet, não contemplando todos os aspectos referidos anteriormente. Assim, torna-se necessário criar uma nova solução capaz de não só organizar a rede de forma automática e dinâmica a nível interno, como também de lidar com a sua interligação à rede global mediante as preferências do utilizador e o contexto de comunicação em cada momento, nomeadamente em relação à versão do protocolo IP usada. Tendo em conta as limitações tecnológicas actuais, Campos e Ricardo propuseram uma nova solução para a autoconfiguração e autogestão de redes pessoais de próxima geração, denominada de *Autoconfiguration and Self-management of Personal Area Networks* (ASPAN), que lida com estes aspectos.

Neste trabalho desenvolveu-se um protótipo que pretende ilustrar o funcionamento de uma rede pessoal de próxima geração, considerando os aspectos acima referidos. Tendo por base a solução ASPAN, o protótipo desenvolvido implementa as seguintes funcionalidades:

1) criação e gestão de uma rede IP (IPv4 ou IPv6) entre os dispositivos que compõem uma rede pessoal;

2) gestão automática e dinâmica da conectividade de uma rede pessoal à Internet;

3) selecção inteligente do acesso à Internet em cada momento.

Com a realização deste trabalho verificou-se que a solução ASPAN permite a implementação dos cenários de ligação à Internet das redes pessoais de próxima geração, estabelecendo assim uma base para trabalhos futuros na área.

Abstract

The next generation of personal networks will bring changes regarding the paradigm of personal communications. Currently, a user carries multiple personal devices that work independently and in isolation. In a future scenario such devices will instead form a Personal Area Network (PAN) around the user, creating a communicating bubble that moves with him and adapts itself to the user preferences and communication context at each moment in time, namely concerning the connection to the global Internet in order to enable several applications, such as Voice over IP (VoIP), video streaming, e-mail, and web browsing. The heterogeneity of the personal devices (Personal Digital Assistants (PDAs), Mobile Phones, Laptops, Desktops, Digital Cameras, MP3/MP4 players), the communication technologies that will form a next generation PAN (Bluetooth, Wi-Fi, Ultra Wide Band (UWB), Ethernet) and the multiple mechanisms of autoconfiguration of networks, as well as the coexistence of two IP (Internet Protocol) versions on the Internet, represent crucial aspects that need to be tackled with new solutions.

Current PAN technologies only allow the creation of incipient PANs, focus on a single technology, such as Bluetooth and Wi-Fi (Wireless Fidelity), and require manual configuration for different Internet Access scenarios, not considering all the aspects aforementioned. Thereby, it is needed to come up with a new solution that is not only able to manage the PAN internally in an automatic and dynamic way, but also to deal with their interconnection to the global Internet considering the user preferences and the communication context at each moment in time, namely the IP protocol version used.

Regarding the limitations of current technologies, Campos and Ricardo proposed a new solution targeting the autoconfiguration and self-management of next generation PANs, called Autoconfiguration and Self-management of Personal Area Networks (ASPAN), which deals with these aspects.

In this work, a prototype of the ASPAN solution was developed, which intends to demonstrate the functioning of a next generation personal network, considering the aspects aforementioned. Based on the ASPAN framework, the developed prototype implements the next features:

1) creation and management of an IP network (IPv4 or IPv6) between the devices composing a PAN;

2) automatic and dynamic management of the Internet connection of a PAN;

3) intelligent selection of the best Internet access at each moment in time.

With this work, it was verified that the ASPAN solution allows the implementation of the Internet access scenarios of the next generation personal networks and thus establishes a base for future work in the area.

Preface

Currently, wireless networks are increasingly becoming part of our lives. This is mostly due to the growing impact of the Internet in people's lifestyle and their need to constantly move without losing global connectivity. In next generation wireless networks, the connection to the Internet will be a must from the end-users perspective, due to the growing number of services that it will provide. With this in mind and considering people to have all of their personal electronic devices connected together establishing an IP-based PAN, the need and the motivation of this work arises. Today's PANs are incipient. They usually require the user to have some networking knowledge and are often restricted to one technology (Bluetooth for example). This work intends to create a prototype that gives PANs the ability to manage available Internet links in its devices and to choose and configure the best Internet connection available in each moment, based on the ASPAN solution. This is intended to be made dynamically and with minimal user intervention.

Acknowledgments

This work would not be what it is without the help of some people. Thereby, I would like to thank Eng. Rui Campos and Prof. Manuel Ricardo for their guidance and efforts in making this work possible and for the enthusiasm and encouragement always demonstrated, helping me whenever possible. Also, I could not go on without thanking my family and closest friends for the comprehension and comfort given during the course of this work, specially my friend João Maia.

Table of Contents

List of Figures

List of Tables

Acronym List

ACK	Acknowledgment
ASPAN	Autoconfiguration and Self-management of Personal Area Networks
BNEP	Bluetooth Network Encapsulation Protocol
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
FQDN	Fully Qualified Domain Name
GbE	Gigabit Ethernet
GN	Group Ad-hoc Network
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IEEE	Institute of Electronic and Electrical Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Provider
L2CAP	Logical Link Control and Adaptation Protocol
LAN	Local Area Network
MAC	Medium Access Control
MAN	Metropolitan Area Network
NAP	Network Access Point
NAT	Network Address Translation
NGN	Next Generation Network
OFDM	Orthogonal Frequency-Division Multiplexing
OS	Operating System
OSI	Open System Interconnection
PAN	Personal Area Network
PANU	Personal Area Network User
PDA	Personal Digital Assistant
PECP	PAN External Connectivity Prototype
PHY	Physical Layer
PoA	Point of Attachment
POS	Personal Operation Space
QoS	Quality of Service
RFC	Request For Comments
SSID	Service Set Identifier
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

USB	Universal Serial Bus
UWB	Ultra Wide Band
VoIP	Voice over IP
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network

1 Introduction

In the Next Generation Networks (NGNs) an all-IP communication era will arise. The IP (Internet Protocol) technology will be used as basis to integrate cellular/mobile networks, Wireless Personal Area Networks (WPANs) and Wireless Local Area Networks (WLANs) under the same umbrella. Also, IP will be used as the common ground to enable all types of services and applications, such as voice communication (VoIP), video on-demand, e-mail, and web browsing. An evolution towards ubiquitous connectivity will happen and the "Always Best Connected" paradigm will be a must. On the other hand, users will carry Personal Area Networks (PANs) with them instead of multiple stand-alone devices as it happens today. The creation and management of PANs in an automatic and dynamic way and the seamless adaptation of the technology to different networking contexts and user needs will be crucial.

Currently, incipient PANs can be created using different technologies. Bluetooth [1] has been used as the standard solution. However, other technologies such as Wi-Fi [2] in ad-hoc mode and the upcoming WiMedia Ultra Wide Band (UWB) [3,4] also enable the creation of PANs. Still, these are just incipient PANs, in the sense that they can only be set up by means of manual configurations and usually require networking knowledge. In addition, they do not provide intelligent mechanisms that are able to adapt automatically and dynamically to different networking contexts and user preferences/needs, namely when it comes to the connection of the PAN to the Internet. In spite of this, all these WPAN technologies represent enabling technologies for next generation PANs. In addition, all can appear as Ethernet links to the upper layers of the protocol stack, which eases the deployment of IP networks over them. Thus, a new solution that takes all this features into account and adds new intelligent adaptive mechanisms that enable the automatic and dynamic adaptation of the PAN to the communication environment and user needs is all that is needed to create a PAN of the future.

Intensive research on this field is being carried out. Ongoing research projects and multiple discussion forums address these topics, and point out solutions; in [5,6,7] some solutions are presented. In [6,8] Campos and Ricardo present a new framework, the Autoconfiguration and Self-management of Personal Area Networks (ASPAN), which represents a new solution for next generation PANs. ASPAN defines mechanisms for self-creating and self-managing a PAN in the heterogeneous environments envisioned for NGNs, and deals with the dynamic and automatic connection of a PAN to the Internet based on user-defined policies.

The work presented herein is a prototype which implements the PAN external connectivity features provided by ASPAN. The implementation considers: 1) creation and management of an IP network (IPv4 or IPv6) between the devices composing a PAN; 2) automatic and dynamic management of the Internet connection of a PAN; 3) intelligent selection of the best Internet access at each moment in time.

1.1 Scope

This work fits in the (Wireless) Personal Area Networks domain. A Personal Area Network (PAN) represents the interconnection of information technology devices within the range of an individual person, typically within a range of 10 meters. For example, a person travelling with a laptop, a personal digital assistant (PDA) and a portable printer could interconnect them without having to plug anything in, using some form of wireless technology. PANs are formed by wireless communications between devices by way of technologies such as Bluetooth or Ultra Wide Band (UWB). The concept of a PAN was proposed by Thomas Zimmerman and other researchers at MIT's Media Lab and later supported by IBM's Almaden research lab. In [9], Zimmerman explains why the concept might be useful:

"As electronic devices become smaller, lower in power requirements, and less expensive, we have begun to adorn our bodies with personal information and communication appliances. Such devices include cellular phones, personal digital assistants (PDAs), pocket video games, and pagers. Currently there is no method for these devices to share data. Networking these devices can reduce functional I/O redundancies and allow new conveniences and services."

In a near future, PAN's will have a major role in people everyday life. The All-IP communication of the NGNs and the Internet services available (VoIP, web browsing, video streaming, e-mail...) will enable the WPANs to grow fast. People will carry a set of electronic personal devices, possibly each one with a different communication technology. Currently, incipient PANs can be created using different technologies but usually they involve networking knowledge and manual configuration. A solution that establishes a base for these devices to automatically configure and communicate together, and also connects them to the global Internet, is still to be implemented. In a next generation scenario, where multiple technologies like UMTS, WLAN and WiMAX will be available, a solution like this gains even more importance. Thus, the main goal of this work is to implement a solution that is able to dynamically manage and configure possible external links available for a PAN, allowing the PAN devices to have an "always-on" Internet connection.

1.2 Project Goals

The goal of this work was to develop a prototype of the ASPAN solution targeting the configuration of a next generation PAN which dynamically adapts to changes in its external network environment. The main objective of the work was to enable PANs to automatically and dynamically connect to the Internet, taking advantage of the capabilities of access of each of the devices belonging to the network and taking into account the changing context of communication as the user moves. However, we can split up this major objective into smaller sub-objectives:

Creation and management of an IP network within a PAN;
Management of the Points of Attachment (PoA) to the Internet available at each moment;
Automatic and dynamic connection to the Internet, through the best PoA;
Support for IPv6-based Internet accesses.

1.3 Major Results

This section identifies the major results achieved along the work. A separated section is dedicated to each relevant result for the sake of clearness.

1.3.1 PAN External Connectivity Prototype

The main result obtained with this work was the creation of an ASPAN prototype that is able to deal with the automatic and dynamic connection of a PAN to the Internet, choosing, at each moment, the best PoA available from the set of PoA provided by the devices forming the PAN. This is called PAN External Connectivity Prototype (PECP) from now on. To achieve this, some partial results were obtained and are listed below.

1.3.1.1 Creation and Management of an IP Network inside a PAN

The ASPAN solution defines the creation of a single logical link inside the PAN. This is the starting point of this work. After a Layer 2 (OSI Model) network is set up, based on whatever technologies are available (Wi-Fi, Bluetooth, Ethernet, etc…), an IP network is created, establishing connection between the PAN devices at a higher level. The process is also capable of dealing with the "joining" and "leaving" of devices and PoA of the PAN, automatically. All of these processes are made using the Dynamic Host Configuration Protocol (DHCP).

1.3.1.2 Automatic and Dynamic Connection to External Networks

The PECP allows the reconfiguration of the PAN whenever a better external access is available in any of the devices of the network. As soon as a new external access (e.g.: to the Internet) is available in one of the PAN devices, a set of Layer 2 messages are exchanged between the PAN members and the best PoA becomes active.

1.3.1.3 "Same PAN IP" Mechanism

The "Same PAN IP" mechanism enables the PAN members to keep always the same IP address even when the PAN PoA changes. Using the "Same PAN IP" mechanism, the PAN internal active connections continue to work even when the PAN external connections change.

1.3.1.4 Management of the External Links Available

The ASPAN solution includes a protocol based on the exchange of Layer 2 messages that elects a device of the PAN as master. The master is responsible for the management of the PAN. This includes the management of the PoA available, at each moment, and their characteristics. The PAN master is the only device that has this information. The other devices inform the master whenever a new external access becomes available or a PoA becomes inactive.

1.3.1.5 IPv6 Support

The PECP also supports the new IP version 6. This way, the PECP supports the heterogeneity associated with the coexistence of the two versions of the IP protocol. A device of the PAN can detect an external access based on the IPv6 protocol and become the PoA of the PAN almost the same way as if it was IPv4 based. The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is the protocol used for distributing global IP addresses within a PAN.

1.4 Structure of the Dissertation

This dissertation is divided into seven chapters. Chapter 2 presents the state of the art on wireless technologies, in particular wireless PAN technologies, the IP protocols available and describes existing solutions dealing with the connection of ad-hoc networks to the Internet. Chapter 3 describes the ASPAN solution used as basis for the implementation work considered in this dissertation and provides some theoretical background. Chapter 4 mentions the software tools used in the implementation work, as a complement to the developed software. Chapter 5 presents the work carried out and the obtained results. Chapter 6 evaluates the PECP. Chapter 7 draws the conclusions and refers to future work.

2 State of the Art

This chapter talks about how things stand in the technological area of this work. There are multiple technologies that can be useful to PANs like UWB, Wi-Fi, Ethernet and Bluetooth. Some of the prominent technologies are presented in this chapter, with special focus on wireless PAN technologies used as enabling technologies in this work. There is also a sub-chapter dedicated to the technologies that allow interconnection between a PAN and the Internet, like Bluetooth and Mobile Ad-hoc Networks (MANETs) solutions. In addition, some protocols and autoconfiguration solutions are also briefly described.

2.1 Wireless Networking Technologies

There are some important wireless technologies that should be referred so that we can understand the importance of this dissertation in the times that run by. A Wide Area Network (WAN) is a computer network that covers a broad area. It is a network whose communication links cross metropolitan or national boundaries. The largest and most well-known example of a WAN is the Internet. Metropolitan Area Networks (MAN) are smaller than WANs but large enough to span a city area. Wireless MAN defines broadband Internet access to fixed or mobile devices via antennas in a city. A Local Area Network (LAN) is a computer network covering a small geographic area, like a home, office or group of building. It is often used as a private network. Current Wireless LANs are most likely to be based on IEEE 802.11 technology [2]. PANs are the smallest computer networks and its reach is typically a few meters. They are formed by devices close to one person. In the figure below we can have an idea of where the PAN technologies fit in the wireless networking world.

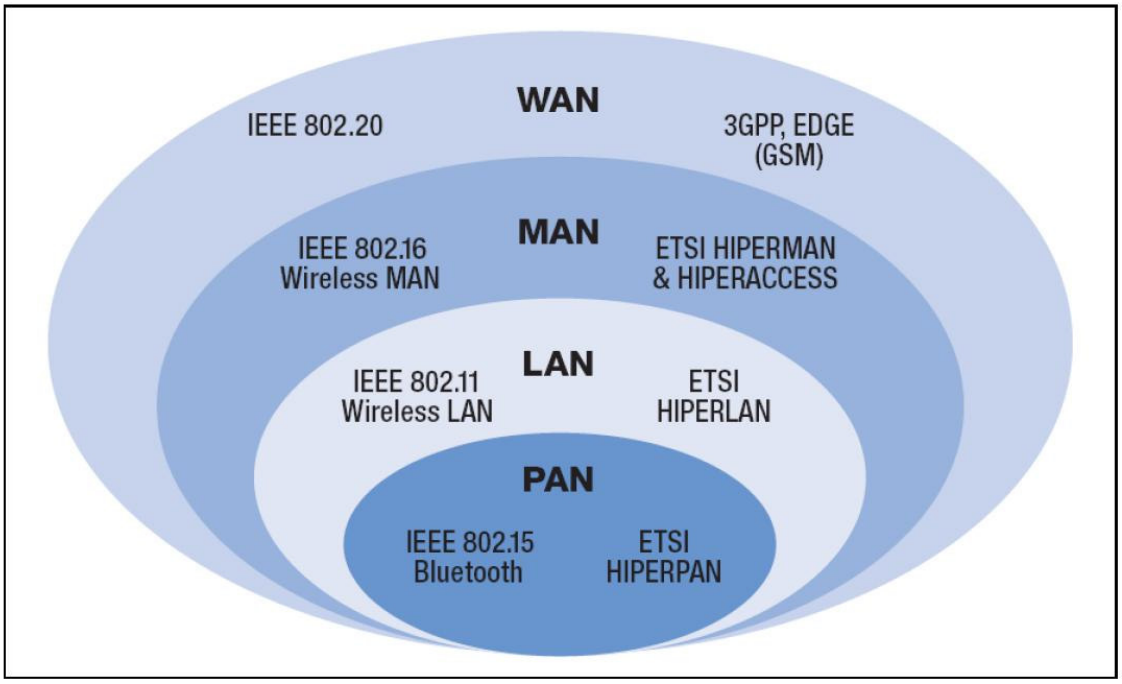

Figure 1 - Global Standards for wireless networks [10]

2.1.1 Bluetooth

Bluetooth is an industrial specification for wireless personal area networks. Bluetooth provides a way to connect and exchange information between devices such as mobile phones, laptops, PCs, printers, digital cameras, and video game consoles over a globally unlicensed short-range radio frequency. This technology is acceptable for situations when two or more devices are in proximity to each other and don't require high bandwidth. It also simplifies the discovery and setup of services. Bluetooth devices advertise all services they provide. This makes the utility of the service much more accessible, without the need to worry about network addresses, permissions and all the other considerations that go with typical networks.

2.1.1.1 Bluetooth PAN Profile

Using Bluetooth wireless technology, devices have the ability to form networks and exchange information. For these devices to interoperate and exchange information, a common packet format has been defined to encapsulate Layer 3 network protocols. That protocol is the Bluetooth Profile version 1 [11] and is used to encapsulate IP packets over BNEP (Bluetooth Network Encapsulation Protocol) headers. BNEP is used to transport common networking protocols over the Bluetooth media such as IPv4 and IPv6. The packet format is based on EthernetII Framing as defined by IEEE 802. BNEP runs over L2CAP and reuses the Ethernet packet format commonly used for local area networking technology. For this profile, three general scenarios are discussed: Network Access Points (NAP), Group Ad-hoc Networks, PANU-PANU (PAN user). Each of the scenarios has unique network architecture and unique network requirements, but all are various combinations of a PAN. A network access point is a unit that contains one or more Bluetooth radio devices and acts as a bridge, proxy, or router between a Bluetooth network and some other network technology. Group ad-hoc networking allows mobile hosts to cooperatively create ad-hoc wireless networks without the use of additional networking hardware or infrastructure. A point to point connection between two PANUs allows direct communication between these two nodes only.

2.1.2 Wi-Fi (IEEE 802.11)

Wi-Fi is a wireless technology standard defined by the IEEE. Wi-Fi networks use a radio technology called 802.11b to provide wireless connectivity. 802.11b uses the 2.4GHz frequency spectrum with a bandwidth of 11Mbps. There are other 802.11 technologies, including 802.11a (5GHz, 54Mbps) and 802.11g (2.4Ghz, 54Mbps). Wi-Fi continues to be the pre-eminent technology for building general-purpose wireless networks. Wi-Fi has become as prevalent a technology at home as it is at work. WiFi-equipped computers and other devices continue to proliferate as the prices of Wi-Fi gear continue to drop. Clearly, Wi-Fi will continue to be an important force in the market for some time to come. Even though it was designed primarily for private applications, WiFi is also being deployed in public places to create so-called hotspots, where WiFi-capable users can obtain broadband Internet access. This new domain of application could be the major future market

opportunity for WiFi, but in order to take advantage of it, several key challenges, both technical and business-related, must be overcome.

Wi-Fi differs from Bluetooth in that the former provides higher throughput and covers greater distances, but requires more expensive hardware and higher power consumption. They use the same frequency range, but employ different multiplexing schemes. While Bluetooth is a cable replacement for a variety of applications, Wi-Fi is a cable replacement only for local area network access. Bluetooth is often thought of as wireless Universal Serial Bus (USB), whereas Wi-Fi is wireless Ethernet, both operating at much lower bandwidth than the cable systems they are trying to replace. However, this analogy is not entirely accurate since any Bluetooth device can, in theory, host any other Bluetooth device - something that is not universal to USB devices.

2.1.3 WPAN (IEEE 802.15)

IEEE 802.15 is the 15th working group of the IEEE 802 which specializes in Wireless PAN Standards. The IEEE 802.15 standard defines physical layer (PHY) and medium access control (MAC) specifications for wireless connectivity with fixed, portable, and moving devices within or entering a personal operating space (POS). A POS is the space about a person or object that typically extends up to 10 m in all directions and envelops the person whether stationary or in motion. The original goal of the IEEE 802.15.1 Task Group was to achieve a level of interoperability that could allow the transfer of data between a WPAN device and an IEEE 802.11 device. Although this proved infeasible, IEEE Std 802.15.1-2005 does have mechanisms defined to allow better coexistence with IEEE802.11b class of devices. WPAN standards include:

- 802.15.1a: Standardizes Blueetoth's MAC and PHY levels (2.4GHz at 1Mbps)
- 802.15.2: Coexistence of PANs with one another
- 802.15.3: High rate PAN, used for UWB (2.4GHz at 55 Mbps)
- 802.15.3a: Alternative high rate PAN for UWB (2.4GHz at 110 Mbps)
- 802.15.4: Low rate PAN - Standardizes ZigBee's MAC and PHY levels
- 802.15.4a: Alternative low rate - low power UWB

2.1.4 Ultra Wide Band

Ultra-Wideband (UWB) [3,4] is a technology for transmitting information spread over a large bandwidth (>500 MHz) that should, in theory and under the right circumstances, be able to share spectrum with other users. This is intended to provide an efficient use of scarce radio bandwidth while enabling both high data rate personal-area network (PAN) wireless connectivity and longer-range, low data rate applications as well as radar and imaging systems. Due to the extremely low emission levels currently allowed by regulatory agencies, UWB systems tend to be short-range and indoors. However, due to the short duration of the UWB pulses, it is easier to engineer extremely high data rates, and data rate can be readily traded for range by simply aggregating pulse energy per data bit using either simple integration or by coding techniques. Conventional Orthogonal Frequency-Division Multiplexing (OFDM) technology can also be used subject to the minimum bandwidth requirement of the regulations. High data rate UWB can enable wireless monitors, the

efficient transfer of data from digital camcorders, wireless printing of digital pictures from a camera without the need for an intervening personal computer, and the transfer of files among cell phone handsets and other handheld devices like personal digital audio and video players.

As a way to allow Ethernet packets to be sent over UWB, the WiMedia Alliance is in the process of publishing the WiMedia Networking Protocol currently known as WiNet. WiNet defines a Logical Link Control Layer networking protocol for the WiMedia radio platform to model the behaviour of an IEEE 802 environment. Since IEEE 802 is the basis of both Wi-Fi (IEEE 802.11) and Ethernet (IEEE 802.3), WiNet is designed to support easy bridging between these networks. The draft standard proposes IEEE 802.1D bridges to integrate UWB networks with the IEEE 802-like networks.

In the next figure we can see where WiNet will stand compared to the already established technologies.

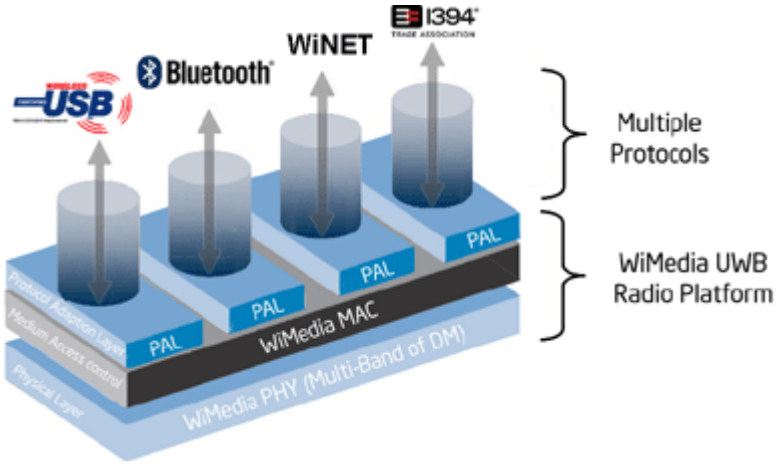

Figure 2 – UWB architecture integrating multiple technologies [12]

It is believed that UWB, with its technical and economic advantages, should help enable mainstream adoption of WPANs. Some people envisions a world of pervasive wirelessly connectivity in the home and in the office for all. UWB can help to achieve such vision.

2.1.5 ZigBee (IEEE 802.15.4)

ZigBee is the name of a specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs). ZigBee is targeted at RF applications that require a low data rate, long battery life, and secure networking. Their protocols are intended for use in embedded applications requiring low data rates and low power consumption. ZigBee's current focus is to define a general-purpose, inexpensive, self-organizing, mesh network that can be used for industrial control, embedded sensing, medical data collection, smoke and intruder warning, building automation, home automation, domotics, etc. The resulting network will use very small amounts of power so individual devices might run for a year or two using the originally installed battery. This technology is not designed for the PAN scenario of this work. It is more adequate to use it in sensor networks.

2.2 Ethernet (IEEE 802.3)

There is basically one wired technology that can be used in PANs. Ethernet is based on the IEEE 802.3 standard. This standard defines the PHY and the MAC sub-layer of the data link layer for this wired technology. This is generally a LAN technology with some WAN applications, and typically uses coaxial cable or special grades of twisted pair wires. It can also be used in PANs if, for instance, a connection between a desktop and a laptop with high data rate is needed. Ethernet bandwidth has been increasing over the years. It started with a thick coaxial cable bus running at 10 Mbit/s and evolved to the recent point-to-point links running at 1 Gbit/s and beyond (GbE). Ethernet is a well established technology in today's networking scenario and, although NGNs will probably be based on wireless technologies, it was used in this work as an enabling technology.

2.3 Firewire (IEEE 1394)

Firewire, also known as i.Link or IEEE 1394, is a high speed PC serial bus interface standard developed by Texas Instruments and Apple computers. Firewire offers data services and high-speed communications between digital devices. It has a data transfer capacity up to 800 Mbps and allows for real-time data transfer between a peripheral and a host computer or device, with guaranteed bandwidth and no error correction. Firewire facilitates faster data transfer rates and usability across multiple devices. This technology can be used in PANs when a transfer of information is needed between certain types of devices which require high-speed data transfer, such as digital camcorders, DVD players and digital audio equipment.

2.4 Internet Protocols

This section is focused on the IP protocols that can establish the Network Layer (or Layer 3) of the OSI model in a PAN. The Internet Protocol is a data-oriented protocol used for communicating data across a packet-switched internet work. As a Network Layer protocol, it is encapsulated in an OSI Layer 2 protocol like Ethernet. The IPv4 protocol and its future substitute - IPv6 - will be referred here. These are the protocols used today on the Internet and on almost every network available and are expected to coexist for many years in the networking context.

2.4.1 IPv4

Internet Protocol version 4 (IPv4) is the first version of the IP protocol still in use in IP networks, namely the Internet. It is described in the Internet Engineering Task Force (IETF) RFC 791 dated September 1981 and consists of the most relevant Layer 3 protocol nowadays. IPv4 uses 32bit addresses, limiting the address space to 4 billion unique addresses. This somewhat limited address space would have been consumed much faster if it was not for the appearance of Network Address Translation (NAT), which is better explained in the next sub-section. Nevertheless, the end of IPv4 is an inevitable reality at some time in the future. The Internet Corporation for Assigned Names and Numbers (ICANN) has even made a pronouncement on this topic, called "On the Deployment of IPv6" that says:

"Whereas, the unallocated pool of IPv4 address space held by IANA and the Regional Internet Registries is projected to be fully distributed within a few years; Whereas, the future growth of the Internet therefore increasingly depends on the availability and timely deployment of IPv6; Whereas, the ICANN Board and community agree with the call to action from the Address Supporting Organization and the Number Resource Organization, Regional Internet Registries, the Government Advisory Committee, and others, to participate in raising awareness of this situation and promoting solutions;

(...) The Board further resolves to work with the Regional Internet Registries and other stakeholders to promote education and outreach, with the goal of supporting the future growth of the Internet by encouraging the timely deployment of IPv6."

The problem with IPv4, besides the address space, is that it is not ready for the deployment or the needs of the NGNs. Features like scalable multicast, mobility "plug-and-play", and real-time flow will become essential in the NGNs scenario and IPv4 was not designed to deal with them.

2.4.1.1 Network Address Translation

Network Address Translation (NAT), also known as IP Masquerading, is an essential technique in today's networking scenario. Without it, the limited address space in the IPv4 protocol would probably be long gone. NAT consists of re-writing the source and/or destination IP addresses and usually also the TCP/UDP port numbers of IP packets as they pass through a router. This way, it is possible to have an Internet Service Provider (ISP) assigned address for a LAN of several computers. NAT will automatically translate the private LAN IP address for each separate PC on the LAN to the single public IP address as it exits the router bound for the public Internet. It also does the reverse translation for returning packets. Nonetheless, NAT can introduce complications in communication between hosts, destroying a key benefit of the Internet as a network of always-on, equally-connected, easily-reachable peers, and may have a performance impact. NAT was mainly deployed for use with IPv4. The future adoption of IPv6, with its abundance of addresses, will eliminate any need for NAT and, by extension, will eliminate the roadblocks to Internet progress that NAT represents.

2.4.2 IPv6

IPv6 defines the next version of the Internet Protocol and is envisioned to replace the current version widely used in the Internet. While IPv4 uses static device configuration (unless a separate application like DHCP is used) and needs user intervention every time a new device joins the network, IPv6 has the advantage of being a "plug-and-play" protocol, meaning that the devices are able to autoconfigure themselves to communicate with each other. Thus, a device can obtain, from the active routers in the network, the prefix provided to that network. To that prefix, the device adds its hardware address, creating a unique address in the world. This is possible due to the larger address space of IPv6, which supports more than 10^{38} different addresses. Contrary to IPv4, the autoconfiguration process is IPv6 native. Also, IPv6 is better prepared for the NGNs needs. It has the Quality of Service

(QoS) and Mobility concepts as main reasons for its development. The idea is to allow a better performance of future services like VoIP and real-time movie streaming, keeping the mobility aspect in mind.

2.5 Autoconfiguration Solutions

This section is devoted to the most relevant IP autoconfiguration mechanisms defined for both IPv4 and IPv6. There are two categories of mechanisms: stateless and stateful. A separated sub-section is dedicated to each one of these categories and their mechanisms

2.5.1 Stateless Autoconfiguration

Both versions of the IP protocol have stateless solutions for autoconfiguration of addresses. The stateless mechanisms have the advantage of not needing a centralized service to autoconfigure its network interfaces. They are briefly described in the next sub-sections.

2.5.1.1 Dynamic Configuration of IPv4 Link-Local Addresses

The Dynamic Autoconfiguration of IPv4 Link-Local Addresses was deployed by the IETF Zeroconf Work Group [13]. This solution defines how a host can automatically configure an IPv4 address that enables it to communicate with other devices in the same link. First, the host generates a random IP address in the 169.254/16 range. Next, it performs duplicate address detection using an Address Resolution Protocol (ARP) probe. If a reply is received, it must consider that the address is being used by other terminal and try a new address. Finally, the host assigns the IP address to the local network interface, and link local connectivity becomes possible.

2.5.1.2 IPv6 Stateless Address Autoconfiguration

This solution is specified in [14] and is similar to the previous but for IPv6. An IPv6 address has two parts: a subnet prefix, representing the network to which the interface is connected and a local interface ID, usually derived from the MAC address of the interface. The prefix is the well-known FE80::0/10, therefore the system can build automatically a link-local address. After uniqueness verification with a process called Duplicate Address Detection (DAD), the system can communicate with other IPv6 hosts on that link without any other manual operation. Moreover, a global address can be configured, also automatically, by combining the prefix announced by the local router, using the Router Advertisement messages defined in [15], with the interface ID. The Router Advertisements contain two flags, M and O, which tell the host weather a DHCPv6 server should be contacted to acquire additional information about the network.

2.5.2 Stateful Autoconfiguration

The stateful autoconfiguration mechanisms require a centralized service to do the state information maintenance of each individual client. The DHCP protocol is the most used stateful autoconfiguration mechanism and it exists for both versions of the IP protocol. The DHCP protocol is briefly described in the next sub-section.

2.5.2.1 The DHCP Protocol

Dynamic Host Configuration Protocol (DHCP) [16] is an autoconfiguration protocol used by networked computers (*clients*) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server. This is known as a stateful autoconfiguration mechanism because the server keeps a record of the state of the network at all times. The DHCP server ensures that all IP addresses are unique, e.g., no IP address is assigned to a second client while the first client's assignment is valid (its *lease* has not expired). Thus IP address pool management is done by the server and not by a human network administrator. DHCP uses the same two Internet Assigned Numbers Authority (IANA) assigned ports as BOOTP [17]: 67/udp for the server side, and 68/udp for the client side. DHCP operations fall into four basic phases. These phases are IP lease request, IP lease offer, IP lease selection, and IP lease acknowledgement. After the client obtained an IP address, the client may start an address resolution query to prevent IP conflicts caused by address poll overlapping of DHCP servers.

DHCP discovery

The client broadcasts on the local physical subnet to find available servers. Network administrators can configure a local router to forward DHCP packets to a DHCP server on a different subnet. This client-implementation creates a UDP packet with the broadcast destination of 255.255.255.255 or subnet broadcast address.

DHCP offers

When a DHCP server receives an IP lease request from a client, it extends an IP lease offer. This is done by reserving an IP address for the client and sending a DHCPOFFER message across the network to the client. This message contains the client's MAC address, followed by the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer.

DHCP requests

When the client PC receives an IP lease offer, it must tell all the other DHCP servers that it has accepted an offer. To do this, the client broadcasts a DHCPREQUEST message containing the IP address of the server that made the offer. When the other DHCP servers receive this message, they withdraw any offers that they might have made to the client. They then return the address that they had reserved for the client back to the pool of valid addresses that they can offer to another computer. Any number of DHCP servers can respond to an IP lease request, but the client can only accept one offer per network interface card.

DHCP acknowledgement

When the DHCP server receives the DHCPREQUEST message from the client, it initiates the final phase of the configuration process. This acknowledgement phase involves

sending a DHCPACK packet to the client. This packet includes the lease duration and any other configuration information that the client might have requested.

At this point, the TCP/IP configuration process is complete.

Although the DHCP description presented before refers to the IPv4 protocol, this mechanism of autoconfiguration can be used with both versions of the IP protocol. The DHCPv6 RFC, submitted in July of 2003, proposes an (almost) entire rewrite of DHCPv4, but for IPv6. The DHCPv6 and the DHCPv4 are very similar, being the exchanged messages the main difference.

2.6 Connection of PANs to the Internet

This section refers to existing technologies that enable the interconnection of a PAN to the Internet. Solutions to this matter are being developed but there are already some solutions created based on Bluetooth or Mobile Ad-hoc Networks (MANETs) technologies. These solutions are described in the next sub-sections.

2.6.1 Bluetooth using the PAN Profile

It is possible to use the Bluetooth PAN Profile, previously described in Section 2.1.1.1, to interconnect a PAN to the Internet if the scenario where a PAN device uses the NAP service is implemented. The device deploying the NAP service is able to provide access to some external networks, such as the Internet. This device acts as a bridge or router between the Bluetooth PAN and the external network allowing the other PAN devices to connect to it as PANUs. However, this is an incipient network in the sense that it needs manual configuration and networking knowledge. If, for instance, a change of PAN gateway is needed, we would have to manually configure it again because the Bluetooth PAN profile does not define any dynamic mechanism to deal with the change in the PAN gateway. As such, a fast and automatic adaptation to the networking context and to a new PoA is not possible with this solution.

2.6.2 Mobile Ad-hoc Networks solutions

There is an IETF working group that is trying to find a solution for the autoconfiguration in Mobile Ad-hoc Networks (MANETs). This group, called MANET AUTOCONF working group is searching for a standard autoconfiguration solution for MANETs, where each terminal is always acting as a router and running a routing protocol to maintain every terminal in the MANET with IP connectivity. There are already some autoconfiguration protocols for MANETs defined in [18] and [19]. The IETF final solution will probably be influenced by them. The current MANETs autoconfiguration and routing protocols need separate solutions for each IP version, and there is no mechanism enabling the selection of a proper framework considering the network context. In what concerns to PAN Internet connectivity, the MANET solutions typically consider the existence of one network gateway and do not have any defined criteria that allows the selection of the best PoA at each moment. The main concern in MANETs solutions is the selection of the shortest path between each network node in the MANET and a predefined gateway,

supported by the PoA, to the Internet. Although the MANETs autoconfiguration is not yet standardized, there is already some work done.

This chapter intended to show the state of the technologies, protocols and autoconfiguration mechanisms currently available. Also, a description of the state of the solutions available to interconnect a PAN to the Internet was presented. We can see that this area of network communications is in strong development nowadays but a solution, which constantly adapts to the external network context at each moment and integrates both IP versions, is not yet available. This work intends to fill in this hole by implementing a possible solution to the problem stated.

3 Theoretical Background

There is not much background theory to this work besides the ASPAN framework and the background theory of PANs. A NGN example is shown in the next figure. Multiple technologies, external accesses and devices are present including Bluetooth, Ethernet and WLAN used in this work.

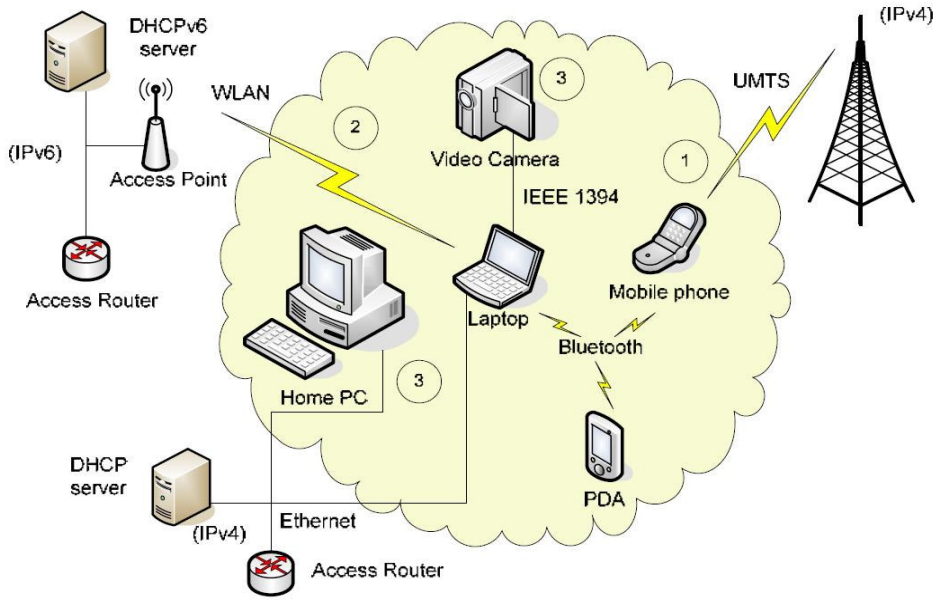

Figure 3 – Example scenario for Next Generation Networks from end-user perspective [8]

3.1 The ASPAN Framework

The Auto-configuration and Self-management of Personal Area Networks (ASPAN) [6,8] is the base framework used in this work. ASPAN has been proposed by Campos and Ricardo and aims at addressing the auto-configuration and self-management of a Personal Area Network (PAN) in a NGN communication scenario. This framework establishes the PAN Control Protocol (PCP), which is the communication protocol used between the different PAN devices. In the following sections, the main features of the framework are presented.

3.1.1 Master-Slave Paradigm

ASPAN is based on a master-slave model. When devices come together to form a PAN one of them is elected as the master of the network using the election algorithm mentioned in Section 3.1.2.1. Afterwards, the master device stores locally a topological tree where it stands as the root and is in charge of telling the other PAN devices when and how to create bridges and what to do to have access to external networks.

3.1.2 Master Election and Topology Discovery

This section describes the mechanism and the algorithm used for electing the master and for discovering the topology of the PAN. The master is only elected when there are at least two devices forming the PAN. In the following, the election algorithm and the parameters

taken into account to elect the master are described. Afterwards, the election and topology discovery mechanism is defined.

3.1.2.1 Master Election Algorithm

The election of the master is performed based on an algorithm that considers four parameters:

- Battery capacity (mWh)
- CPU capability (MHz)
- Memory capacity (MB)
- Number of network interfaces

ASPAN considers weights associated to each of these parameters in order to account for parameters that may have higher importance than others. For that purpose, ASPAN defines the following coefficients associated to each parameter:

- W_{bat} – weight associated to the battery capacity parameter
- W_{CPU} – weight associated to the CPU capability parameter
- W_{mem} – weight associated to the memory capacity parameter
- W_{netif} – weight associated to the number of network interfaces parameter

The values assigned to each of these coefficients depend on the relevance assigned to each parameter. If all coefficients have the same relative relevance, then:

$W_{bat} = W_{CPU} = W_{mem} = W_{netif} = 0.25$

From now on, it is considered that all parameters have the same relevance.

The election algorithm works as follows. As soon as the device that has started the election process collected all required information from its partners, using the mechanism explained in the next section, it will run the election algorithm. For election purposes each PAN device is modelled as a Cartesian point in the 4-dimensional Cartesian space defined by the parameters presented above. Thus, for instance, a Laptop can be modelled by the following Cartesian point:

Laptop = (battery capacity, CPU capability, memory capacity, nº of network interfaces)
= (W_{bat}, W_{CPU}, W_{mem}, W_{netif})

Given the points representing each PAN device, the master is the device which distance to the origin of the 4-dimensional Cartesian space is the highest. Each PAN device computes its distance and reports it back to the device that initiated the election process which, in turn, will inform the elected device using the mechanism described in the next section.

3.1.2.2 Master Election and Topology Discovery Mechanism

At the very beginning, when PAN devices come together to create the PAN the topology of the network is unknown. The election process requires that all nodes get visited in order to collect information needed to run the election algorithm explained in previous section.

Therefore, the mechanism used for collecting such information can be used to collect information about the topology of the network; this is exactly what is considered herein.

The device initiating the process (initiator) broadcasts an Election message towards its neighbours (i.e., the nodes connected to the links it is connected to). A node receiving an ELECTION message elects the sender of that message as its parent node from the election mechanism point of view. The parent device is the device to which the current device has to return the topological information it could found out while interacting with its own neighbours. Upon receiving an ELECTION message, and if not yet participating in any election process, the current device re-broadcasts the message to its own neighbours. After receiving the election message the device replies with an ACK message to the election starter. This message already includes its distance to the origin of the 4-dimensional Cartesian point. The election mechanism finishes when the initiator has received ACK messages from all its neighbours.

It is worth noting that, while collecting information from the PAN devices used for running the election algorithm at the initiator, this mechanism is able to collect the topological information from the network. Then, at this point, the initiator has information about all devices currently connected to the PAN and the way they are connected to each other (topological information). This information includes the MAC addresses of each node interface, the MAC address it's connected to and the type of technology used in this connection. At this point, the topological information consists of a set of branches that combined form the connectivity graph modelling the topology of the PAN.

This following figure shows an example of an election process. The different ELECTION and ACK messages are displayed.

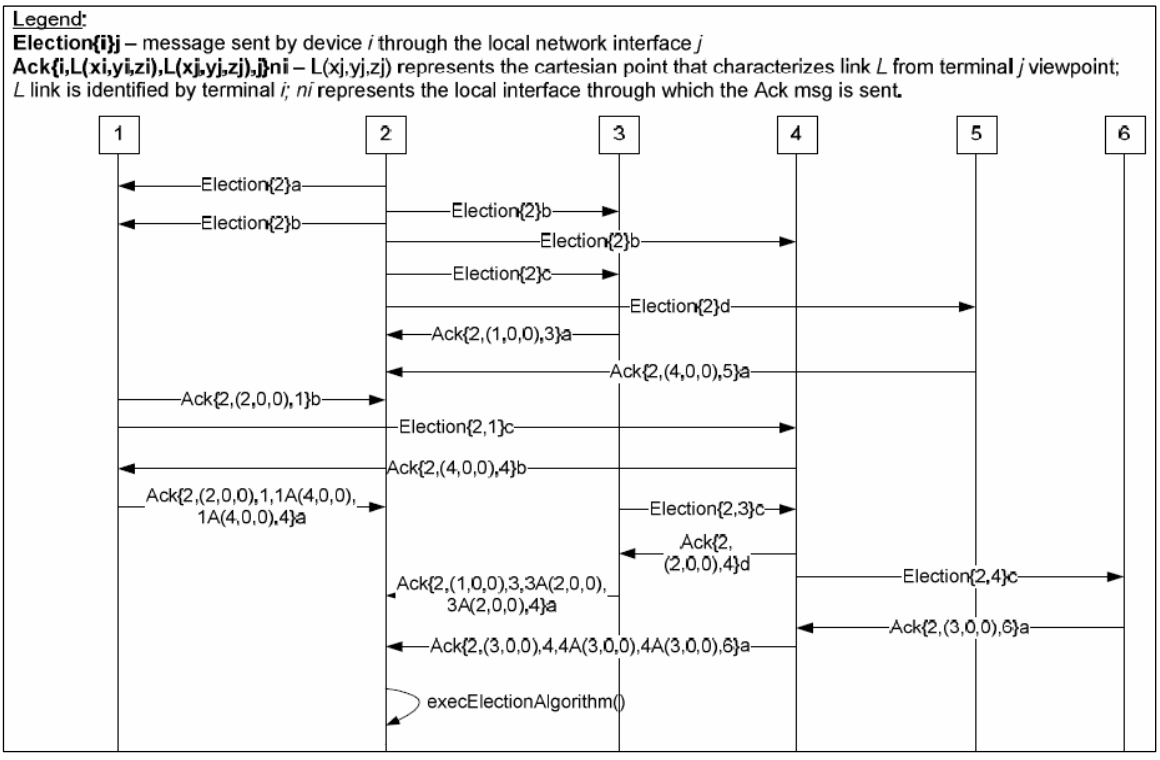

Figure 4 – Illustration of an election process

3.1.3 Device Identification within the PAN

In the ASPAN scope the identification of PAN devices is performed by reusing the identification strings already defined by legacy technologies, such as Bluetooth and WLAN. The identification of a device is always referred to the local domain defined by the PAN, whose composition is specified by the user, who identifies the terminals belonging to his PAN; for instance, JohnsPAN and BobsPAN identify possible IDs for the PAN local domain. For that purpose, the Service Set Identifier (SSID) and the Bluetooth Device Name parameters are reused. In fact, either WLAN or Bluetooth do not specify any concrete syntax for these identification strings. Thereby, one is free to specify the most suitable syntax for the applicability domain; the syntax associated to a Fully Qualified Domain Name (FQDN) used in the Internet for device identification was then used. The same identification is used regardless the specific Link Layer technology being used. The identification string (or FQDN) is mapped into both a MAC address and IP address (when IP connectivity is already established).

3.1.4 Joining Procedure

When a user's device is joining the PAN, it firstly discovers the device(s) of the PAN in the neighbourhood by using the proper Layer 2 mechanisms. This new device can only find the PAN if there's some device in it using the same kind of technology. After detecting the presence of one or more devices, the joining device broadcasts a message requesting to join the PAN. For the sake of simplicity this message is similar to the election message. The device which receives the election message knows that the PAN is already created. It replies saying to the joining device to ask for an IP address to the PAN master, in this case, using DHCP protocol.

When a new node joins the PAN, it may occur that it offers a better access to the Internet than the PAN external access being used. Thus, after the PAN master is informed by the joining device about the potential external access the latter can offer to the PAN, it checks against the user-defined policies if the access is better than the current access. If that is true, reconfigurations within the PAN are required with respect to the gateway towards the outside world. This is better described in Section 3.1.7

3.1.5 Leaving Procedure

The leaving mechanism is based on the control topological tree kept by the PAN master. Although the original ASPAN framework defined that every device connected to the PAN would regularly scans its links, the detection that some partner has left the PAN is engaged by the user with a "soft-leave" made in the Operating System (OS). The master, which knows the PAN topology, is notified and using that information, it updates the control topological tree accordingly. Also, it notifies its slaves about the current event so that each slave can update its local configurations related to the leaving device, which is no more available for communication. Furthermore, it includes the update of the local table containing the mapping between device names, corresponding MAC addresses, and the network interface through which the device is accessible.

If the leaving node is the master device, the sub-master is elected as the new master and a new sub-master is elected. On the other hand, if it is the sub-master that is leaving the PAN, a new sub-master is just elected and the PAN can still operate without any change. For simplicity and efficiency reasons the election of the new sub-master is performed by the master alone, since it has in hands all the information it needs to nominate the most suitable device to become the new PAN sub-master; in that sense, it is more a sort of nomination rather than an election. Finally, if both the master and sub-master leave the PAN at the same time, the PAN has to be created from the scratch by the remaining PAN devices.

Apart from the scenarios we have considered in the previous paragraph, which have more to do with the control plane issues, we can also consider the situation where, from a data plane point of view, the leaving device is the current gateway of the PAN to the outside world (e.g., Internet). In this scenario, a new gateway for the PAN is selected by the master of the PAN taking into account the user-defined policies. After the new gateway is selected, the master notifies the slaves accordingly. This implies reconfigurations at each node concerning the new gateway for the PAN. In addition, since the new PoA may support a different IP version, each device may have to enable the proper IP stack and configure the corresponding routing table accordingly. The mechanism used to perform such reconfigurations depends on the network configuration used within the PAN. In the case of this work, the DHCP protocol was the mechanism used.

A small deviation to the original ASPAN framework was made in this procedure. Nevertheless, it is of importance to mention that it is a possibility of the framework to implement other means that allow the detection of devices leaving the PAN.

3.1.5 Network Configuration

Network configuration in the context of the ASPAN framework is divided in two components: Configuration of specific PAN devices as interconnection nodes between different links of the PAN; Configuration of IP addresses and optional information for each PAN device for enabling IP connectivity within and to the outside of the PAN.

These two components are explained in detail in the following sections.

3.1.5.1 Configuration of Devices acting as Interconnection Nodes

In multi-hop scenarios the configuration of devices for enabling connectivity between the multiple devices composing a PAN is performed using bridging, specifically IEEE 802.1D bridges. Using bridging to interconnect devices connected to different links within the PAN results in the multiple devices becoming connected to the same logical link. This eases the deployment of traditional auto configuration mechanisms, such as DHCP. Furthermore, it enables the creation of a single IP sub network to which all PAN devices can be connected; this also eases the operation of traditional mechanisms, such as Address Resolution Protocol (ARP) [20] and Neighbour Discovery Protocol (NDP) [15]. On the other hand, even from the ASPAN framework, this type of PAN configuration can ease the transmission of control messages between PAN devices, since there is direct connection from every device to every device; concerning notification of some event the master just has to broadcast it to the local link and all slaves get informed.

3.1.5.1 Bluetooth Technology-dependent Aspects

When deploying the PAN using Bluetooth technology the Bluetooth PAN profile is considered. This profile defines three scenarios and three related roles for the Bluetooth devices: Gateway Node (GN), Network Access Point (NAP), and PAN User (PANU). When a new Bluetooth device using "mobile.BobsPAN" as ID string tries to join/create a PAN it will scan looking for any device with an ID string, whose suffix is ".BobsPAN". If such device is found an election message is sent to the existing device. Now, depending whether the existing Bluetooth device is part of a PAN or not two distinct things can happen. If the PAN does not exist yet, the existing device replies with an ACK message to the election initiator and the election process carries on normally.

3.1.5.2 Wireless LAN Technology-dependent Aspects

The WLAN technology, such as Bluetooth, specifies the use of an identification string, the SSID. Nevertheless, rather than in Bluetooth, where this string is used for informational purposes only, in WLANs it is used for distinguishing between different WLAN networks. Therefore, in the context of the ASPAN solution the following configurations are employed:

All PAN devices that are not connected to the PAN are configured with their own identification strings which, in this case, are mapped to the WLAN SSID; such as in Bluetooth, the FQDN syntax is employed, e.g., "Laptop.BobsPAN.";

After finding out some neighbour PAN device, the current PAN device changes the SSID of its local WLAN network interface from its own identification string to the identification string of the PAN, for instance, from "Laptop.BobsPAN." to "BobsPAN."; every PAN device does this in order to form a single WLAN network with the neighbour PAN devices;

When a PAN device is already connected to the PAN and has a WLAN network interface enabling the connection of new devices to the PAN, it also configures the WLAN interface with the FQDN of the PAN.

Using this approach PAN devices are able to find out whether the PAN is already created or not by just considering the FQDN announced by its neighbour devices.

3.1.6 Configuration of IP Connectivity within a PAN

In the beginning, when the PAN devices are forming a PAN, IP connectivity does not exist yet. Upon forming the PAN or joining it, PAN devices configure, at least, one IP address for intra-PAN communication. This "local" address is just intended to be used within the PAN and its configuration depends on PAN logical topology. Since the PAN devices are assumed to be all connected to the same logical link, the traditional autoconfiguration mechanisms can be used for IP address configuration. From IP connectivity standpoint, an important aspect is that devices have "static" addresses used for intra-PAN communication and which do not change every time the PoA for the PAN changes.

In the PECP, both IPv4 and IPv6 have been considered. In the IPv4 scenario, the PAN gateway needs to perform NAT to the other devices in the PAN, while with IPv6 this is not

needed. In addition, DHCP was selected as the autoconfiguration method that distributes IP addresses to the PAN devices. The DHCP protocol is presented in Section 2.5.2.1.

3.1.7 Reconfigurations due to a New PAN Gateway

The leaving of the PAN gateway or the selection of a new gateway will only influence the configuration of the PAN devices with respect to the outside world. This allows for the intra-PAN IP connectivity to remain unchanged. The migration to a new gateway may occur due to the leaving of the previous gateway or to the appearance of a better gateway. The master detects such event and sends a notification message towards the PAN slaves in order to have them changing their local IP configurations accordingly. The notification message contains information about the autoconfiguration mechanism to be used for acquiring a global IP address and allow the PAN slaves to have access to the new PoA of the PAN. Upon receiving the notification message for a new gateway, each slave triggers the proper legacy autoconfiguration mechanism and gathers from the message the IP address of the new gateway and the MAC address of the local interface through which the gateway is accessible. The configuration of the route towards the new gateway is then finalized without any further signalling exchange. As said before, the autoconfiguration mechanism used in this work is the well-known DHCP protocol.

In conclusion, this is an essential chapter for the comprehension of the following chapters as it describes the background theory used along the work. The ASPAN framework is the key element of the implementation described in Chapter 5.

4 Software Tools Used Along the Work

This chapter refers to some of the software programs used to create the PECP. Linux was the OS used in the implementation. Some of the most used Unix tools will be introduced in the first sections. Moreover, some software programs were also of great help, especially for debugging and testing the solution. Those are presented after.

4.1 Standard Unix Built-in Programs

In this section, the different Linux commands used during this work are listed.

4.1.1 *ifconfig*

It was used to configure the kernel-resident network interfaces. Using it, we could retrieve the status of a desired network interface and/or configure the interface. This tool is widely used by this software.

```
root@joao-desktop:/home/joao# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:6E:89:BD:C2
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:185

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:272 (272.0 b)  TX bytes:272 (272.0 b)

nas0      Link encap:Ethernet  HWaddr 00:0E:50:6D:3A:69
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:50ff:fe6d:3a69/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:102 errors:0 dropped:2 overruns:0 frame:0
          TX packets:25 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8085 (7.8 KiB)  TX bytes:1434 (1.4 KiB)

ppp0      Link encap:Point-to-Point Protocol
          inet addr:87.196.24.208  P-t-P:212.0.167.185  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1492  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:518 (518.0 b)  TX bytes:99 (99.0 b)

root@joao-desktop:/home/joao#
```

Figure 5 - *ifconfig* example

4.1.2 *iwconfig*

It is similar to ifconfig, but is dedicated to wireless networking interfaces. It was used to set the parameters of the network interface which are specific to the wireless operation (eg. SSID, mode, frequency…). iwconfig may also be used to display those parameters, and the wireless statistics (extracted from /proc/net/wireless).

```
root@joao-desktop:/home/joao# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

ra0       RT2400PCI  ESSID:off/any
          Mode:Managed  Channel=1  Bit Rate:11 Mb/s
          RTS thr:off   Fragment thr:off
          Encryption key:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  invalid crypt:0  invalid misc:0

sit0      no wireless extensions.

nas0      no wireless extensions.

ppp0      no wireless extensions.

panbr     no wireless extensions.

root@joao-desktop:/home/joao#
```

Figure 6 – *iwconfig* example

4.1.3 *iwlist*

It is used to display some additional information from a wireless network interface that is not displayed by iwconfig. The main argument is used to select a category of information, iwlist displays in detailed form all information related to this category, including information already shown by iwconfig. The command is primarily used to generate a list of nearby wireless access points and their MAC addresses and SSIDs. Using this tool, we could determine if the PAN is created, if there's one device listening/waiting to create the PAN or if this network interface is the first one in the (still not created) PAN.

4.1.4 *route*

It manipulates the kernel's IP routing tables. Its primary use is to set up static routes to specific hosts or networks via an interface after it has been configured with the ifconfig program. When the 'add' or 'del' options are used, route modifies the routing tables. Without these options, route displays the current contents of the routing tables. With this tool, we can check if the computer is connected to the Internet. Also, when a new access becomes available, the OS automatically adds a route in this table. This is essential for new external access detection and is better explained in the next chapter.

```
root@joao-desktop:/home/joao# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
212.0.167.185   *               255.255.255.255 UH    0      0        0 ppp0
192.168.0.0     *               255.255.255.0   U     0      0        0 nas0
default         *               0.0.0.0         U     0      0        0 ppp0
root@joao-desktop:/home/joao#
```

Figure 7 – IP routing table obtained with *route* command

4.1.5 *iptables*

It is used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains. Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a `target', which may be a jump to a user-defined chain in the same table. This program was used to configure the NAT mechanism.

4.1.6 *grep*

This command searches the named input files for lines containing a match for the given patterns. Matching lines are printed by default. The standard input is searched if no files are given or when the file is specified. This tool was used to retrieve information from ifconfig's, iwconfig's and iwlist's outputs using the pipe command "|" in the CLI.

```
root@joao-desktop:/home/joao# ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:272 (272.0 b)  TX bytes:272 (272.0 b)

nas0      Link encap:Ethernet  HWaddr 00:0E:50:6D:3A:69
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:50ff:fe6d:3a69/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2086 errors:0 dropped:2 overruns:0 frame:0
          TX packets:1133 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2788677 (2.6 MiB)  TX bytes:107741 (105.2 KiB)

ppp0      Link encap:Point-to-Point Protocol
          inet addr:87.196.24.208  P-t-P:212.0.167.185  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1492  Metric:1
          RX packets:1952 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1075 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:2763870 (2.6 MiB)  TX bytes:70582 (68.9 KiB)

root@joao-desktop:/home/joao# ifconfig | grep nas0
nas0      Link encap:Ethernet  HWaddr 00:0E:50:6D:3A:69
root@joao-desktop:/home/joao#
```

Figure 8 – *grep* command used after *ifconfig*.

4.1.7 *awk*

It scans each input file for lines that match any of a set of patterns specified literally in prog or in one or more files specified as -f profile. With each pattern there can be an associated action that will be performed when a line of a file matches the pattern. Each line is matched against the pattern portion of every pattern-action statement; the associated action is performed for each matched pattern. Combining (through a pipe, once again) this program with grep, we are able to retrieve only one text field from the stdout. This procedure will be explained in detail in Chapter 5.

```
root@joao-desktop:/home/joao# ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:272 (272.0 b)  TX bytes:272 (272.0 b)

nas0      Link encap:Ethernet  HWaddr 00:0E:50:6D:3A:69
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:50ff:fe6d:3a69/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2090 errors:0 dropped:2 overruns:0 frame:0
          TX packets:1136 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2788861 (2.6 MiB)  TX bytes:107869 (105.3 KiB)

root@joao-desktop:/home/joao# ifconfig | grep nas0
nas0      Link encap:Ethernet  HWaddr 00:0E:50:6D:3A:69
root@joao-desktop:/home/joao# ifconfig | grep nas0 | awk '{print$5}'
00:0E:50:6D:3A:69
root@joao-desktop:/home/joao#
```

Figure 9 – *awk* command used after "ifconfig | grep nas0".

4.1.8 Linux DHCP Server

The Internet Systems Consortium DHCP Server, *dhcpd*, implements the Dynamic Host Configuration Protocol (DHCP) for IPv4. DHCP allows hosts on a TCP/IP network to request and be assigned IP addresses, and also to discover information about the network to which they are attached.

The DHCP protocol allows a host which is unknown to the network administrator to be automatically assigned a new IP address out of a pool of IP addresses for its network. In order for this to work, the network administrator allocates address pools in each subnet and enters them into configuration file. On start-up, *dhcpd* reads the configuration file and stores a list of available addresses on each subnet in memory. When a client requests an address using the DHCP protocol, *dhcpd* allocates an address for it. Each client is assigned a lease, which expires after an amount of time chosen by the administrator (24hours, by default).

The PAN master runs this daemon in order to set up the IPv4 network over the PAN. This procedure will be explained in Chapter 5.

```
root@joao-desktop:/home/joao# dhcpd3 eth0
Internet Systems Consortium DHCP Server V3.0.3
Copyright 2004-2005 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/
Wrote 1 leases to leases file.
Listening on LPF/eth0/00:0c:6e:89:bd:c2/192.168.1/24
Sending on   LPF/eth0/00:0c:6e:89:bd:c2/192.168.1/24
Sending on   Socket/fallback/fallback-net
root@joao-desktop:/home/joao#
```

Figure 10 – *dhcpd3* output

4.1.9 Linux DHCP Client

The Internet Systems Consortium DHCP Client, *dhclient*, provides a means for configuring one or more network interfaces using the Dynamic Host Configuration Protocol based on the IPv4 protocol. The DHCP protocol allows a host to contact a central server which maintains a list of IP addresses which may be assigned on one or more subnets. A DHCP client may request an address from this pool, and then use it on a temporary basis for communication on network. The DHCP protocol also provides a mechanism whereby a client can learn important details about the network to which it is attached, such as the location of a default router, the location of a name server, and so on.

```
root@joao-desktop:/home/joao# dhclient eth0
Internet Software Consortium DHCP Client 2.0pl5
Copyright 1995, 1996, 1997, 1998, 1999 The Internet Software Consortium.
All rights reserved.

Please contribute if you find this software useful.
For info, please visit http://www.isc.org/dhcp-contrib.html

Listening on LPF/eth0/00:0c:6e:89:bd:c2
Sending on   LPF/eth0/00:0c:6e:89:bd:c2
Sending on   Socket/fallback/fallback-net
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3
DHCPOFFER from 192.168.1.1
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 192.168.1.1
bound to 192.168.1.3 -- renewal in 1296000 seconds.
root@joao-desktop:/home/joao#
```

Figure 11 – *dhclient* output

4.2 Other Software Tools Used

In this section, some of the software used during the implementation of the PECP is described.

4.2.1 Ethereal

Ethereal is the standard network packet analyzer. A network packet analyzer will try to capture network packets and display the packet data as detailed as possible. One could think of a network packet analyzer as a measuring device used to examine what's going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course). Ethereal was mainly used to troubleshoot network problems and for debugging. With it, we could determine if a message was correctly sent and/or received by the software. This was a very helpful way to debug the software. If, for some reason, the message was not received on the receptor, we could immediately know whether the problem was on the emitter or in the receiver, saving precious time. A screenshot of the program is displayed in Figure 12.

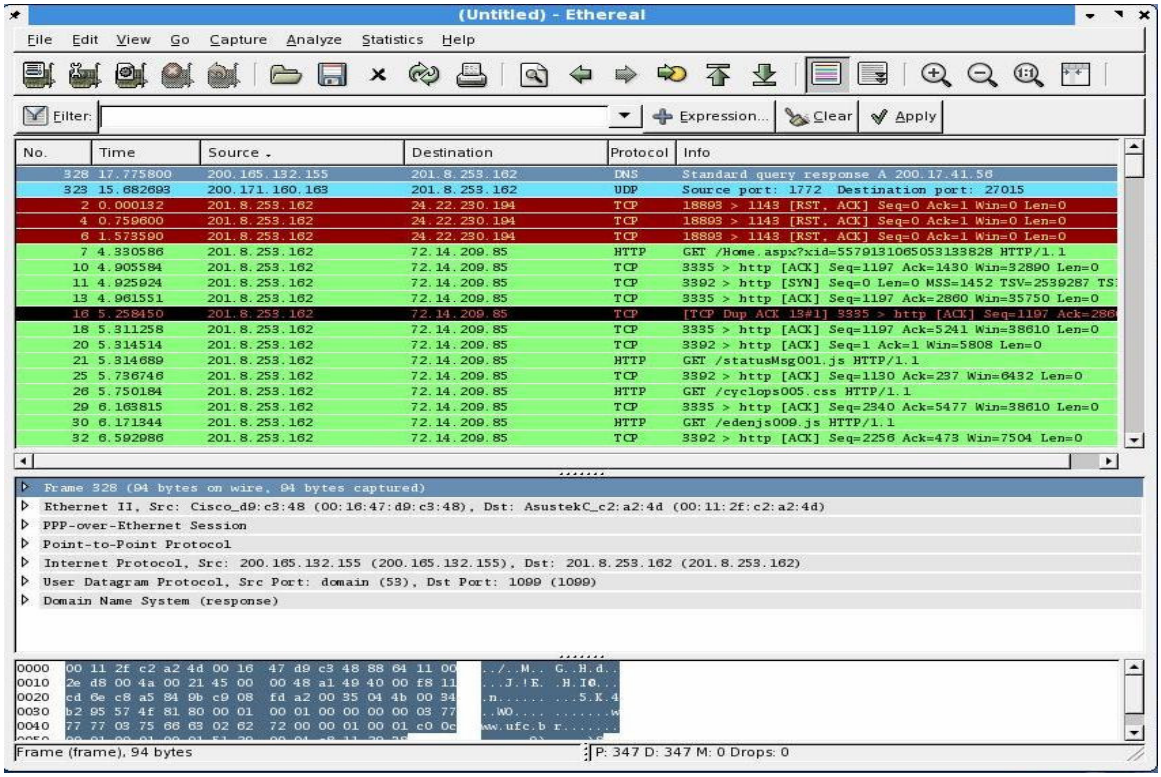

Figure 12 – Ethereal GUI

4.2.2 Dibbler

Dibbler is a portable DHCPv6 implementation. It supports stateful as well as stateless autoconfiguration for IPv6. In this work, only the stateful IPv6 autoconfiguration was used. Its functionality is very similar to the Linux DHCP for IPv4. It has two different programs, the dibbler-client and the dibbler-server. These programs enable the creation of an IPv6 network in a PAN.

4.2.3 Darkstat

A packet sniffer that runs as a background process on a cable/DSL router, gathers all sorts of statistics about network usage, and serves them over HTTP. One can measure the traffic passing trough an interface by observing the graphs produced in a HTTP page on our own web browser. This program was used for testing the final solution, especially in terms of the throughput of the PAN devices to an external host or ISP. These results are presented in Chapter 6. The next figure shows a screenshot of the Darkstat HTTP layout.

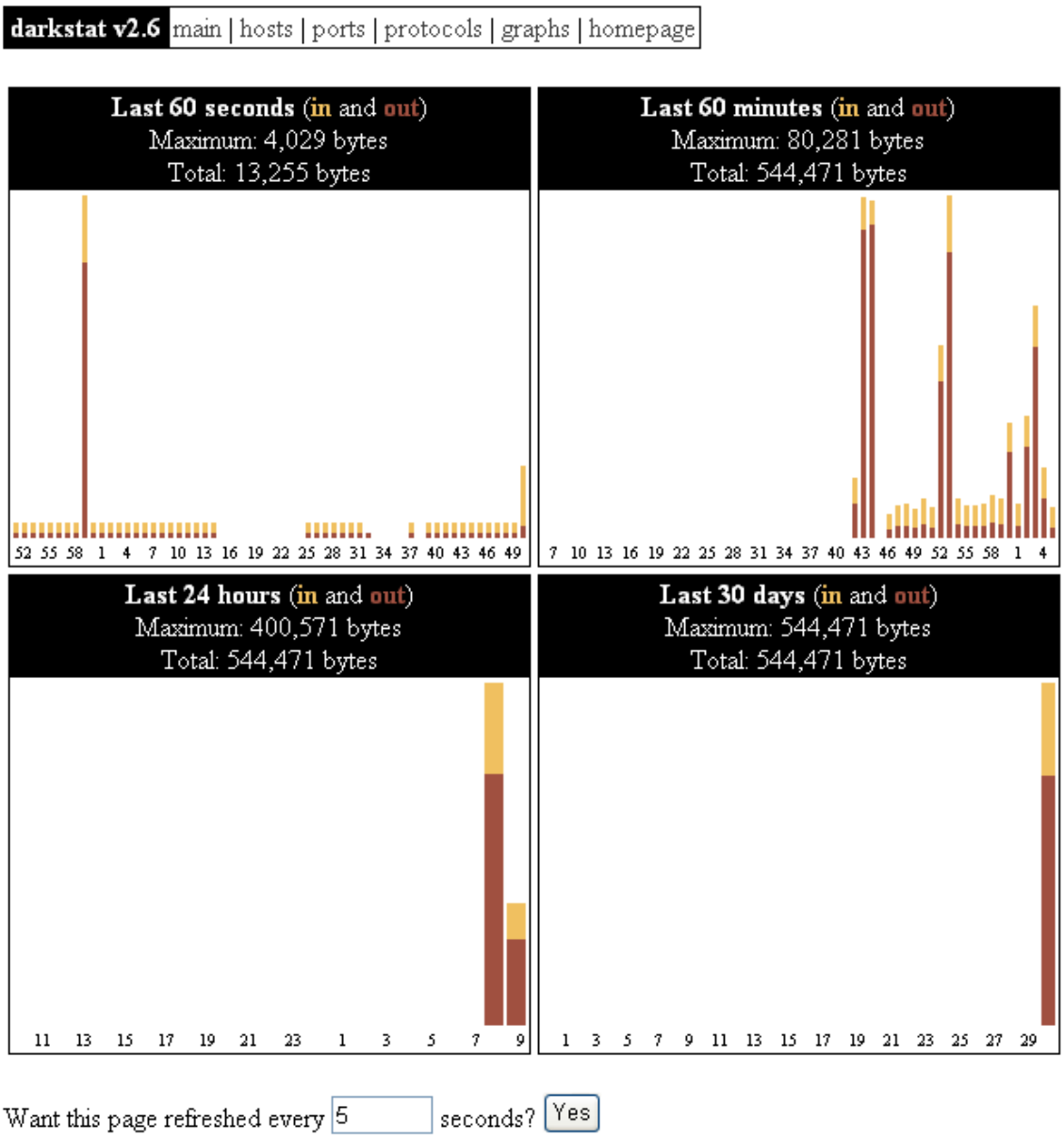

Figure 13 – Darkstat screenshot

5 The PAN External Connectivity Prototype

This chapter describes the implementation of the PECP. This implementation is based on the ASPAN specification. The PECP implementation can be split up into two phases. The first phase had the objective of automatically connect a PAN to the Internet in a scenario where only a PoA was available, which meant that no dynamic was associated with the process. Also, in the first phase of this prototype, as only one PoA was available, the implementation did not consider any intelligent PoA selection mechanism. In a second phase, the main goal defined for the PECP was to give PANs the ability to dynamically self-manage their external connectivity, choosing always the best PoA available at each moment. The different parts of the PECP and their implementation details are described next. The PECP implementation can be divided into four main aspects: PAN external access detection; PoA management by the PAN master; IPv4/IPv6 network setup; Joining/Leaving of PAN devices with an external access. For better understanding, each main feature of the PECP is explained in a different section.

5.1 PAN External Access Detection

This is an essential feature of the PECP. The PECP is able to detect, at all times, if a new external access is available in any of the devices of the PAN – *new access detection*. When a new access is detected, specific information about the external link is gathered. The information is sent to the PAN master and used to manage the PoA of the PAN (this is explained in Section 5.1.2). The PECP is also able to detect when the external access in a PAN device is no more available and inform the PAN master about this change – *access unavailability detection*. The *new access detection* and the *access unavailability detection* are mechanisms implemented in a similar way. Both use the routing table of the OS and check whether there are changes in the external connectivity status of the device. The routing table can be checked with the use of the route command described in the previous chapter and uses flags to identify the route type. The G flag indicates a route using a gateway. We can see whether a link is working as gateway by analysing the correspondent flag in the table. An "UG" flag is placed in front of the route which uses a gateway (The U flag means the route is up). The OS automatically updates the routing table of the system whenever a new link is available or loses availability. (Generally, the external access of the OS has only one gateway. This way, if a new gateway is available in the routing table, it means that the previous is no longer configured. It is possible to have more than one gateway, but that usually involves manual configuration.) Therefore, if a new gateway-flagged address appears in the routing table, it means that a new external access is available. In the same way, if a known gateway address is not present in the table, it means that the access is no longer available. This procedure is employed in the same way for both IP versions.

5.2 PoA Management

This feature is restricted to the PAN master. Accordingly to the ASPAN solution, the PAN master is the only device with knowledge about all the external accesses available for the PAN at each moment and therefore, the only device who can manage the PoA of the PAN. The master of the PAN keeps a record of the external accesses available in each PAN

device and maintains a database with all the necessary information for each of these external accesses. This information includes the category of the external access, which is a number used to distinguish the different external accesses based on the nominal throughout of their technology, and the IP address and the identification of the PAN device supporting the PoA. As stated in the previous section, the PAN master is immediately updated by its members, whenever a change happens in any of the PAN external accesses. This update is made through a Layer 2 message. This way, the master can always decide which the best PoA for the PAN is. If a change of PoA is necessary, the master informs all the PAN members through a Layer 2 message telling what they should do to reconfigure the new PAN external access. Currently, the DHCP protocol is the mechanism used to do this reconfiguration. The PAN members run the version of the DHCP client present in the Layer 2 message sent by the master. The PAN device supporting the new selected PoA is also informed by the PAN master of its new duties. The IP version aspects are better explained in the next section. Figure 14 shows an example of a *new access detection* in a PAN master and the PoA table kept by it.

```
(11:27:20) ## Interface eth0 with new IPv6 internet access: type 4 and GW IP: fe80:1234:5678::abcd
(11:27:20) ## NEW PoA available here! I am the MASTER: Checking PoA table...

----------------------------PoA TABLE----------------------------
| NETTYPE = 3 | NAME = laptop    | GATEWAY = 192.168.1.101        |
| NETTYPE = 4 | NAME = desktop   | GATEWAY = fe80:1234:5678::abcd |
-----------------------------------------------------------------
```

Figure 14 – *new IPv6 access detection* and PoA table example

5.3 IPv4/IPv6 Network Setup

The IP network setup of the PECP is available for both versions of the IP protocol. This section refers to the features available in the PECP that enable the creation of an IP network and that are supported by the ASPAN solution. The creation of an IP network for the PAN is made using the DHCP protocol described in Section 2.5.2.1 and assuming that an OSI Layer 2 network is already established beneath. DHCP is a stateful protocol where a device needs to act as a server. The PAN device chosen to run the DHCP server is always the one acting as PoA of the PAN or, if there is no PoA available, the master of the PAN. This allows easy distribution of the connectivity parameters within the PAN according to the current PoA and, thanks to the use of standard autoconfiguration mechanisms, support of legacy devices. The DHCP server launched by the PAN device supporting the PoA, and therefore the IP version used within the PAN, depends on the IP version used by the external access chosen as PoA for the PAN. If the PAN PoA changes, the new external access may have a different IP version. If this happens, the IP version used within the PAN changes to match the IP version used in the external access of the PoA. The decision to change the PANs PoA is made and announced by the PAN master as described in the previous section.

In the case of an IPv4 access, the PoA needs to perform NAT between the PAN and the external network (Internet) before it launches the DHCP server. This is made using the *iptables* command described in the previous chapter. The subnet used with IPv4 is the

10.0.0.0/24, which allows for 254 different addresses to be assigned to the PAN devices. If the PoA of the PAN changes and the device acting as server of the network also changes, a new DHCP server will be launched and new random addresses for the PAN devices would be generated. This new IP address generation is avoided through a mechanism that allows for the PAN devices to keep the same IP address, even when a change in the PAN PoA requires a renewal of the address – *"Same PAN IP" mechanism*. This mechanism is based on the *leases* that every device running a DHCP client (or server) has stored in a local file. If the PoA of the PAN changes and the device acting as server of the network also changes, a new DHCP server will be launched. If we can assure that the PAN devices acting as clients always request the same IP address to the DHCP server, and that the DHCP server has a clean lease file, the requested IP is always offered to the respective PAN device. Therefore, a random IP address is generated, by each PAN device, using the last four numbers of their MAC address to generate a random number between 0 and 254. This number is then used as the last number of their IP address in the 10.0.0.0/24 subnet. This is the address they will request to the DHCP server, whenever an IP renewal is required, and the address they use for themselves when they are the ones acting as server.

IPv6 is a recent protocol and none or few ISPs provide IPv6-based connection to end clients. Therefore, it was more difficult to test correctly this part of the PECP implementation. These tests are addressed in the next chapter. If the PAN master selects an IPv6-based external access, some configuration differences should be referred. With IPv6, there is no need to have NAT between the external network and the PAN. Also, the mechanism that allows for the IP address of a PAN device to be always kept the same is not needed for IPv6 because the link-local addresses, which never change, can be used to communicate within the PAN. In this 6th version of the IP protocol, it is possible to have more than one address assigned to each interface. An address prefix is assigned to each subnet and the rest of the global address of each device is defined by the DHCPv6 server running on the PoA of the PAN. The PAN IPv6 subnet prefix used for testing was the 2000:1234::/64. In addition, although IPv4 is the default protocol to be used, it is possible to create an IPv6 PAN (if no IPv4-based external access is available) by introducing a *flag* when launching the software. (This was introduced mainly for testing, but can be used with other purpose.)

5.4 Joining/Leaving of PAN Devices with an External Access

Since the beginning, the PAN dynamism was one of the main goals of this work. This section talks about the dynamism obtained through the IP autoconfiguration of the PAN when: a new device arrives; a device leaves the network; a new external access becomes available; an external access is no more available.

The joining of devices is very simple from the PECP point of view. Since the OSI Layer 2 network is supposed to be created beforehand, the new PAN device just needs to obtain a valid IP to communicate with the other PAN members. This is once more done with the help of the DHCP protocol. When the new device arrives it receives a Layer 2 message from the PAN master telling it what to do. Two different situations are possible from the PECP perspective. Either the new device is assigned as the new PAN master or it is told, by the

PAN master, to run the appropriate version of the DHCP client allowing it to obtain a valid PAN IP and, if available, the PoA address for PAN external access. If the joining device is assigned as the new PAN master, all the necessary information is transferred from the former master to it, including the PAN PoA database. Thus, the new master has everything it needs to decide which the next PAN PoA is, by using the process described in Section 5.1.2. Also, if the arriving device has already an external connection available when he joins the PAN but it is not declared as new master (this may happen if, for instance, a better connection is already available in the PAN when the new device joins), an update message, with the external access information, is sent to the PAN master as described in Section 5.1.2.

Although the ASPAN solution proposes different mechanisms to detect that a device has left the PAN, the mechanism considered here is that in which the device informs the master before he leaves the PAN. From the PECP perspective, this is only needed if the device that is leaving had an external access. If that is the case, a Layer 2 message is sent to the PAN master, removing the corresponding PoA database entry. If the leaving device is the PAN master device, the same procedure used for the joining of a new master is used. Before leaving, a new master is assigned and the PAN PoA database is sent to it. Thus, the new master is ready to run the PAN and its PoA.

From the PECP point of view, the pure joining or leaving of devices does not involve reconfiguration of the PAN unless the PAN master or PAN PoA changes.

It is also possible for legacy devices to "join" and "leave" the PAN. They can connect and communicate in the IP Layer only though. If somehow they connect themselves to a PAN member in a lower level (with an Ethernet cable for instance) and run a DHCP client, they will be granted access to the other PAN devices and to the PAN PoA currently in use.

In this chapter, the work carried out in the implementation of the PECP was explained in detail. The different PECP features described allow for the dynamic and automatic connection of PANs to external networks and are, therefore, of great importance for the content of this work.

6 Work Evaluation

A set of tests have been made in order to evaluate the PECP presented in Chapter 5. In this chapter, those tests and their results are presented. The ASPAN prototype tested was a conjunction of the PECP and a prototype made by João Maia which deals with the interconnection of PAN devices and the creation of one logical link as specified by the ASPAN solution. Nonetheless, some specific tests have been made, concerning mainly the PECP. The results presented herein try to evaluate the PAN performance when IP configuration is needed due to the joining/leaving of devices or when a new external access becomes available. Throughput measurements have also been made in order to evaluate the Internet connection performance of the devices within a PAN.

6.1 Test#1 - PAN Reconfiguration due to a Joining Device

Some PAN scenarios have been set which consider the arriving of new devices. This was done to evaluate the IP configuration time of a joining device, namely the time it needs to acquire an IP Layer address that allows it to communicate with the PAN PoA and therefore, the Internet. The scenarios involve Bluetooth and Wi-Fi technologies, an Internet Access and four PAN devices. The next table shows the characteristics of the possible PAN devices emulated by laptops in our tests.

Table 1 – Test#1: Device characteristics

PAN Device	Internet Access	Available Interfaces for PAN
Desktop	IPv4	Bluetooth
Laptop	No	Bluetooth and Wi-Fi
PDA	No	Wi-Fi
Mobile Phone	No	Bluetooth

The next figures show the three different PAN scenarios tested. All of them involve IPv4 Internet access through the "Desktop".

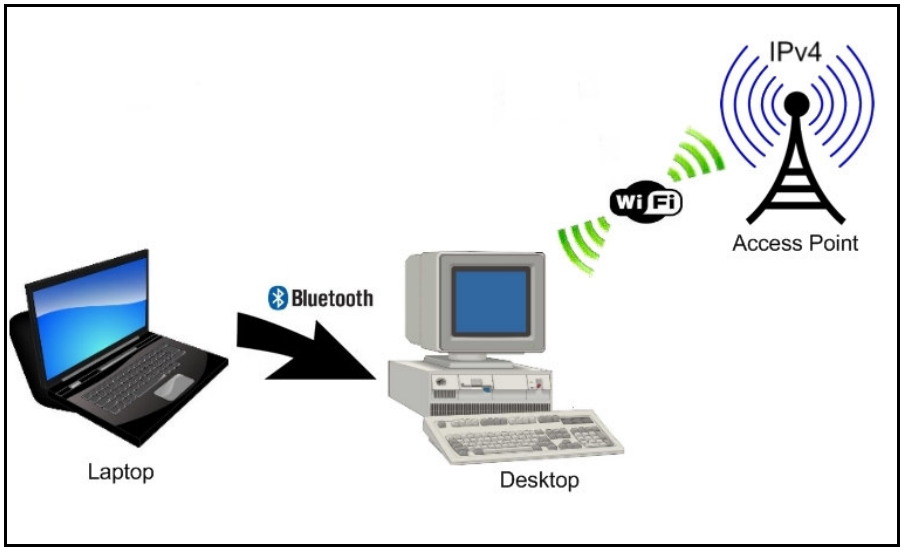

Figure 15 – 2nd PAN device connects using Bluetooth

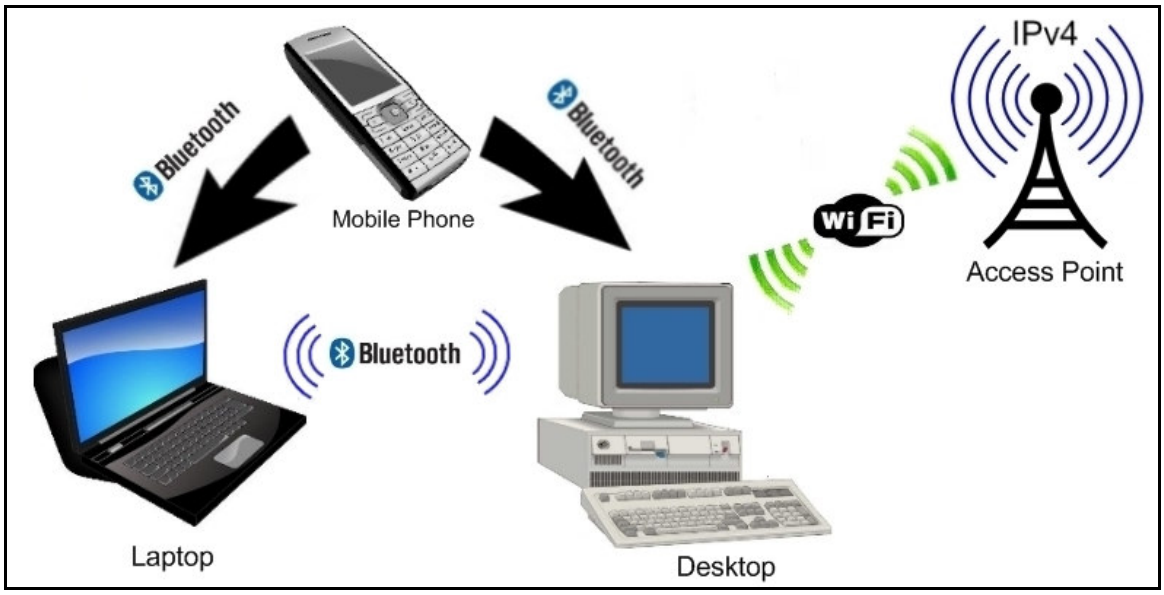

Figure 16 – 3rd PAN device joins using Bluetooth

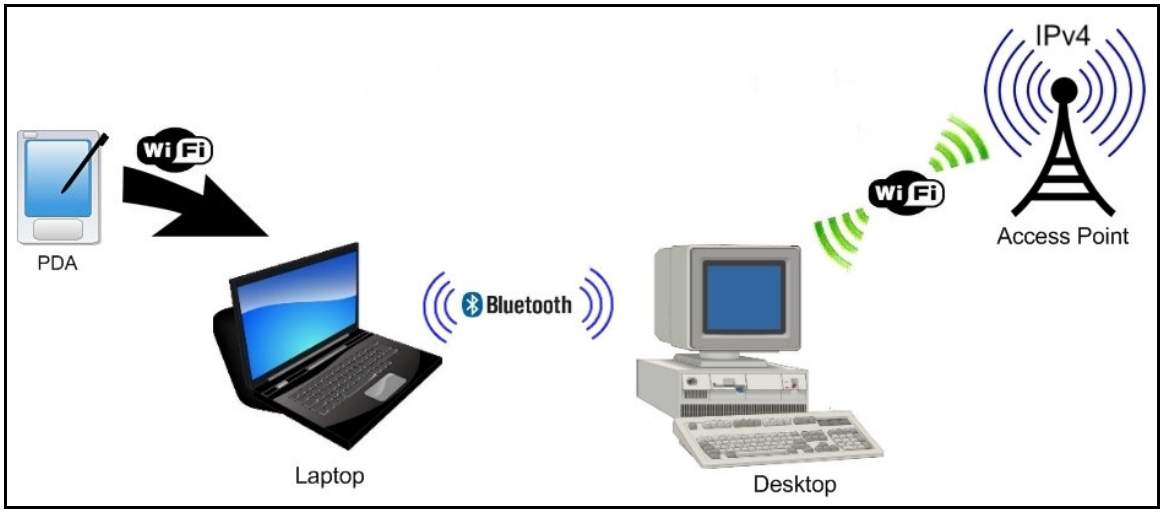

Figure 17 – 3rd PAN device joins using Wi-Fi

In Figure 15 we can see the scenario used to test the formation of the PAN with two devices. The figure shows the Laptop connecting to the Desktop using Bluetooth technology. Before this happens, there was no PAN created because there was only one device, the desktop. This scenario evaluates the arriving of a second device to the PAN. In both Figures 16 and 17, we can see the scenarios used to test the joining of a third device to the PAN. Figure 16 shows the joining of the Mobile Phone using Bluetooth technology and connecting to both PAN members, as both possess that technology. Figure 17 shows the joining of the PDA using Wi-Fi technology and connecting to the Laptop, which is the only device with that technology available for the PAN.

These tests intend to evaluate the IP configuration time of a joining device in different aspects: joining of a second member; joining of a third member using a different technology; joining of a third member using the same communication technology. The next figures show

the obtained results. The tables with the values used to create the graphics are presented in Annex A.

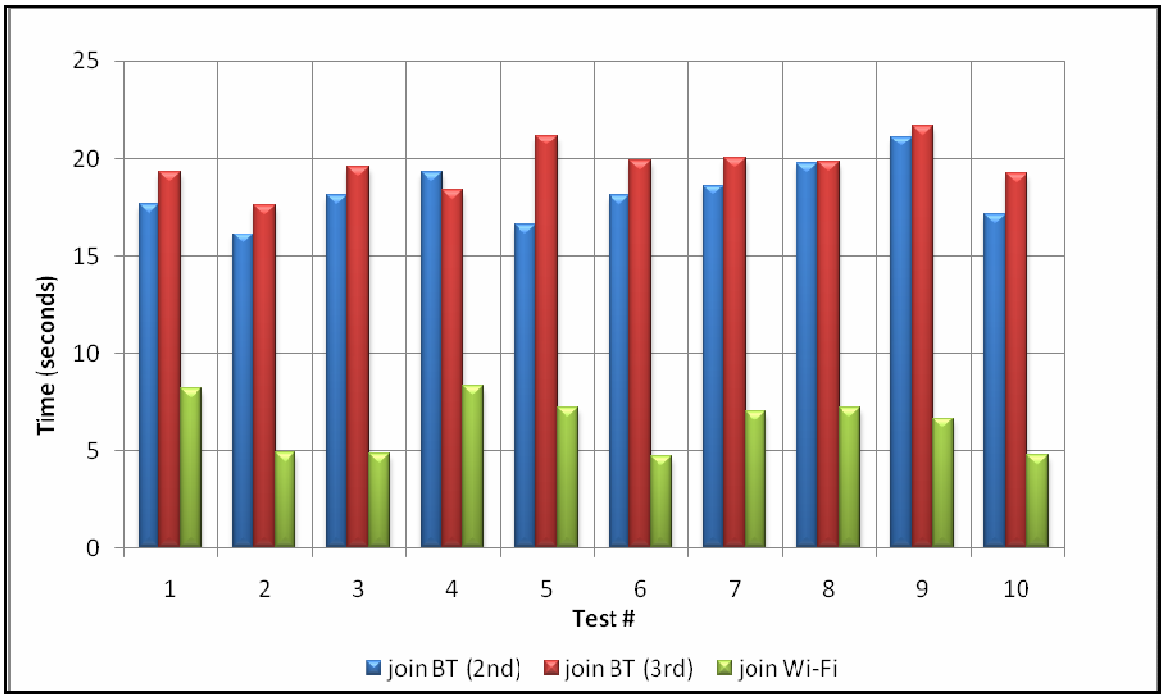

Figure 18 – PAN total configuration times

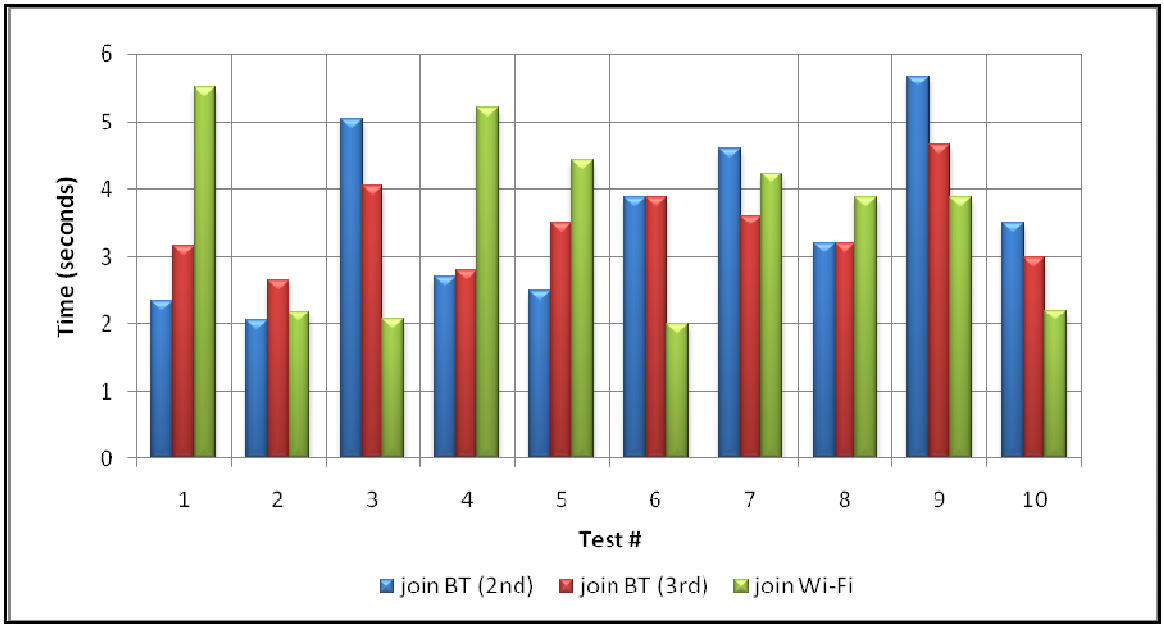

Figure 19 – LINUX *dhclient* times

Figure 18 shows the PAN reconfiguration times tested 10 times for each scenario. The blue and red bars show, respectively, the total PAN configuration times for the joining of a second and a third member using Bluetooth technology. The green bar shows the configuration time for the joining of a third PAN member using Wi-Fi technology. These times were measured since the joining device starts the software until it obtains a valid PAN

IP address and is ready to communicate with the PAN PoA and, as such, the Internet. We are interested in the IP configuration time of the joining device. We should take into account that the tests were made in an area filled with wireless connections and that these are global reconfiguration times, which means that some necessary technology aspects (like Bluetooth and Wi-Fi device scanning and association) are included. These aspects are independent from this software and are not related to the PECP.

Figure 19 shows the fraction of the times of Figure 18 that concerns to the *dhclient* process. From the IP Layer point of view, the evaluation of these test scenarios can be made by analyzing the time spent using the LINUX *dhclient* program to acquire a valid IP from the DHCP server on the PAN. From the results present in Figure 19 we can see that the *dhclient* times do not follow any pattern for the scenarios presented. The times are random and do not depend on the number of members forming the PAN or the technology used by the joining device.

Considering the results presented, we can say that the PAN reconfiguration time due to the arriving of a new device, including the IP Layer configuration, is usually not more than 20s. However, only less than 1s of that time is due to software processing (see Annex A). This means that less than 5% of the PAN reconfiguration time is due to the protocol implemented in this ASPAN prototype and that the majority of the time is spent in technology dependent aspects and in acquiring an IP address using the LINUX *dhclient*.

6.2 Test#2 - Joining/Leaving of the PAN Master and PoA

The next PAN scenario intends to test the arrival and leaving of a device with a better external access. As such, the PAN reconfiguration time due to the change in its PoA is evaluated. Although this is not in the ASPAN specification, the main criteria to elect the PAN master was the external access category. This way, this test also considers changes of the PAN master and therefore of the PAN topology. This is a global test of the ASPAN prototype dynamics. The scenario involves Ethernet, Bluetooth and Wi-Fi technologies, two different Internet Accesses and four PAN devices. The next table shows the characteristics of the PAN devices emulated by laptops in our tests.

Table 2 – Test#2: Device characteristics

PAN Device	Internet Access	Available Interfaces for PAN
Desktop	No	Ethernet, Bluetooth and Wi-Fi
Laptop A	No	Ethernet
Laptop B	IPv4	Wi-Fi
PDA	IPv4	Bluetooth

The next figures show the PAN scenario tested. The scenario involves two IPv4 Internet accesses: one through the "PDA" and other through the joining Laptop B.

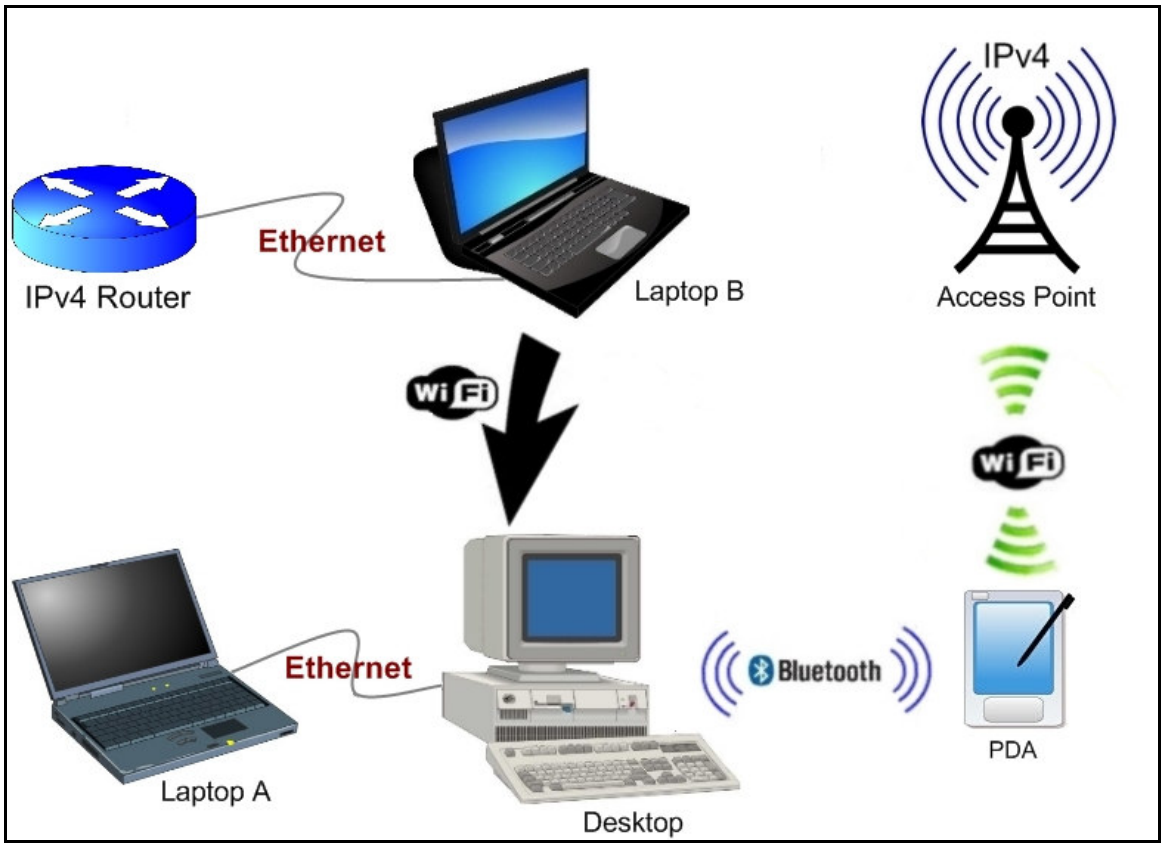

Figure 20 – Arrival of new PoA and new PAN Master using Wi-Fi

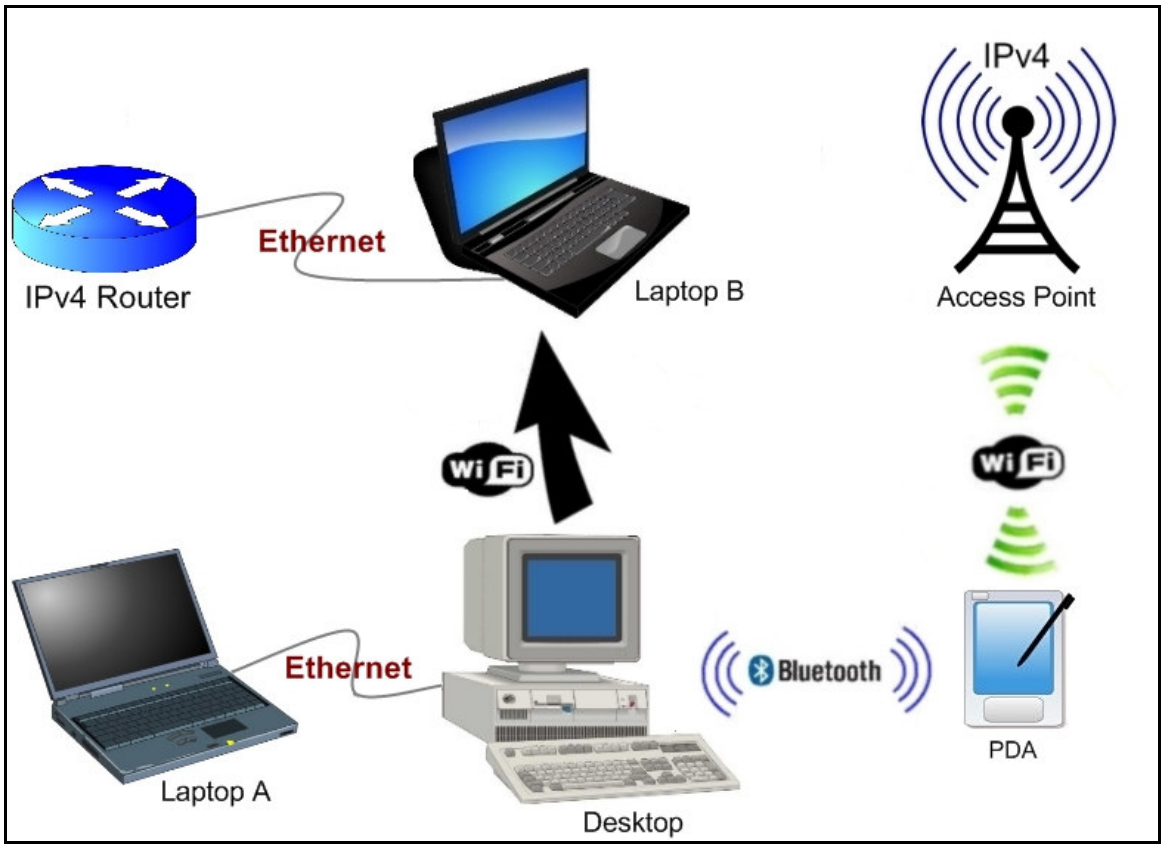

Figure 21 – Leaving of PoA and PAN Master using Wi-Fi

Figure 20 shows the scenario used to test the arrival of a new device with a new PoA to the PAN. The figure shows Laptop B connecting to the Desktop using Wi-Fi technology. This scenario implies a PAN reconfiguration. Before the arrival of Laptop B to the PAN, PDA was the PAN master due to its external access. After the arrival of Laptop B and its better external access (in theory, an Ethernet access is better than a Wi-Fi access), the PAN reconfigures itself automatically and nominates the joining Laptop B as new master and PoA for the PAN. Figure 21 shows exactly the inverse scenario. Laptop B, which is the master and the PoA of the PAN, leaves the network and this fact starts a PAN reconfiguration process which leads to the nomination of the PDA as new PAN master and PoA.

These tests intend to evaluate the PAN reconfiguration time in different aspects: arriving of a new PAN master with a new and better PoA for the PAN; leaving of the PAN master and PoA of the PAN. The next figure shows the obtained results. The tables with the values used to create the graphic are presented in Annex B.

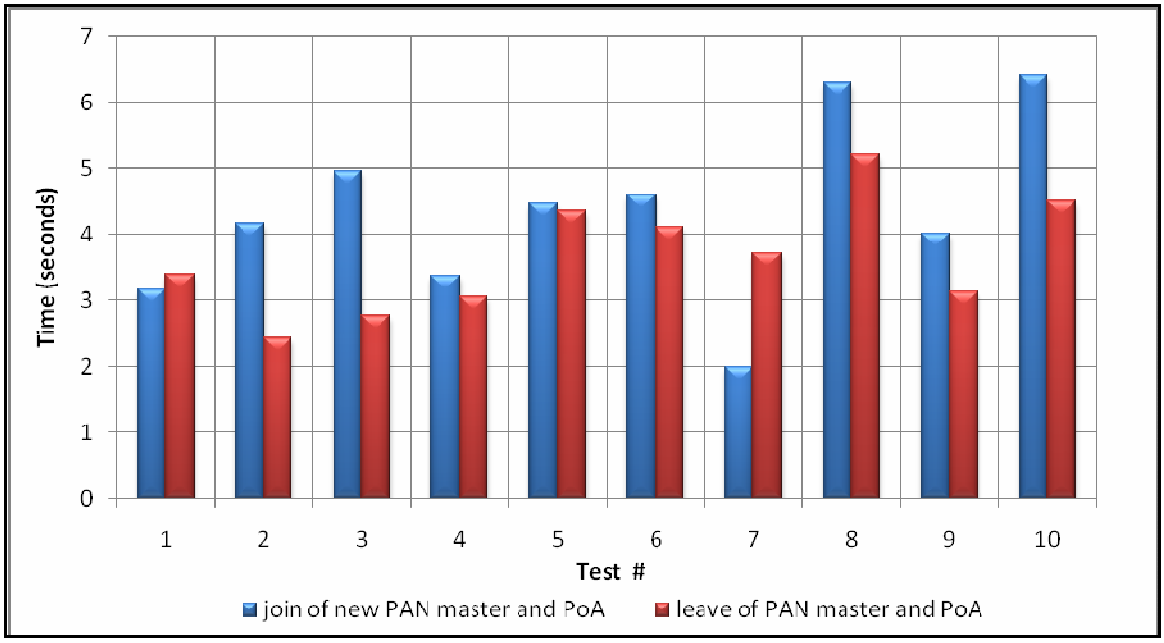

Figure 22 – Reconfiguration time due to a join/leave of PAN master and PoA

Figure 22 shows the reconfiguration time considering 10 tests made for this scenario. The blue bars in the graph show the PAN reconfiguration time for the joining of a new master and PoA for the PAN, while the red bars show the time needed for the PAN to reconfigure upon the leaving of its master and PoA. These times were measured since Laptop B device sends its first Layer 2 message to the PAN and until the PAN is stabilized and every member has a valid PAN IP address and is therefore ready to communicate with the Internet through the PAN PoA. We should notice that Test#2 is made in a different way than Test#1 because the objective here is to measure the time the PAN is actually reconfiguring and not the time the whole process of joining of devices takes. Nevertheless, the values measured here include the time spent running the LINUX *dhclient* program, used to acquire the IP address from the device supporting the new PoA (which runs the DHCP server).

From these results we can see that the leaving of the master and PoA of the PAN is usually a bit faster than the joining counterpart. This is due to the fact that there are fewer messages exchanged when the master leaves (and therefore less message processing). The next figure shows the time a PAN member spent running the *dhclient* program to obtain an IP address from the DHCP server in the PAN.

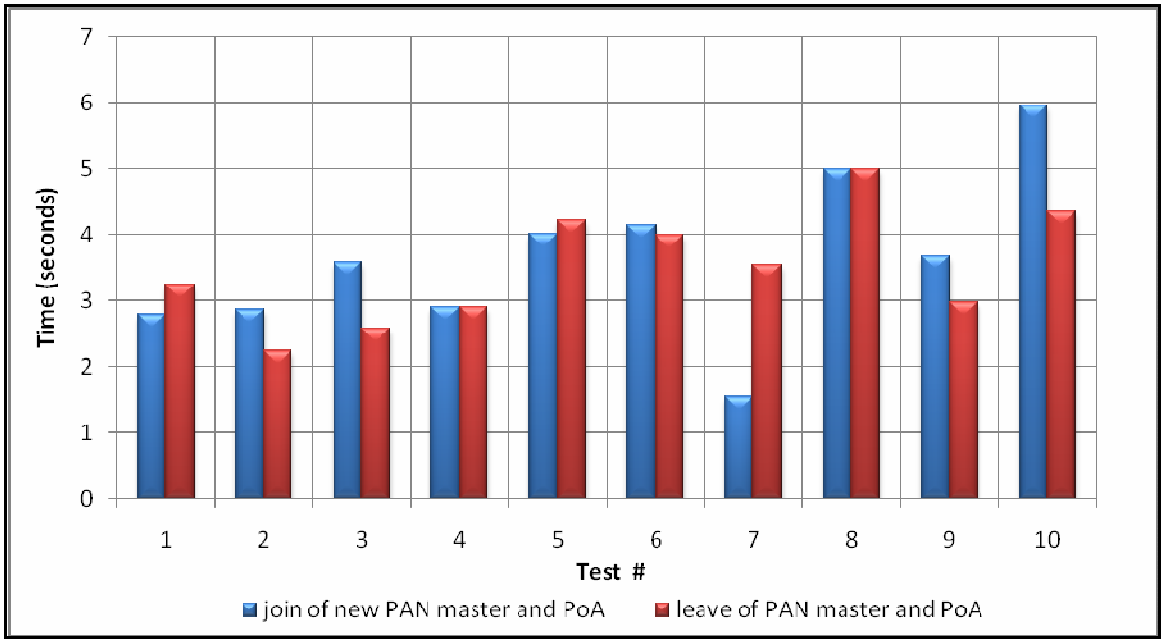

Figure 23 – LINUX *dhclient* times

Figure 23 shows the fraction of the times of Figure 22 that concern to the *dhclient* process. By comparing both figures, we can see that a large part of the PAN reconfiguration time in this scenario is due to the autoconfiguration mechanism used. Moreover, the oscillations verified are also due to the DHCP process.

In conclusion, the leaving of a PAN master is faster than the joining. In this test scenario, the PAN reconfiguration time, from the PAN members point of view, takes less than 7 seconds, in the worst case. This means that, the period of time between the moment a PAN member loses its Internet access until it regains external connectivity again, is less than 7s in the worst case scenario (new PAN master arrival).

6.3 Test#3 - PAN PoA Setup due to New External Access

Two PAN scenarios have been set for testing the changing of the PAN PoA. This can happen due to one of three things: 1) a PAN is without external connectivity and an external access becomes available; 2) a better external access becomes available to the PAN; 3) the PoA that is in use becomes unavailable and the PAN reconfigures to use the second best external access. The first option was considered in the tests reported below. The scenarios involve Bluetooth and Wi-Fi technologies, an Internet access and three PAN devices. In the first test scenario, an IPv4 Internet access is used, while in the second test scenario an IPv6 Internet access is considered. These tests use exclusively the PECP. The next table shows the characteristics of the PAN devices emulated by laptops in our tests.

Table 3 – Test#3: Device characteristics

PAN Device	Internet Access	Available Interfaces for PAN
Desktop	No	Ethernet, Bluetooth
Laptop	No	Ethernet
PDA	Connecting	Bluetooth

The next figure shows the scenario used to test the PAN PoA autoconfiguration time when a new external access becomes available to one of its devices.

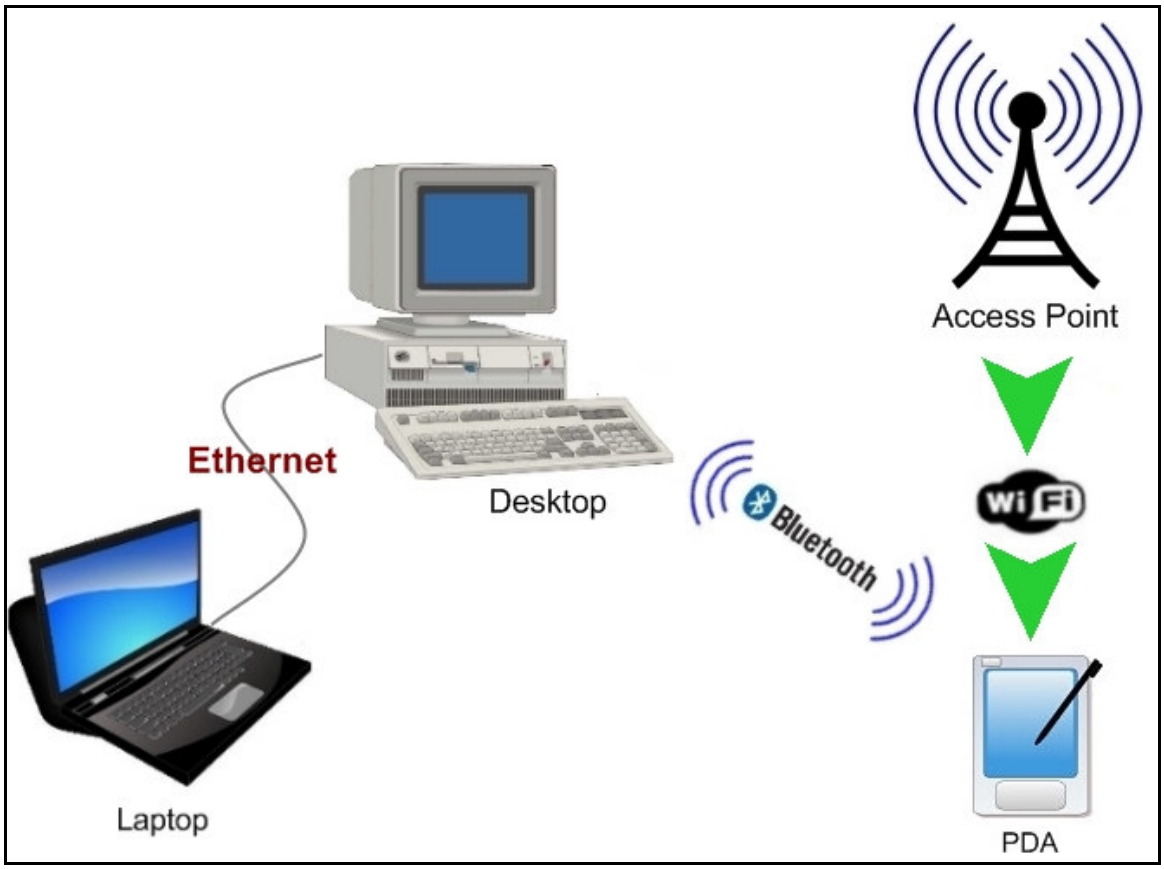

Figure 24 – New External Access Connection

Figure 24 shows a PAN composed by a Laptop, a Desktop, and a PDA, in which the PAN master is the Desktop. When the PDA establishes a connection to an external access with its Wi-Fi interface, the PAN master is notified and starts the process (described in Chapter 5) that enables the PDA to become the PAN PoA. This test intends to evaluate the time the PAN takes to automatically setup its new PoA when: 1) a new IPv4 external access becomes available; 2) a new IPv6 external access becomes available. The next figure shows the obtained results. The tables with the values used to create the graphic are presented in Annex B.

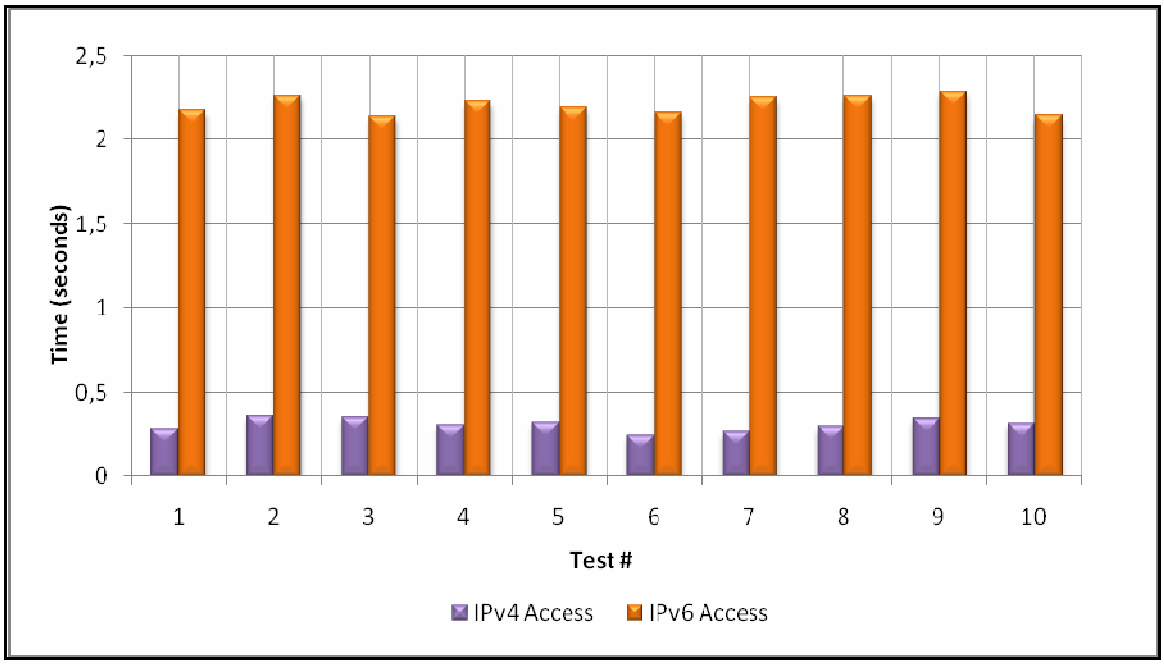

Figure 25 – PoA setup time - IPv4 vs IPv6

Figure 25 shows the results of Test#3. The purple bars in the graph show the PAN PoA setup time when an IPv4 external access is detected by a PAN member, while the orange bars show the same thing but for an IPv6 access. IPv6 access is emulated by an OS command that introduces an IPv6 gateway route in the routing table, allowing the software to detect and assume that as a new IPv6 external access. The times shown in Figure 25 are measured from the moment the PDA detects the new external access until it configures the respective version of the DHCP server (and the NAT mechanism for IPv4) and becomes the PANs PoA.

Test#3 proves that the PoA setup time due to a new IPv4 external access takes just a few hundred milliseconds. In addition, the test shows a big difference between the setup time of an IPv6 external access compared to an IPv4 external access. This is due to the longer time needed for a DHCPv6 server to start compared to an IPv4 server (see Annex C). Test#3 scenario shows the arrival of a new external access to a PAN device. If we consider a scenario where a better IPv4 (or IPv6) external access becomes available after a PAN PoA is already configured, the steps and the times would be almost the same as in this Test#3 scenario. This means that the arriving of a PoA to the PAN is dealt in the same way than the changing of the PAN PoA due to a new and better external access or even the changing to a second best PoA due to the unavailability of the best PoA.

Therefore, we can say that a change in a PANs PoA takes no more than 400ms for an IPv4-based access and less than 2,4s for an IPv6-based access (using Dibbler, see Section 4.2.2). Moreover, the time a PAN member takes to reconfigure for a new PoA is about the times referred, plus the time of a *dhclient*.

6.4 Test#4 - PAN Links Throughput

This test was made to evaluate the capacity of the links in a PAN using the ASPAN prototype. A scenario was set to measure the throughputs of the PAN members to the Internet. This test was made with the help of Darkstat (see Section 4.2.3). The scenario considers the following technologies within the PAN: Ethernet, Bluetooth and Wi-Fi. The Internet access used was IPv4-based with a bandwidth greater than 11Mbit/s, which is the bandwidth of the Wi-Fi link used in the PAN (802.11b). The next table shows the characteristics of the possible PAN devices emulated by laptops in our tests.

Table 4 – Test#4: Device Charecteristics

PAN Device	Internet Access	Available Interfaces for PAN
Laptop A	Yes	Bluetooth
Laptop B	No	Bluetooth,Wi-Fi
PDA	No	Wi-Fi

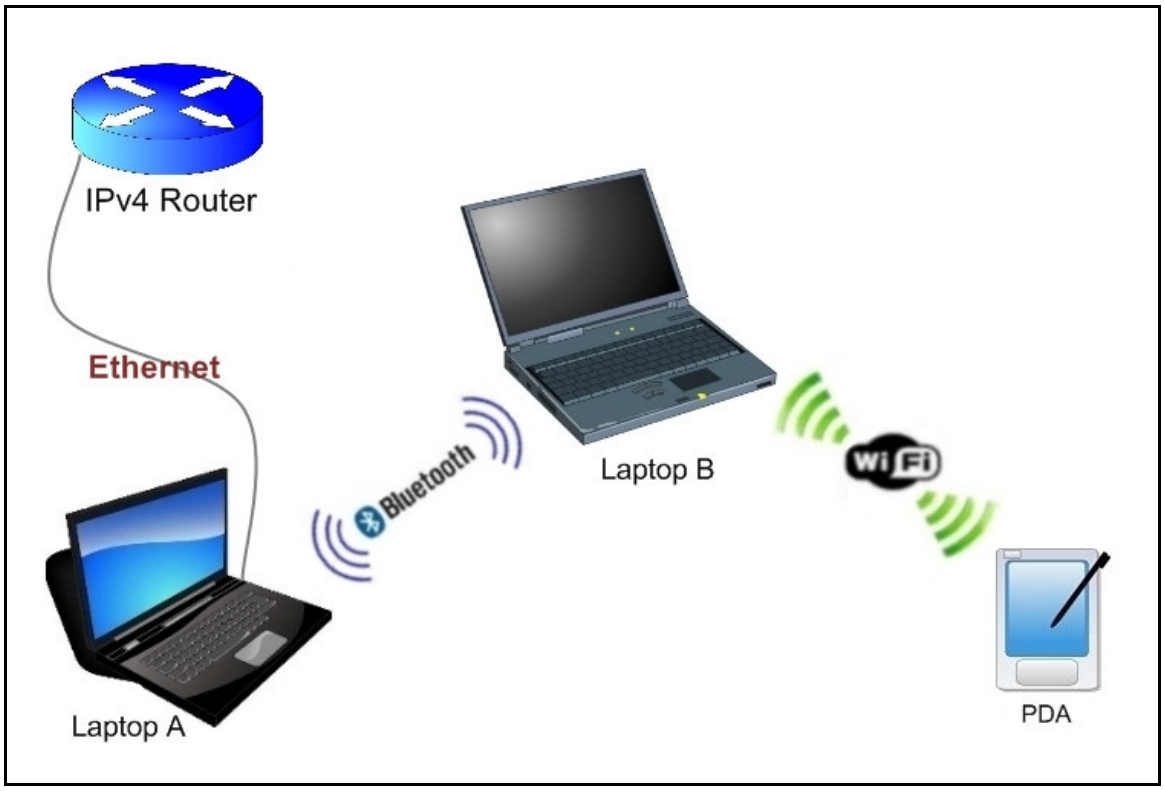

Figure 26 – Scenario used to measure throughput

Figure 26 shows the scenario used to test the PAN devices Internet throughput. The figure shows a PAN composed by a Desktop, two Laptops and a PDA, in which Laptop A is supporting the PoA of the PAN. The throughput tests were made by downloading a big file from the Web to Laptop B and then to the PDA (and also to Laptop A for comparison purposes) and by checking the bytes downloaded with the help of Darkstat. The next table shows the results obtained with these tests.

Table 5 – Throughput results

Internet Access Throughput	Technologies Used	Kbytes/s
From Laptop A	Ethernet	4549,64
From Laptop B	Ethernet + Bluetooth	35,36
From the PDA	Ethernet + Bluetooth + Wi-Fi	35,21

Table 5 shows the throughput results obtained with Darkstat. In the table we can see that throughput is decreasing as the path to the PoA becomes longer, as expected. The results of Table 5 show a somewhat poor performance of the Bluetooth link.

6.5 Discussion

By analysing the results obtained in this chapter, we can see that the time spent with technology dependent aspects and the IP autoconfiguration mechanism used occupy most of the PAN reconfiguration times in every scenario tested. The Test#1 results show that the Bluetooth scanning and association time are the main time consuming factors when reconfiguring a PAN due to the arriving of a new device. However, Test#2 shows that, if we only consider the time it takes for a PAN to reconfigure in the worst case (arriving of a new PAN master and PoA), the process that needs more time is the IP address renewal using the DHCP mechanism. This process is essential because it allows the PAN devices to have external access through the new PAN PoA. Also, Test#3 shows that if a PAN is established at Layer 2 and it needs an IP reconfiguration due to a new external access that became available, the most time consuming process is again related with the autoconfiguration mechanism used. The time of a DHCP server configuration, especially in an IPv6-based scenario, is the main factor for the results obtained when testing the PAN PoA setup time due to a new external access. In addition, the results of Test#3 show that the changing of a PAN PoA, from a PAN member point of view, is a fast process which depends mainly of the autoconfiguration mechanism used.

In the last test, the throughput results obtained show, as expected, that Bluetooth was the bottleneck technology used in the test scenario. The somewhat low throughputs obtained are probably due to packet loss in Bluetooth given the "noisy" environment where the tests were performed.

The leaving of PAN devices was also tested but was not included herein because it was almost instantaneous (the leaving device just needs to inform the PAN master of its departure). Tests showed an 8ms time for the master to become aware of this event.

In conclusion, the tests presented in this chapter allow for the verification of the ASPAN prototype, and the PECP in particular, in accordance with the specification. The PAN reconfiguration times were all less than twenty seconds and are considered reasonable. The ASPAN PCP used is a viable protocol for communication between PAN devices. Also, the throughput results obtained show good stability and speed in the PAN links.

7 Conclusions

With this work, we were able to conclude that the ASPAN framework establishes a base for the deployment of next generation PANs, in which connectivity to the Internet will be a must. Namely, we concluded that the ASPAN framework makes the PoA reconfiguration within a PAN, the PoA management, and its intelligent selection an agile and fast process. The DHCP protocol proved to be a good autoconfiguration mechanism to setup an IP network within a PAN and allow the PAN PoA to share its Internet access with every PAN device. Also, the creation of an IP network, for both IPv4 and IPv6, was considered a smooth and easy process using DHCP. The NAT mechanism was considered a valid tool in the configuration of an IPv4-based external access for a PAN. With the results obtained in various test scenarios, we managed to conclude that the reconfiguration times of a PAN (less than 20s) are reasonable and acceptable. Moreover, we concluded that the technology of the external access used in the PAN is the main factor for the limit of the external links throughput of the PAN devices.

In the following sections a work revision is presented and the objectives of the work as well as the relevant results are recalled. In the last section we refer the future work.

7.1 Work Revision

With this work, as initially intended, a next generation PAN External Connectivity Prototype (PECP) was created. The work started, in a first phase, by implementing the autoconfiguration of a PoA for the PAN considering that a single possible external access was available; in a second phase, we extended the prototype to deal with the availability of multiple PAN external accesses. In order to achieve this result some sub-objectives were defined: 1) creation and management of an IP network within a PAN; 2) management of the PoA to the Internet available at each moment; 3) automatic and dynamic connection to the Internet, through the best PoA; 4) support for both IPv4 and IPv6 Internet connectivity.

All the objectives proposed were achieved.

The PECP shows a new way of Internet use, targeting the users increasing need of constant Internet connectivity.

7.2 Relevant Results

In this section, the main results obtained during this work are briefly explained. For the sake of clearness, a different section is used for each result.

7.2.1 PAN External Connectivity Prototype

The PECP was the main objective achieved with this work. This is a prototype based in the ASPAN solution proposed by Campos and Ricardo and addresses the management and autoconfiguration of PANs external connectivity. Its main features are described in the next sections.

7.2.1.1 Creation and Management of an IP Network inside a PAN

Considering that a Layer 2 network is set up and a connection between the PAN devices is established, an IP network is created allowing communication between the PAN devices at a higher level. The DHCP protocol is used here as the IP autoconfiguration mechanism. This feature also includes mechanisms that deal with the "joining" and "leaving" of devices to the PAN at the IP level.

7.2.1.2 Automatic and Dynamic Connection to External Networks

This feature allows the PECP to automatically connect to external networks whenever they become available in one of the PAN devices. The best PAN external access (e.g.: to the Internet) is chosen and the PAN is reconfigured to use it, by exchanging Layer 2 messages between the PAN members.

7.2.1.3 "Same PAN IP" Mechanism

The "Same PAN IP" is a mechanism that enables the PAN devices to keep the same IP address even when the PAN PoA changes and a new DHCP server is launched. This mechanism is based on the lease files of the DHCP protocol and allows for intra-PAN communication to remain intact if only the PAN external connections need to be reconfigured.

7.2.1.4 Management of the External Links Available

The PCP of the ASPAN solution elects a PAN master device, which is responsible for managing the network. This includes the management of the PoA available, at each moment, and their characteristics. The other PAN devices inform the PAN master whenever a new external access becomes available or a PoA becomes inactive. This way, the PAN master is the only device who always knows which the best PoA for the PAN is.

7.2.1.5 IPv6 Support

The PECP has support for the new IP version 6. A device of the PAN can detect an IPv6-based external access and become the PoA of the PAN following the same steps as an IPv4-based access. With the use of the DHCPv6 protocol, the PAN devices can obtain the information they need about the IPv6-based external access and connect to the external network. This feature allows for a better integration of the PECP with the NGNs.

7.3 Future Work

The PECP may be used as base for future development in this area. With possible improvements to this prototype in mind, some new features are suggested to improve its applicability and performance. Those are pointed out in the next sections.

7.3.1 Multiple Simultaneous PAN External Accesses

This ASPAN prototype only allows a PoA for the PAN at each moment. One possible improvement to the PECP is to enable the configuration of more than one PAN PoA allowing simultaneous external connectivity to the PAN members.

7.3.2 Other IP Autoconfiguration Mechanisms

Besides the DHCP protocol used in the PECP, there are other autoconfiguration mechanisms that allow the creation of an IP network. With the NGNs in mind, future solutions may be developed in this area. This prototype could include other ways of setting up an IP network which allow the PAN PoA to share its Internet connectivity.

7.3.3 IP Autoconfiguration Mechanism Intelligent Selection

If other IP autoconfiguration mechanisms were included in this prototype, a way of selecting the best mechanism could also be implemented. Considering the external IP connectivity used by the current PoA, the best autoconfiguration mechanism could be selected to distribute the IPv4 or IPv6 addresses within the PAN.

References

[1] Bluetooth SIG, *Specification of the Bluetooth System (version 2.0)*, November 2004.

[2] ANSI/IEEE Std 802.11, Part 11: *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 1999 Edition (R2003)

[3] Standard ECMA-368, *High Rate Ultra Wideband PHY and MAC Standard*, December 2005

[4] Standard ECMA-369, *MAC-PHY Interface for ECMA-368*, December 2005

[5] M. Takizawa, et al., *MaCC: Supporting Network Formation and Routing in Wireless Personal Area Networks*, in Proceedings of the 18th International Conference on Advanced Information Networking and Application (AINA'04), March 2004

[6] R. Campos and M. Ricardo, *Autoconfiguration and Selfmanagement of Personal Area Networks: a New Framework*, in Proceedings of the 15th Meeting of the Wireless World Research Forum, December, 2005

[7] R. Wakikawa, et al. *Global connectivity for IPv6 Mobile Ad Hoc Networks,* Internet Draft, draft-wakikawa-manetglobalv6-05 (work in progress), March 2006

[8] R. Campos and M.Ricardo. *Dynamic and Automatic Connection of Personal Area Networks to the Global Internet*.

[9] T. G. Zimmerman, *Personal Area Networks: Near-field intrabody communication*, MIT Media Lab, April 1996

[10] The Independent European Centre for RFID, *Wireless and Mobility: Wireless Standards*, Figure available at http://www.rfidc.com/docs/introductiontowireless_standards.htm.

[11] IEEE Workgroup 802.15.1, *Personal Area Networking (PAN) Profile*, June 2001.

[12] Intel Corporation, Intel's UWB vision, Ultra-Wideband (UWB) Technology, Figure available at http://www.intel.com/technology/comms/uwb/index.htm.

[13] More information available at http://www.zeroconf.org.

[14] S. Thomson, et al., *IPv6 Stateless Address Autoconfiguration*, RFC 2462, December 1998.

[15] T. Narten, et al., *Neighbour Discovery for IP version 6 (IPv6)*, RFC 2461, December 1998.

[16] R. Droms, *Dynamic Host Configuration Protocol*, March 1997

[17] B. Croft, John Gilmore, *Bootstrap Protocol (BOOTP)*, September 1985

[18] K. Weniger, et al., *Address Autoconfiguration in Mobile Ad Hoc Networks: Current Approaches and Future Directions*, IEEE Network, vol. 18, (August 2004), 6-11.

[19] K. Weniger, et al., *PACMAN: Passive Autoconfiguration for Mobile Ad Hoc Networks*, IEEE Journal on Selected Areas in Communications (JSAC) Special Issue 'Wireless Ad hoc Networks', March 2005

[20] Plummer, D., *An Ethernet Address Resolution Protocol* – RFC-826, November 1982

Annex A

Values obtained with the scenario of Test#1 represented in Figure 15.

Table A-6					
Test #	**Total time**	**BT scanning**	**BT panding**	***dhclient* time**	**Software Processing**
1	17,623	13,320	1,694	2,352	0,257
2	16,114	11,509	1,960	2,050	0,595
3	18,105	10,750	1,453	5,044	0,858
4	19,292	14,638	1,609	2,698	0,347
5	16,650	12,208	1,552	2,485	0,405
6	18,107	11,531	2,253	3,879	0,444
7	18,582	11,932	1,621	4,594	0,435
8	19,759	14,177	1,945	3,205	0,432
9	21,090	13,466	1,535	5,676	0,413
10	17,128	11,610	1,624	3,495	0,399
Medium Values	18,245	12,514	1,725	3,548	0,459

Values obtained with the scenario of Test#1 represented in Figure 16.

Table A-7					
Test #	**Total time**	**BT scanning**	**BT panding**	***dhclient* time**	**Software Processing**
1	19,310	12,570	3,152	3,152	0,436
2	17,569	11,840	2,614	2,650	0,465
3	19,559	12,066	3,065	4,044	0,384
4	18,360	11,680	3,479	2,798	0,403
5	21,181	13,736	3,619	3,485	0,341
6	19,876	12,432	3,212	3,879	0,353
7	20,033	13,121	2,865	3,594	0,453
8	19,826	12,545	3,533	3,205	0,543
9	21,670	13,523	3,123	4,656	0,368
10	19,274	12,324	3,543	2,995	0,412
Medium Values	19,666	12,584	3,221	3,446	0,416

Values obtained with the scenario of Test#1 represented in Figure 17.

Table A-8					
Test #	**Total time**	**Wi-Fi Scanning**	**Acquiring Cell**	***dhclient* time**	**Software Processing**
1	8,170	0,258	1,695	5,502	0,715
2	4,879	0,375	1,950	2,183	0,371
3	4,848	0,259	2,153	2,071	0,365
4	8,292	0,375	1,923	5,207	0,787
5	7,180	0,379	1,925	4,435	0,441
6	4,707	0,263	2,142	1,988	0,314
7	7,044	0,260	1,949	4,237	0,598
8	7,200	0,369	2,135	3,885	0,811
9	6,628	0,260	2,135	3,885	0,348
10	4,747	0,259	1,950	2,202	0,336
Medium Values	6,370	0,306	1,996	3,560	0,509

Annex B

Values obtained with the scenario of Test#2 represented in Figure 20.

Table B-9			
Test #	**Total time(1)**	***dhclient* time**	**Software Processing**
1	3,160	2,791	0,369
2	4,156	2,858	1,298
3	4,959	3,570	1,389
4	3,374	2,904	0,470
5	4,474	4,005	0,469
6	4,606	4,142	0,464
7	1,985	1,543	0,442
8	6,299	4,991	1,308
9	4,022	3,670	0,352
10	6,406	5,954	0,452
Medium Value	4,344	3,643	0,701

(1) Total reconfiguration time of the old PAN Master

Values obtained with the scenario of Test#2 represented in Figure 21.

Table B-10			
Test #	**Total time(2)**	***dhclient* time**	**Total time(3)**
1	3,389	3,232	0,157
2	2,424	2,232	0,192
3	2,770	2,570	0,200
4	3,041	2,904	0,137
5	4,360	4,223	0,137
6	4,114	3,987	0,127
7	3,719	3,543	0,176
8	5,206	4,991	0,215
9	3,122	2,970	0,152
10	4,495	4,344	0,151
Medium Value	3,664	3,500	0,164

(2) Total reconfiguration time in the PAN members

(3) Total reconfiguration time of the new PAN master (includes NAT and DHCP server)

Annex C

Values obtained with the scenario of Test#3 represented in Figure 24.

Table C-11	
Test #	**Total time(1)**
1	0,285
2	0,353
3	0,349
4	0,306
5	0,320
6	0,243
7	0,265
8	0,294
9	0,345
10	0,315
Medium Value	0,308

(1) Total time needed for a device to configure as PoA for an IPv4-based access (includes NAT and DHCPv4 server)

Values obtained with the scenario of Test#3 represented in Figure 24.

Table C-12			
Test #	**Total time(2)**	**DHCPv6 server**	**Software Processing**
1	2,178	2,066	0,112
2	2,263	2,094	0,169
3	2,143	2,023	0,120
4	2,232	2,065	0,167
5	2,198	2,034	0,164
6	2,167	2,054	0,113
7	2,254	2,076	0,178
8	2,265	2,098	0,167
9	2,287	2,101	0,186
10	2,149	2,032	0,117
Medium Value	2,214	2,064	0,149

(2) Total time needed for a device to configure as PoA for an IPv6-based access (includes DHCPv6 server)