Title:	Document Version:
Deliverable D3.2 **Deployment of the Basic IPv6/PLC Test-bed**	2.3

Project Number:	Project Acronym:	Project Title:
IST-2001-37613	6POWER	IPv6, QoS & Power Line Integration

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
30/09/2003	25/12/2003	R – PU

* Type:	P - Prototype, R - Report, D - Demonstrator, O - Other
** Security Class:	PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Responsible and Editor/Author:	Organization:	Contributing WP:
Emilio García	ASSA	WP3

Authors (organizations):

Jean-Mickael Guerin (6WIND), Pedro Ruiz (ASSA), Javier Sedano (ASSA), Jordi Palet (Consulintel), Alvaro Vives (CONSULINTEL), Chano Gómez (DS2), Juan A. Garrigosa (ENDESA), Marco Stahlmann (MCL), Alan Delaney (PACE), Daniel Martínez (UMU), Juan José Pujante (UMU).

Abstract:

In the framework of the IST-project 6POWER, work package 3 is in charge of the design of the PLC network to be used for the connection among partner's test-beds, the internal trials and the external ones. This deliverable describes the deployment of an internal test-bed infrastructure, as well as the interconnection between partners to achieve a global testing environment. It also deals with the development and early deployment of the advanced services (Autoconfiguration, Security, QoS) proposed in D3.1, leading the path to the testing and collection of results which will be summarized in D3.3.

Keywords:

Advanced PLC network deployment, auto-configuration, security, network deployment, QoS.

© 6POWER Consortium

Revision History

The following table describes the main changes done in the document since its creation.

Revision	Date	Description	Author (Organization)
v1.0	17/09/2003	Document creation to collect all contributions	Alvaro Vives (Consulintel)
v1.1	09/11/2003	Added Consulintel's Monitoring Tools Information	Alvaro Vives (Consulintel)
v1.2	21/11/2003	Added others contributions	Emilio García (ASSA)
v1.3	24/11/2003	Section 3.1 (autoconfiguration)	Jean-Mickael Guerin (6WIND)
v1.4	26/11/2003	Added ENDESA´s network architecture, scenarios and ENDESA test-bed.	Juan A. Garrigosa (ENDESA)
v1.5	27/11/2003	Added contributions from UMU: Test-bed description, QoS solution and security aspects	Daniel Martínez (UMU), Juan José Pujante (UMU)
v1.6	01/12/2003	Editorial work to consolidate contributions to the date	Emilio García (ASSA)
v1.7	02/12/2003	Added content to Section 2.3 (External connections)	Alvaro Vives (Consulintel)
v1.8	02/12/2003	Added content to 6Wind test-bed section	Juan-Mickael Guerin (6WIND)
v1.9	03/12/2003	Editorial work: Abstract, Executive Summary and Conclusions	Emilio García (ASSA)
v1.10	12/12/2003	Contribution by DS2	Chano Gómez (DS2)
v2.0	16/12/2003	Editorial work: some errata and style corrections	Emilio García (ASSA)
v2.1	18/12/2003	Editorial work	Emilio García (ASSA)
v2.2	19/12/2003	Test-bed description of PACE	Alan Delaney (PACE)
v2.3	25/12/2003	Final review	Jordi Palet (Consulintel)

Executive Summary

As a follow up of the analysis phase of the project, where several possible topologies for the deployment of an IPv6 PLC network were studied, the implementation work began with the actual deployment of the equipments.

The main idea behind the selection of each one of the possible topologies has been to simulate, as closely as possible, the real scenarios that will be met by end-users. In that sense, we have tried to cover a broad variety of situations, not only to master any possible chance but to find in a practical sense which solution is most suitable for each casuistic.

But not only is the physical layer the point of our work, but also the provision of adequate services on top of it. So some tools have been installed on some test-beds, to monitor the real status of the system. Security is always a concern is networking, and therefore an infrastructure has been studied and implemented by some partners. QoS is the other big issue, and therefore the first steps towards a definite quality-provisioning platform have been done and tested on other test-beds.

This document details the final architecture of the test-bed in the different locations of the partners, and the interconnection between them. It also covers the advanced services that are being developed and tested on top of them. All is related to the more theoretical work of D3.1, where a more profound description was made, if only from a theoretical point of view. Results of these tests and an evaluation of the whole performance of the platform will be covered in the last deliverable, D3.3.

Table of Contents

Table of Figures

1. INTRODUCTION

Inside project 6POWER, WP3 deals with the design, setup and operation of the network and services that will serve in internal as well as public trials. The first deliverable, D3.1, covered the analysis of the possible solutions, focusing in the special issues that might arise when deploying an IPv6 PLC network. Therefore, a variety of situations were studied, in the form of scenarios for each kind of potential users of this technology.

Not only were topologies considered, but also which network services would be of interest; security, QoS, Autoconfiguration, DNS… were studied from different angles.

After that initial phase, some actual test-beds were deployed in each one of the partners, each of them taking into consideration which was the best way to study, from the most practical point of view, all the solutions proposed. All of this work is thought to serve as support for the final public trial, so isolated test-beds would not be of much use if a real-world scenario were to be resembled. Thus, the interconnection of all the test-beds took also place as a part of the initiative to deploy IPv6 over PLC in a broad fashion.

The previously studied services needed also be installed in each test-bed, so each partner chose among all the solutions, which were of interest, and the result is that all the topics covered in D3.1 are now being tested. As a consequence of all of this, the work also introduces the foundations of Zaragoza public trial, from the network deployment point of view.

This document is organized as follows: Section 2 makes a light review of the scenarios considered in the previous deliverable, and deals with the actual external network topology selected for the project test-bed. Section 3 covers the advanced services that have been implemented or installed: Autoconfiguration, Security, QoS and Multicast. Section 4 introduces Zaragoza public trial test-bed, while section 5 details the test-bed deployed at each partner. It is expected that similarities can be seen among all of them, and also with the real public trial test-bed. Section 6 gives some conclusions on the work done for this deliverable.

2. FINAL BASIC PLC NETWORK DESIGN

2.1 Scenarios

Different types of deployment scenarios were covered in Deliverable D3.1 [6POWER_D3.1], depending on the nature of the users targeted, and their equipments. For the actual PLC network of the project, which will be shown practically in the public trial infrastructure (Section 4), all the possibilities are summarized in Figure 2-1.

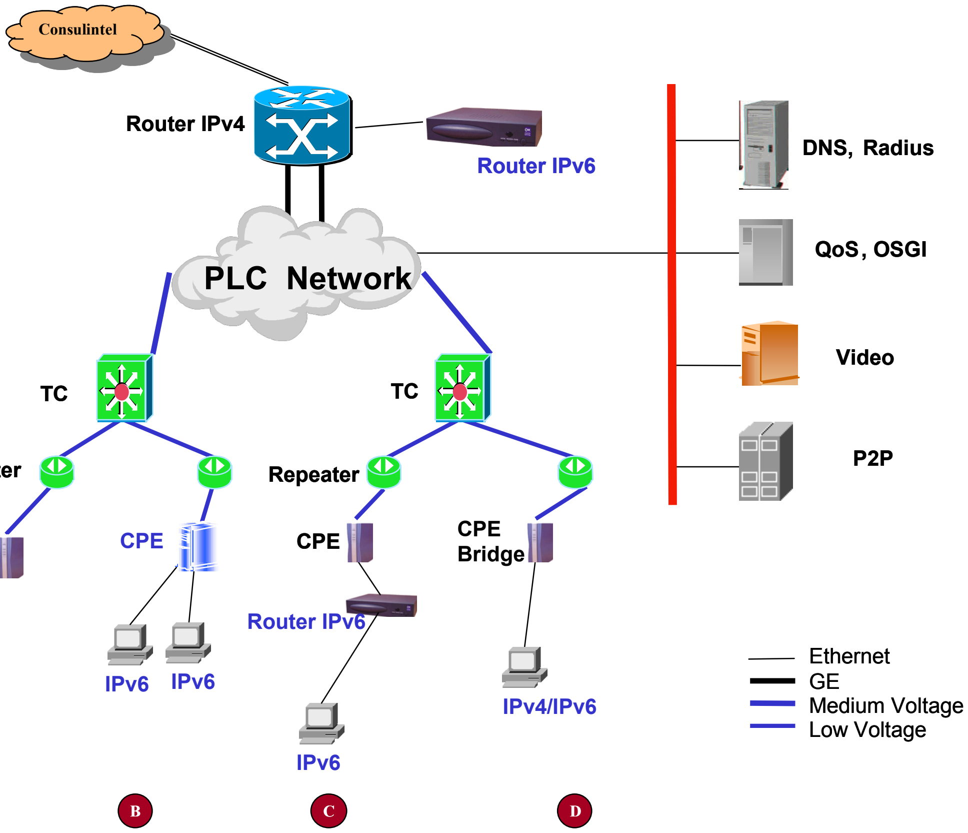


Figure 2-1: Type of Deployment Scenarios

The ways of connecting the end-user equipment (mostly PCs) to the Internet through the PLC network fall in one of these categories:

A) **CPE acting as a Router**: This is thought for the scenario with Home Users. The CPE only delivers, using RA, a prefix for the end-user terminal. This prefix is usually a /64, so that a network of machines can be configured.

B) **CPE Router, supporting IPv6 on multiple interfaces**: Several networks can be built from the same CPE, if it is able to obtain, for example, a /60 prefix from the router, and then provide /64 prefixes on demand.

C) **Router owned by the customer**: This is typical for a professional environment, where the IPv6 router of the company is already present, and is not to be substituted by the CPE. CPE acts only as a bridge, and the complexity of the RA (or DHCPv6) is hidden by the existing router.

D) **CPE Bridge-only**: This can help transition scenarios. IPv4/IPv6 addresses are given directly from the HE to the end-user terminal. In case of IPv4, access has to be done using NAT. The advantage for the user in moving to IPv6 is the suppression of that barrier

While all these possible scenarios can be present when deploying a real network, test-beds in the partners (described in Section 5) cover A, C and D.

2.2 External connections

The final connection of the different test-beds of 6POWER project followed the design depicted in Deliverable D3.1 [6POWER_D3.1], with minor changes.

This way, the Euro6IX (www.euro6ix.org) network has been used as the *core* network. The general scheme can be seen in Figure 2-2.

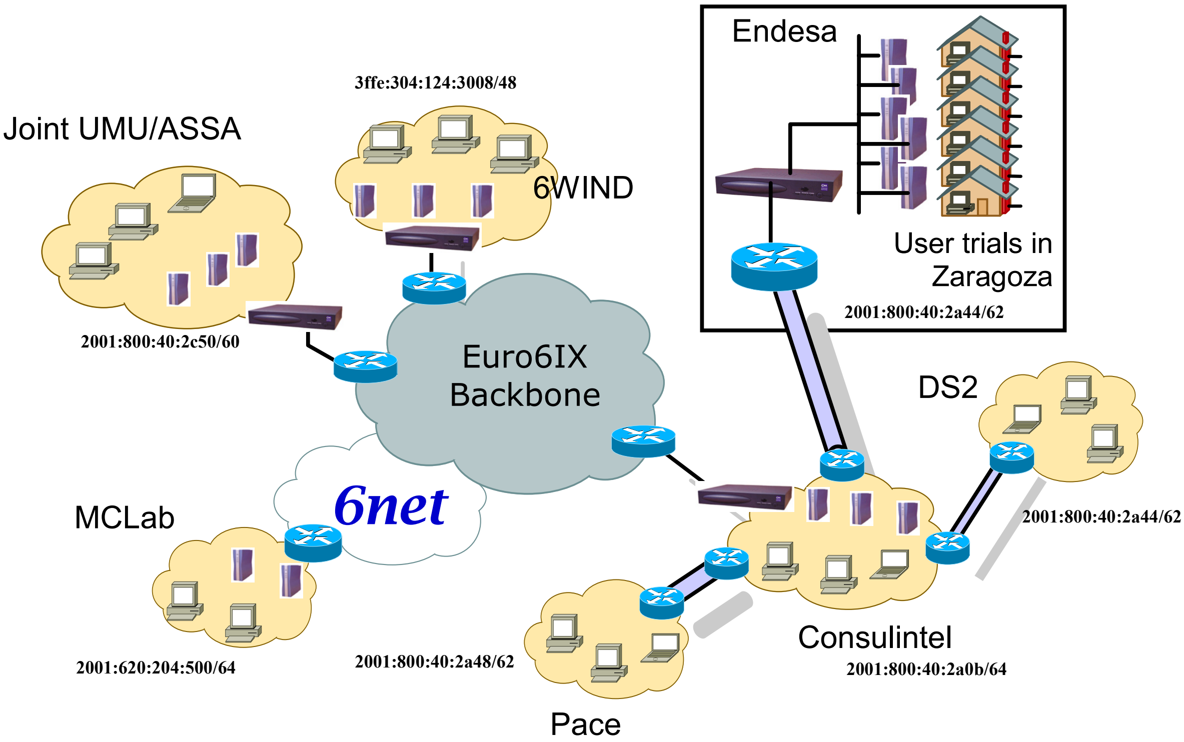


Figure 2-2: External Interconnections

Partners like 6WIND, ASSA, Consulintel and UMU are connected using Euro6IX network. MCL uses the 6NET (www.6net.org) network that was already connected to Euro6IX network. Finally those partners that had no direct access to the mentioned networks created an IPv6-in-IPv4 tunnel towards Consulintel. These partners are DS2, ENDESA and PACE, whose addressing is shown in Table 2-1.

Partner	Server IPv4	Server IPv6	Client IPv4	Client IPv6	Prefix
Consulintel	-----	2001:800:40:2a0b::1	-----	-----	2001:800:40:2a0b::/64 (RA)
DS2	213.172.48.138	2001:800:40:2a3a::11/126	80.81.115.131	2001:800:40:2a3a::12/126	2001:800:40:2A40::/62
Endesa	213.172.48.138	2001:800:40:2a3a::21/126	TBD	2001:800:40:2a3a::22/126	2001:800:40:2A44::/62
PACE	213.172.48.138	2001:800:40:2a3a::31/126	194.60.92.2	2001:800:40:2a3a::32/126	2001:800:40:2A48::/62
Available	213.172.48.138	2001:800:40:2a3a::41/126	TBD	2001:800:40:2a3a::42/126	2001:800:40:2A4C::/62

Table 2-1: Addressing of Tunnels to Partners

2.2.1 Addressing

Assuming the configuration explained above, the addressing scheme for all the sites is summarized in Table 2-2.

	Home Gateway	Internal prefix
Partner	**IPv6**	**IPv6**
6WIND	2001:660:3008:3600::1	2001:660:3008::/48
Consulintel	2001:800:40:2a0b::1	2001:800:40:2a0b::/64
DS2	2001:800:40:2a3a::12	2001:800:40:2A40::/62
MCL	2001:620:204:500::1	2001:620:204:500::0/64
UMU/ASSA	2001:800:40:2c00::2	2001:800:40:2c50/60
PACE	2001:800:40:2a3a::32	2001:800:40:2a48::/62
Trial users	2001:800:40:2a3a::22	2001:800:40:2A44::/62

Table 2-2: Partner's Addresses

All the sites use, at least, a /64 prefix, which enables autoconfiguration. Sites connected through the tunnel in Consulintel can use a /62.

2.2.2 DNS

The project domain is managed by Consulintel, which also manages some partners' sub-domains. Other partners preferred to have their sub-domain delegated to their own DNS server. The following table (Table 2-3) shows the actual status.

Partner	Subdomain	DNS server
6WIND	6wind.6power.org/.net	proxy.ipv6.6wind.com
ASSA	assa 6power.org/.net	ns1.euro6ix.com
Consulintel	consulintel.6power.org/.net	ns1.euro6ix.com
DS2	ds2.6power.org/.net	ns1.euro6ix.com
Endesa	endesa 6power.org/.net	ns1.euro6ix.com
MCL	mcl.6power.org/.net	ns1.mclab.ch / atlas.mclab.ch
UMU	umu 6power.org/.net	dns6p.ipv6.um.es
PACE	pace 6power.org/.net	ns1.euro6ix.com

Table 2-3: DNS Domains and Servers

3. DESIGN OF ADVANCED NETWORKING FUNCTIONALITIES

3.1 Autoconfiguration

DHCPv6 Prefix delegation, combined with stateless autoconfiguration, provides a global IPv6 autoconfiguration solution in PLC access network and end users network.

DHCPv6 prefix delegation is based on RFC 3315 [RFC3315] and an Internet Draft [IETF_PREFIX]. The Head End plays the role of delegating router while CPE is the requesting router. The Head End chooses IPv6 prefix from radius server configured at time of subscription of CPE.

By means of DHCPv6 option, CPEs learn IPv6 domain name server [IETF_DNS] and configure automatically the proxy DNS.

IPv6 Stateless autoconfiguration on users network is done according to RFC 2462 [RFC2462] and is implemented in every IPv6 stack. CPEs sends router advertisement based on IPv6 prefix acquired during prefix delegation.

As there is no standard yet for IPv6 hosts to learn IPv6 name servers, dual stack hosts can run DHCPv4 client to get one. In this case CPEs will have to enable DHCPv4 server to provide itself as IP address for DNS server. DNS request will then be over IPv4 from hosts to CPE, and over IPv6 from CPE to DNS servers thanks to proxy DNS in CPE.

3.2 Security Aspects

As it was established in the analysis, the securization of 6POWER network will be done by means of the use of the IPSec protocol to set up static/dynamic Virtual Private Networks among the project partners' test-beds. This mechanism, besides the use of IPv6 filters and firewalls, form the security mechanism to protect the test-bed and 6POWER network.

3.2.1 IPSec

The IPSec protocol is a mandatory component of the IPv6 stack. It provides security services to the IP layer. A system using IPSec is able to select the required security protocols, determine the algorithm(s) to use for the service(s), and obtain the required cryptographic keys to provide the requested services.

These objectives are met through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols.

The IP Authentication Header (AH) provides connectionless integrity, data origin authentication, and an optional anti-replay service. The Encapsulating Security Payload (ESP) protocol may provide confidentiality (encryption), and limited traffic flow confidentiality. It also may provide connectionless integrity, data origin authentication, and an anti-replay service (one or the other set of these security services must be applied whenever ESP is invoked). Both AH and ESP are vehicles for access control, based on the distribution of cryptographic keys and the management of traffic flows relative to these security protocols.

These protocols may be applied alone or in combination with each other to provide a desired set of security services. Both protocols have two modes of use: transport mode and tunnel mode. In transport mode the protocols provide protection primarily for upper layer protocols; in tunnel mode, the protocols are applied to tunneled IP packets.

Because these security services use shared secret values (cryptographic keys), IPSec relies on a separate set of mechanisms for putting these keys in the required place (keys are used for authentication/integrity and encryption services). IPSec requires support for both manual and automatic distribution of keys. It defines a specific approach (**IKE**) for automatic key management, but other automated key distribution techniques may be used.

ESP provides encryption service to the packets, causing the data to be random in nature, rendering compression at lower protocol layers ineffective. IP payload compression (IPComp) [IPComp] provides a way to compress packets before encryption by ESP. This protocol reduces the size of IP datagrams and increases the overall communication performance.

3.2.2 IKE

Internet Key Exchange, IKE, is the protocol used to establish security associations that are needed by various services. IPSec uses IKE to establish the security associations (SA) needed to generate and refresh its keys. To establish security associations, the keys must be formed in a secure and protected way and IKE provides this mechanism.

IKE is a protocol which includes part of Oakley [Oakley] and part of SKEME [SKEME] as key exchange protocol, inside the ISAKMP [ISAKMP] framework. A Security Association (SA) is a simplex "connection" that affords security services to the traffic carried by it. These security services are afforded to an SA by means of the use of AH, or ESP, but not both. To secure typical, bi-directional communication between two hosts, or between two security gateways, two Security Associations (one in each direction) are required.

A security association is uniquely identified by a triple:

- Security Parameter Index (SPI): It identifies the SA.
- IP Destination Address.
- The Security Protocol (AH or ESP) identifier.

IKE is made up of two phases as defined in the ISAKMP framework, and within these phases, Oakley defines a number of modes that can be used.

Phase 1 is the process where the ISAKMP security association must be established. It assumes that no secure channel currently exists and therefore it must initially establish one to protect any ISAKMP messages. This SA is different from other SAs that are negotiated for other services and it is owned by ISAKMP. **Phase 2** is where the security associations required by others services are negotiated on their behalf. The ISKMP SA generated in Phase 1 protects all subsequent ISAKMP messages.

Also, in Phase 1, there are available two modes: Main mode and aggressive mode. Support for main mode is a mandatory requirement for IKE, while aggressive mode has the advantage of being able to use three instead of the six message flows required to establish the ISAKMP SA.

Within phase 2, quick mode is used to negotiate the SAs for the services. Informational mode is used to give the other party some information, normally abnormal conditions due to failures. Other mode is new group mode, which is used to negotiate private groups for Diffie-Hellman exchanges. Although protected by the Phase 1 exchange, this is not part of a Phase 2 exchange.

The IKE mechanism is quite efficient in that it is able to negotiate many security associations with relatively few messages. With a single Phase 1 negotiation, multiple Phase 2 negotiations can occur. And within a single Phase 2 negotiation, multiple SAs can be negotiated.

3.2.2.1 IKE Phase 1

During this phase, the partners exchange proposals for the ISAKMP SA and agree on one. This SA contains the specifications of the authentication methods, hash functions and encryption algorithms to be used to protect the key exchanges. Then, the partners exchange information to generate a shared master secret:

- Cookies that also serve as SPIs for the ISAKMP SA.
- Diffie-Hellman values.
- Random Numbers.
- Optionally exchange IDs when public key authentication is used.

Both parties generate then keying material and shared secrets before exchange additional authentication information. When all goes fine, both parties derive the same keying material and actual encryption and authentication keys without ever sending any keys over the network. In addition to this, phase 1 also authenticates the two parties involved in the exchange.

There are four authentication methods available:

- Digital signatures.
- Public key encryption.
- Revised public key encryption.
- Pre-shared keys.

During phase 1, only a single SA is negotiated, the ISAKMP SA. Only one proposal is offered always-proposing Oakley as the key exchange method. Within that proposal multiple transforms can be offered which negotiate the following parameters:

- Authentication method.
- Lifetime/lifesize of the SA.
- Diffie-Hellman group.
- Hash algorithm.
- Encryption algorithm.

3.2.2.2 IKE Phase 2

During phase 2, the partners exchange proposals for protocol SAs and agree on one. This contains specifications of authentication methods, hash functions and encryption algorithms to be used to protect packets using AH and/or ESP. To generate keys, both parties use the keying material from a previous Phase 1 exchange and they can optionally perform an additional Diffie-Hellman exchange for PFS (Perfect Forward Secrecy).

3.2.3 Public Key Infrastructure

The target of a Public Key Infrastructure (PKI) is to provide Public Key Certificate (PKC) management to the group of security protocols designed to protect Internet. These protocols, as **IPSec** (Internet Protocol Security), SSL (Secure Sockets Layer), TLS (Transport Layer Security) or S/MIME (Secure Multipurpose Internal Mail Extensions) use public key cryptography to provide services such as:

- Confidentiality.
- Data integrity.
- Data origin authentication .
- Non-repudiation.

The users of public key based systems must trust in a PKC. It is a data structure that binds a public key to the user subject. This binding is achieved by having a trusted CA that verify the subject identity and digitally sign each digital certificate.

A PKI is defined as a system based on public key cryptography, including software, people, policies, hardware, etc, allowing create, manage, store, distribute and revoke public key certificates. The main components of a generic PKI are:

- Certification Authorities (CAs) issue, renew and revoke PKCs.
- Registration Authorities (RAs) authenticate off-line users and add certificate's properties.
- PKI clients can encrypt and sign digital documents.
- PKI clients validate digital signatures from a known public key of a trusted CA.
- Public repositories make available certificates and certificate revocation lists (CRLs).

PKI offers services that can be reached via Internet, such as certification requests, retrieval, revocation or renewal of PKCs, etc.

These services allow user to encrypt, use digital sign in documents, etc. Also, the services offered by the PKI can be used by the services or by devices that require secure communications. This is the case of the VPN service in IPv6 networks, the main service we are interested in. Though there are other network services such as secure web servers (HTTPS) and Authentication, Authorization and Accounting services (AAA), which can use the PKI infrastructure to protect information or to authenticate users.

Thanks to this infrastructure, the users of the IPv6 network can make use of cryptographic services to secure the communications.

The main characteristics are:

- Users can issue, renew and revoke certificates.
- LDAPv6 directory supported to store users and CA's certificates and CRLs.
- Final users can carry out certification operations from their own navigator or through RAs.
- Users can storage cryptographic information (private key, certificate and CA's certificate) in their smart cards. This allows total mobility, so that, if an user requests a certificate from a navigator or from the RA, this certificate can be recovered in any moment from another different navigator.
- Basic configuration of PKI through HTTP.
- Policy definition will establish the opportune restrictions inside an organization.

- Administrators will define this Policy and it will be applicable in all the PKI‘s components.
- PKI has been developed completely in Java, what allows use of any platform in the system. It is based on standards specified by the IETF inside the PKIX [PKI] work group.
- SCEP protocol supported (Simple Certificate Enrollment Protocol) for VPN Clients.
- 6WIND VPN routers supported.
- Cross-certification is allowed in two ways, peer-to-peer and hierarchical cross-certification
- Communications between components are over IPv6 or IPv4.

The PKI also offers several added value services dedicated to enrich the range of possibilities it offers. Among them, a very useful one is the support for SCEP (Simple Certificate Enrollment Protocol) protocol and the certification for 6WIND routers.

3.2.3.1 SCEP

Thanks to the support for SCEP protocol, this service gives certification support to VPN devices requiring the use of digital certificates. SCEP is a protocol developed by CISCO broadly used by devices as routers to obtain their secure information when setting up virtual private networks.

The implementation of this service is based on a SCEP server, implemented with Java Servlets. The server waits for certification requests or queries from VPN devices. Current implementation is based on use of single keys and it has been tested successfully in CISCO routers.

3.2.4 6WIND Routers

6WIND routers, IPv6 routers, require an special way to obtain cryptographic information. the issuance and retrieval of certificates is based on SSH protocol.

The PKI allows clients to request or retrieve Certificates by means of SCP operations. This implementation is based on Java Servlets making pooling over a special user directory, which only 6WIND-authorized clients can put and get information. When authorized clients put a certification request, this is validated or not by the RA administrator. When the certificate is issued, the client can retrieve it from the same directory. Besides, authorized clients can get CA and CRL certificates.

3.3 Quality of Service

In this section, the basic network solution for QoS introduced in D3.1 will be detailed. A concrete design of an advanced QoS service for IPv6 over PLC is explained here, specifying QoS management on each of the segments identified in D3.1.

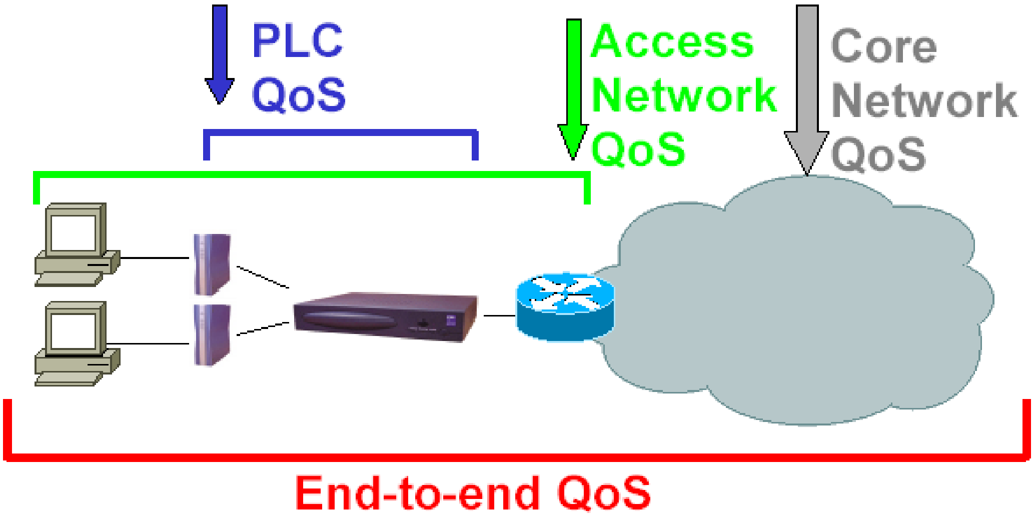


Figure 3-1: Segments Involved in End-to-End QoS

First, native QoS support on the involved segments must be analyzed. The following table summarizes the available QoS mechanisms and where each one is located.

QoS technique	Where is it available?
Per-CPE bandwidth allocation	PLC driver
Per-DSCP traffic queuing	PLC driver / 6WIND Routers
Per-DSCP bandwidth allocation	6WIND Routers

Table 3-1: Available QoS Techniques

The QoS solution will make use of these mechanisms in order to achieve end-to-end QoS. Here, the key issues are:

- The per-CPE bandwidth allocation feature provides partial PLC QoS, both in the upstream and the downstream.
- Besides bandwidth allocation, traffic queuing is desirable as a part of the total PLC QoS. The latest version of the PLC driver supports this, using traffic marking (either via VLAN tags, the VLAN priority field, UDP ports or DSCP value).
- Traffic marking is needed also so that QoS-sensitive flows get an adequate treatment outside the PLC network. The DSCP field can be used here too, as a standard method for specifying QoS requirements, which are to be interpreted by heterogeneous routers. This allows for QoS both at the access and core networks.

Deliverable D5.2 introduced an external entity, the QoS Broker, which received SIP signaling from the end applications and acted on the PLC nodes to ensure bandwidth allocation at the PLC layer. This simple scheme is extended now as follows, to achieve end-to-end QoS:

- The QoS Broker will still receive signaling from end applications, and act on the PLC master nodes in order to ensure partial PLC QoS (bandwidth allocation) both in the upstream and the downstream. This was already showed in D5.2.

- In addition to this, the QoS Broker can also interact with the access router to instruct DSCP marking for the incoming and outgoing traffic, which belongs to the flow being prioritized. Source and destination addresses/ports can be used to specify this. This DSCP marking will allow for an adequate QoS management outside the PLC network, as well as inside it for the downstream traffic (traffic which enters the PLC network after being marked by the access router).
- Upstream traffic will need to be marked by the end applications in order to use DSCP queuing inside the PLC network (although it can get bandwidth allocation). This can be left out as an application-specific optional feature.

The following figure depicts the full QoS architecture:

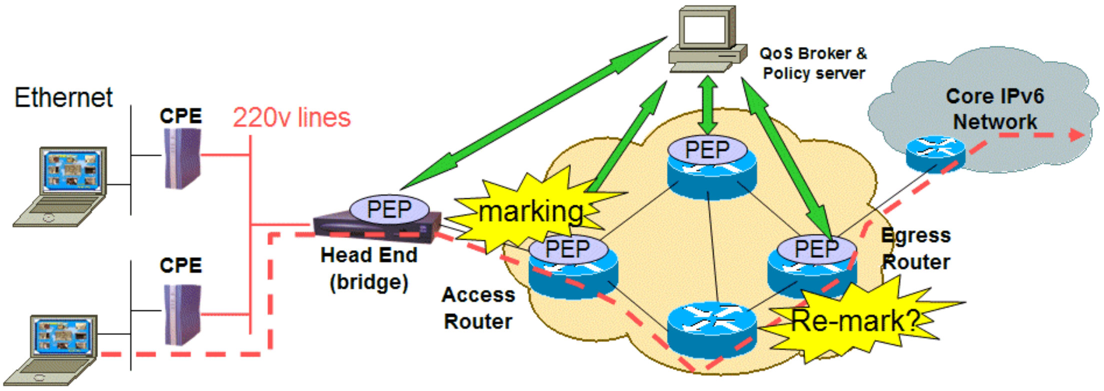


Figure 3-2: Full QoS Architecture

The following table summarizes the results obtained with this QoS solution, which forms the whole end-to-end QoS:

Network segment	Result
PLC QoS	Bandwidth allocation and DSCP-based traffic queuing, both provided by the PLC driver
Access network QoS	Router-dependant PHB based on DSCP. Both bandwidth allocation and traffic queuing are available on 6WIND routers.
Core network QoS	Network-dependant PHB's based on DSCP. Hopefully, at least traffic queuing should be available.

Table 3-2: Results Provided by the QoS Solution

4. PUBLIC TRIAL INITIAL INFRASTRUCTURE

At the end of 2001 ENDESA began the deployment of a Massive Technology Trial in Zaragoza, reaching (at July 2002) up to 2100 users, providing Broadband Internet Access (>2 Mbps) and Voice service (VoIP). Zaragoza MTT was finished in December 2003, once decided the business opportunity that PLC technology offers, guaranteed by the 6PWOWER developments. C1 License was obtained to work in a multicarrier environment. Since December 2003, AUNA offers PLC commercial service through ENDESA´s network in Zaragoza and in January 2003 in Barcelona.

However, one part of the Zaragoza´s network has been assigned to research and development. Some final users of this part of the network are ENDESA´s contribution to 6POWER project.

The following picture shows the general design of ENDESA´s network.

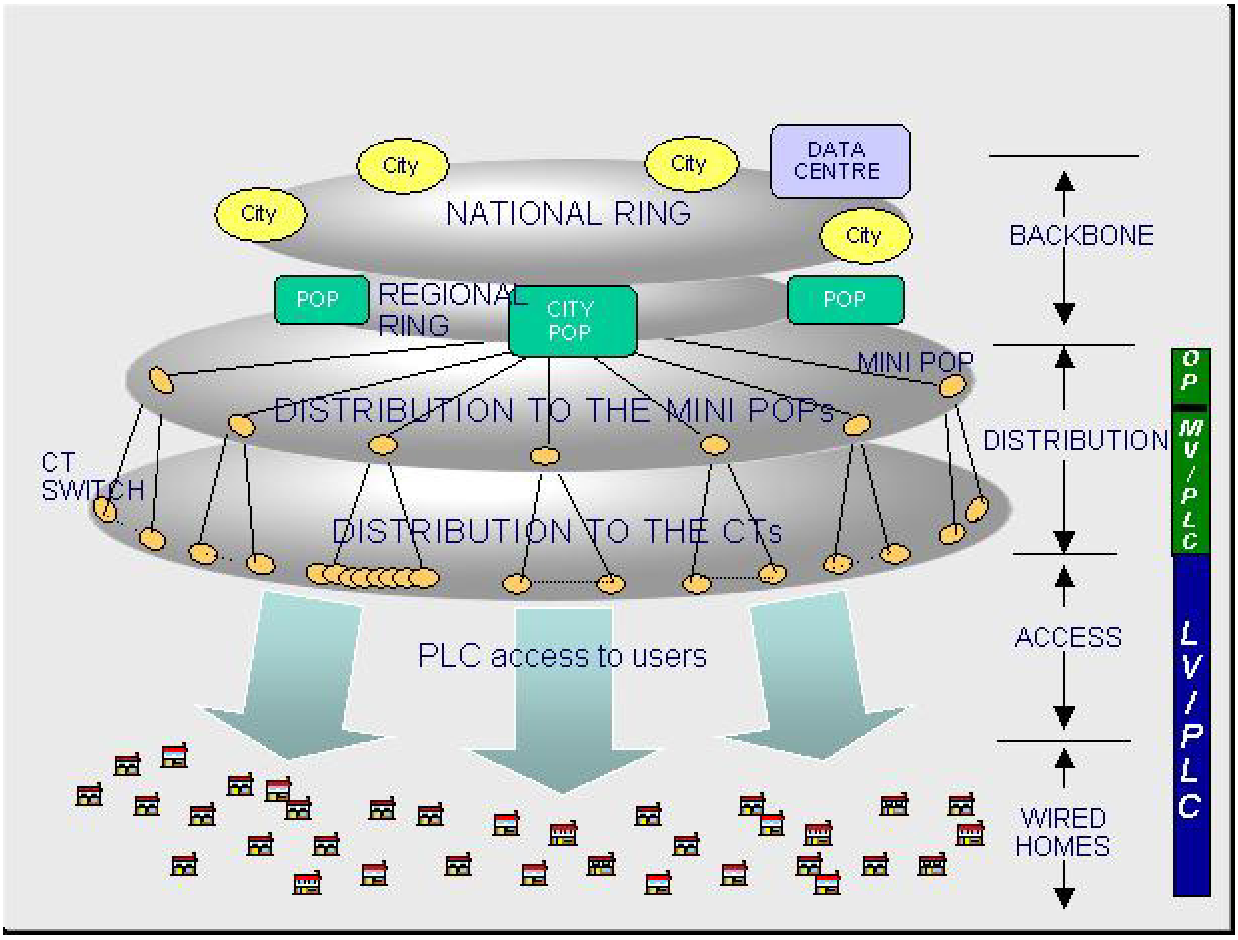


Figure 4-1: Endesa's Network

A City Pop connected to MAN POPs, with dark fiber and Gigabit Ethernet switches, deploys the Distribution network, on a first level. On a second level, only Medium Voltage links are used to join MV Substations (TCs), sometimes in rings, sometimes in branches.

Voice, Internet and carriers connections are located in the City Pop. In this point, interconnection to 6POWER network will be also made.

Not only in GE rings, but it also in Medium Voltage rings, Spanning Tree Protocol is running, as redundant protocol, in order to provide high availability.

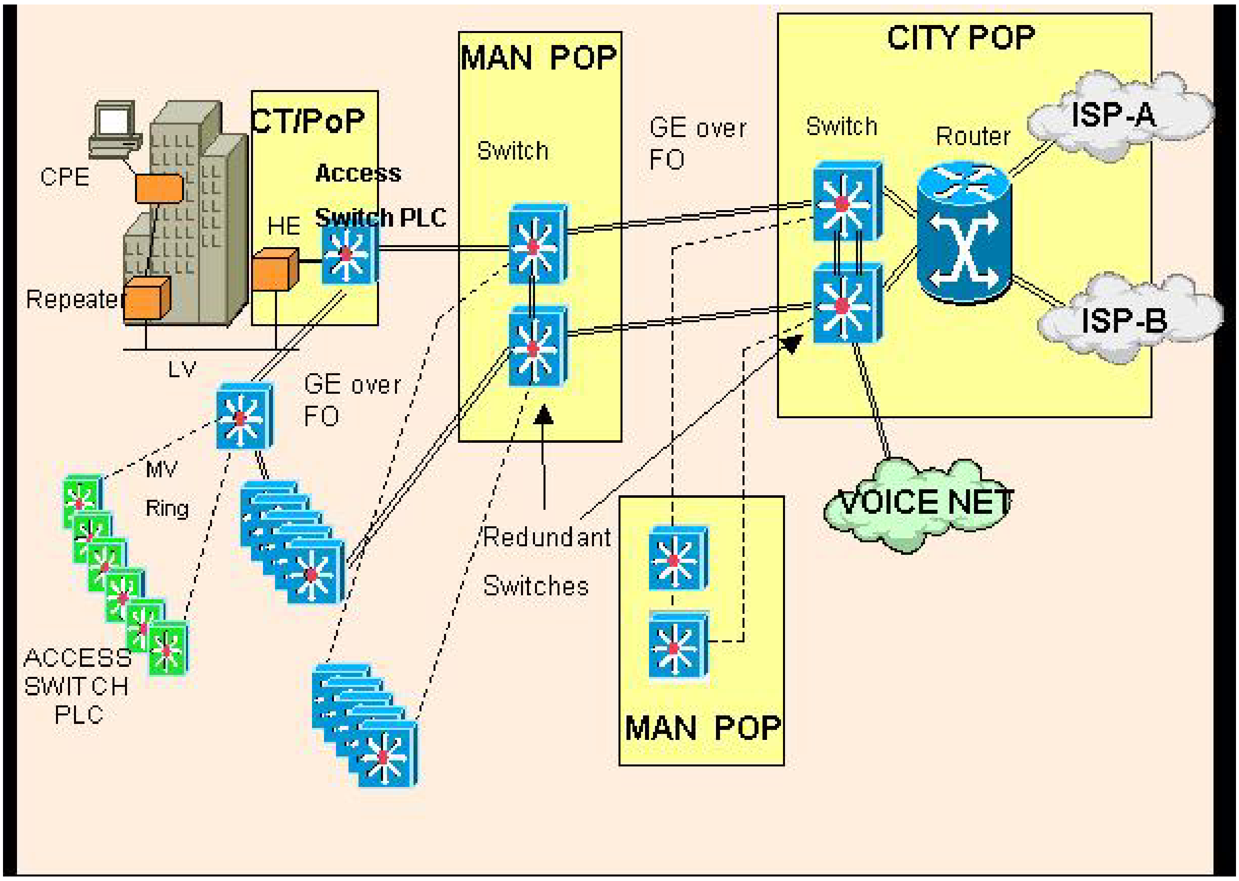


Figure 4-2: Detail of Internal Interconnections

802.1p/Q has been implemented in the network to provide service prioritization (voice and management traffic over internet traffic) and the implementation of a VLAN scheme.

One VLAN has been reserved to 6POWER project. Security guaranteed due to an appropriate VLAN administration with a different VLAN ID for every service. There is no visibility between different VLANs so it is guaranteed no visibility between PLC users.

Network design provides scalability, redundancy, security and it is resilience to extensions. Also, main Systems are duplicated in order to provide full redundancy.

Manufacturers Mitsubishi and Sumitomo provide all PLC equipments on ENDESA´s network.

Provisioning system is already running with redundant servers. Basically, as ENDESA is in a multicarrier environment, once one CPE is connected, the repeater learns automatically its MAC address (autoprovisioning feature). The repeater assigns it a private IP address with a plain configuration profile. With this profile, the connection to repeater is allowed and repeater checks in a RADIUS server this MAC, previously added. Once RADIUS authenticates the MAC address, repeater allows DHCP request to DHCP server. DHCP server as well checks the authentication to the RADIUS server and consults the LDAP system in order to provide an appropriate profile of one of the carriers and final CPE configuration. Voice service is activated in this final step.

5. DESCRIPTION OF THE DIFFERENT TEST-BEDS

5.1 Joint UMU/ASSA Test-bed

The UMU/ASSA test-bed is described in Figure 5-1.

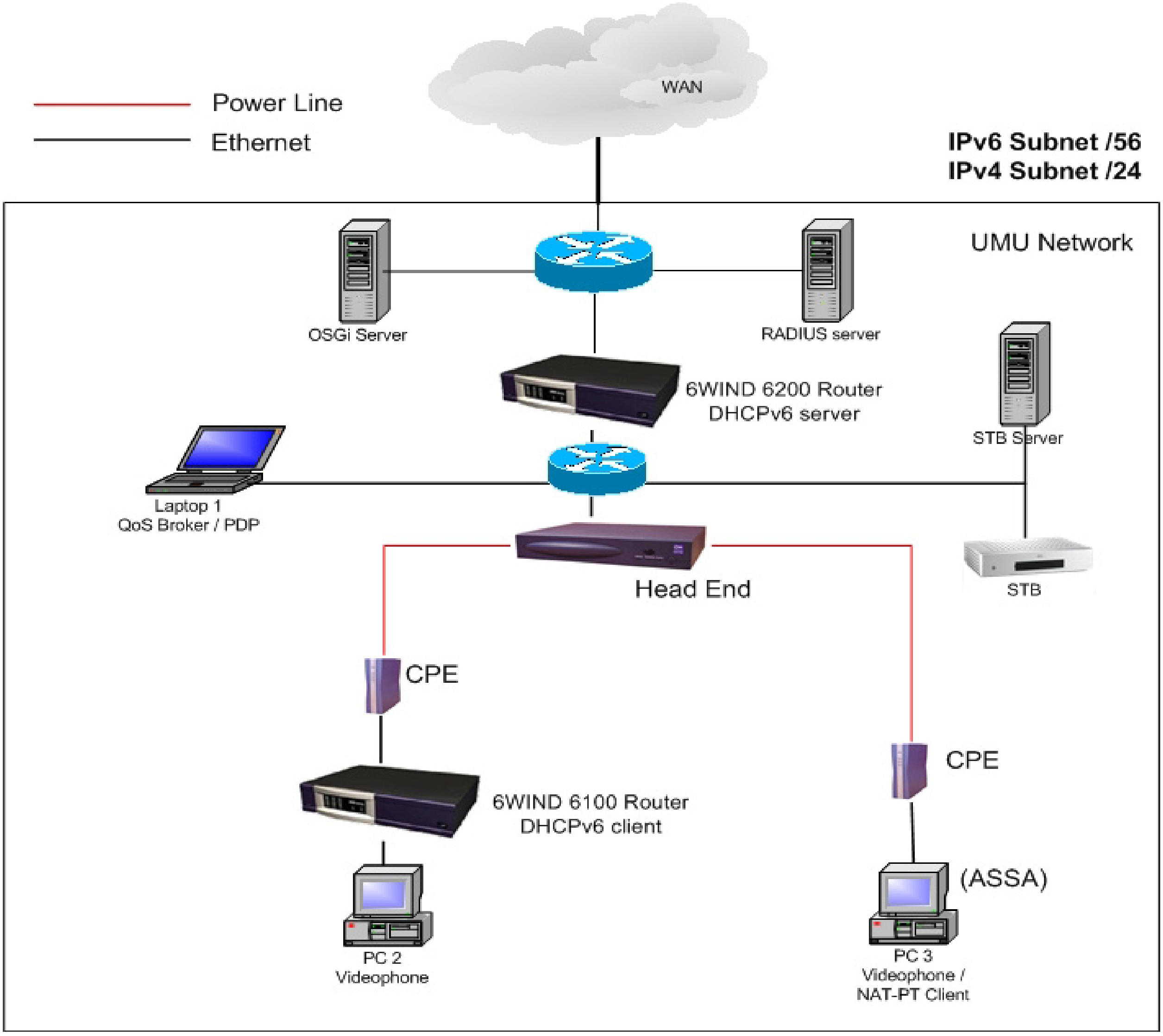


Figure 5-1: Joint UMU/ASSA Test-bed

As it can be seen, the test-bed has two differentiated parts. These areas are distinguished by the use of PLC. In the PLC area have been placed the hosts running the videophone application and that make use of the QoS Broker to configure the QoS of the PLC network.

In our test-bed we make use of addresses from the prefix of UMU in the Euro6IX project. The prefix used is 2001:800:40:2cff::/64. The IPv4 addresses assigned to the hosts belong to the 155.54.95.x network from UMU.

Also, in the test-bed there are installed two 6WIND routers for testing the prefix delegation functionality. The prefix used for this is 2001:800:40:2cf9::/60.

The test-bed has a DNS server where the umu.6power.org domain is managed. This is a dual-stack server that also manages the IPv4 network domain.

The hosts that are placed behind the 6WIND router that acts as DHCPv6 client, make use of autoconfiguration as the way to obtain an IPv6 address. The rest of hosts are configured with a static IPv6 address.

5.2 Consulintel Test-bed

This test-bed follows the design described in D3.1 [6POWER_D3.1]. It has been designed as being part of the Euro6IX network. So we have assigned addresses among the prefix we have received to be used in this project.

Also this test-bed gives connectivity to other partners by means of an IPv6-over-IPv4 tunnel, allowing both the connection to our network and to Euro6IX backbone, which is connected to 6Bone.

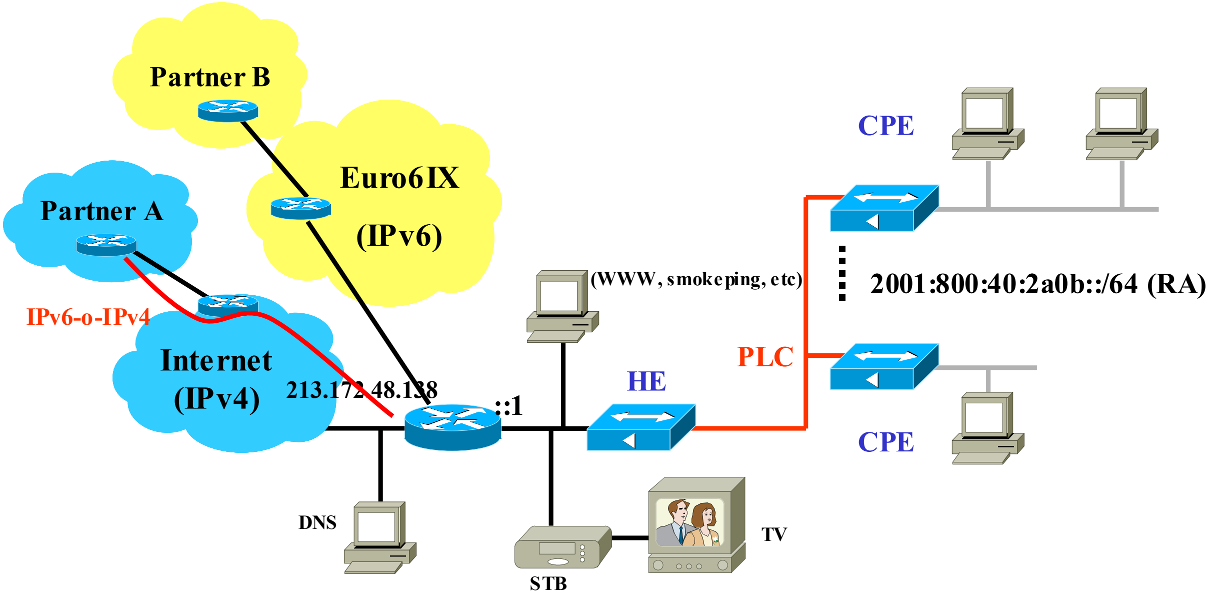


Figure 5-2: Consulintel's Test-bed

Partner A is a partner with IPv4 connectivity. It can make a tunnel to Consulintel's premises, receiving the corresponding /62 prefix. Actually, both DS2 and PACE have configured a tunnel to Consulintel.

Partner B is a partner that already has connectivity to Euro6IX.

As agreed within the project, each partners has a DNS entry under their sub-domain, to be used for network monitoring purposes (ping6.consulintel.6power.org).

As services, we have a dual-stack DNS server that is used as the main DNS server of the project, hosting the project domains (6power.org and 6power.net) and some of the partners' sub-domains. An HTTP server and some monitoring tools are also installed in our test-bed.

At last but not least, we have the first prototype of STB delivered by PACE in order to make some local tests.

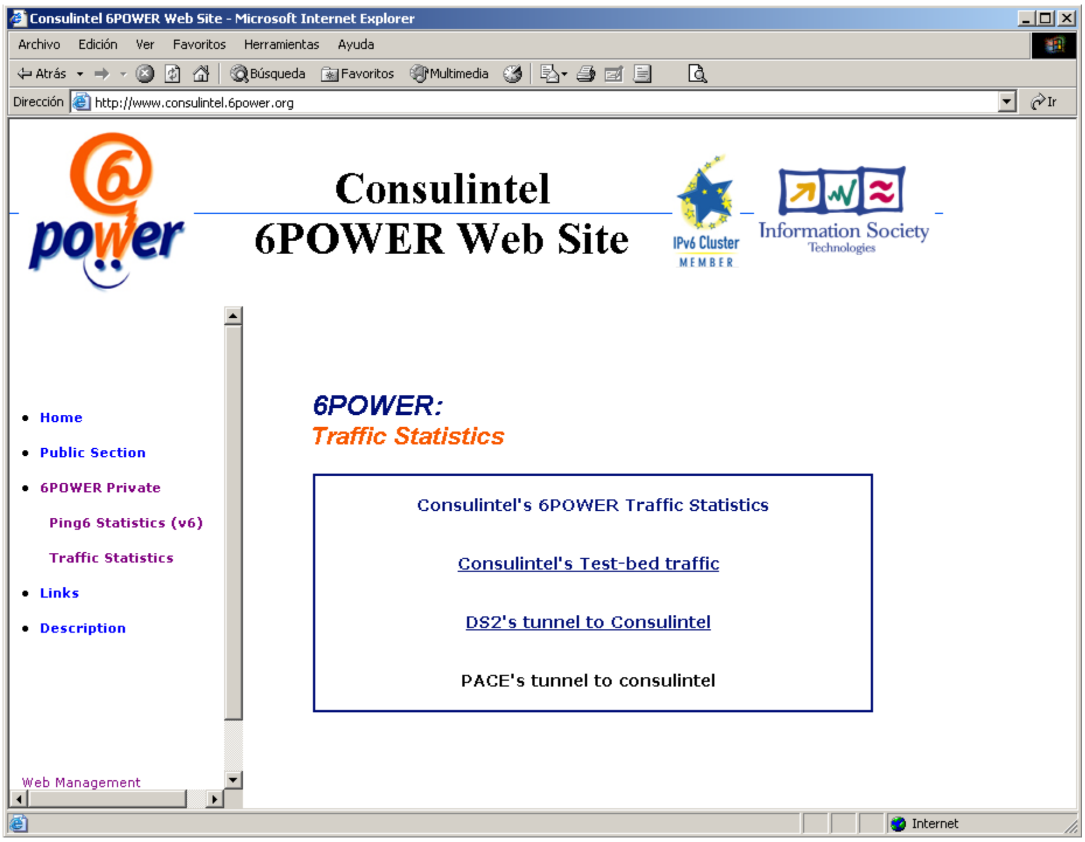
A description of our test-bed and even some configuration hints could be found in www.consulintel.6power.org.

5.2.1 Monitoring Tools

In Our test-bed we have installed the following monitoring tools:

- MRTG: Multi Router Traffic Grapher.
- Smoke Ping.

With the MRTG tool we can monitor the traffic in our local test-bed and also in the different tunnels we have towards other partners. Following some screenshots.



Consulintel 6POWER Web Site - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Multimedia
Dirección http://www.consulintel.6power.org
Ir
Internet

Consulintel
6POWER Web Site

- Home
- Public Section
- 6POWER Private
  - Ping6 Statistics (v6)
  - Traffic Statistics
- Links
- Description

Web Management

6POWER:
Traffic Statistics

Consulintel's 6POWER Traffic Statistics

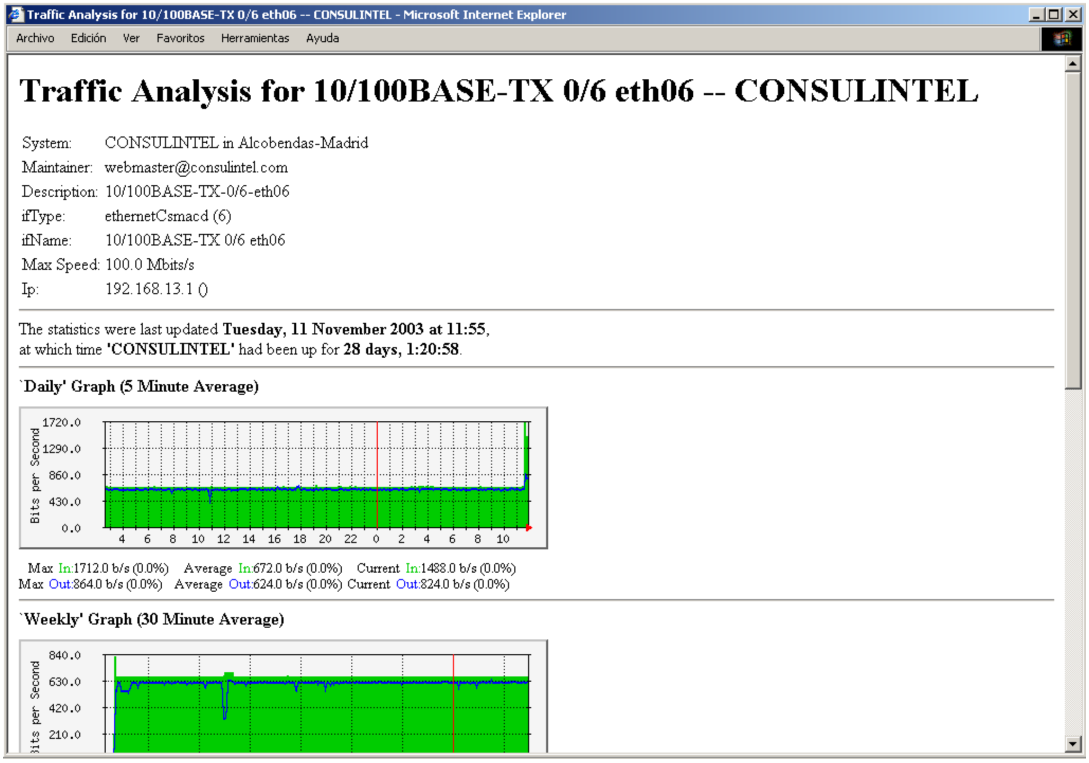
Consulintel's Test-bed traffic

DS2's tunnel to Consulintel

PACE's tunnel to consulintel

Figure 5-3: Consulintel's Test-bed Traffic Statistics Menu

With the Smoke Ping tool we can test the reachability of different points of the project's IPv6 network. This tool is only reachable using IPv6. Is available for partners only, at the 6POWER private area of project web site and in http://sp6.consulintel.6power.org/cgi/smokeping.cgi.


Traffic Analysis for 10/100BASE-TX 0/6 eth06 -- CONSULINTEL - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Bits per Second
1720.0
1290.0
860.0
430.0
0.0
4 6 8 10 12 14 16 18 20 22 0 2 4 6 8 10
840.0
630.0
420.0
210.0

Traffic Analysis for 10/100BASE-TX 0/6 eth06 -- CONSULINTEL

System:	CONSULINTEL in Alcobendas-Madrid
Maintainer:	webmaster@consulintel.com
Description:	10/100BASE-TX-0/6-eth06
ifType:	ethernetCsmacd (6)
ifName:	10/100BASE-TX 0/6 eth06
Max Speed:	100.0 Mbits/s
Ip:	192.168.13.1 ()

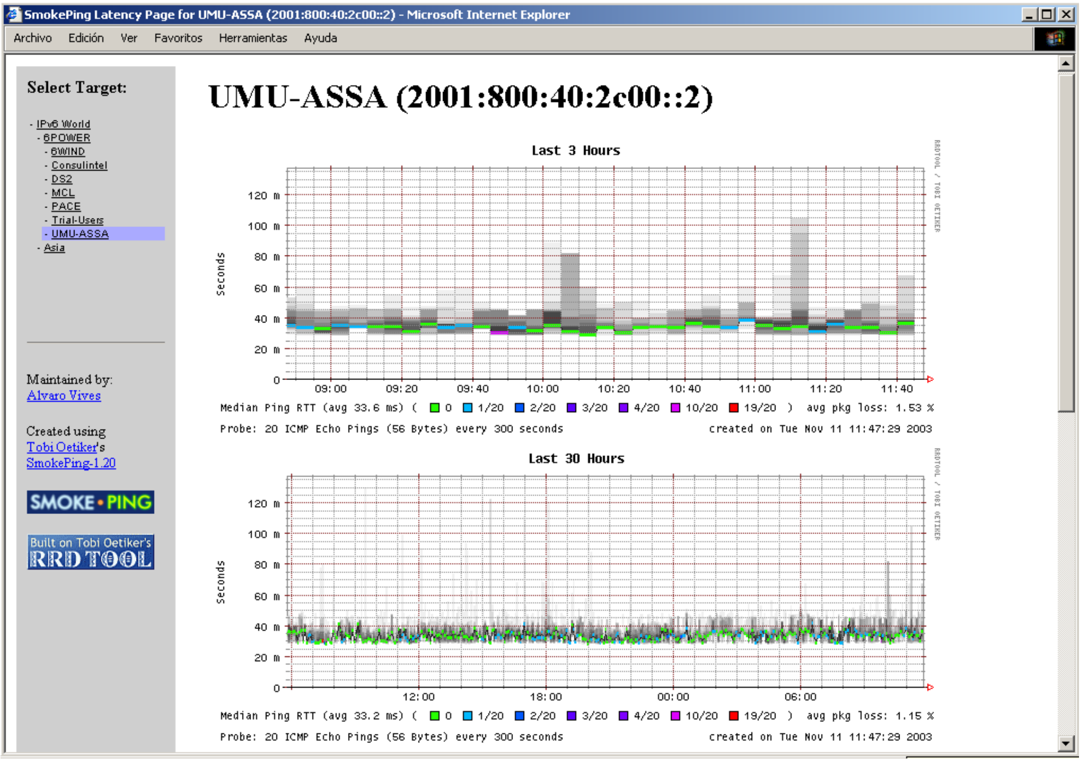
The statistics were last updated **Tuesday, 11 November 2003 at 11:55**, at which time **'CONSULINTEL'** had been up for **28 days, 1:20:58**.

`Daily' Graph (5 Minute Average)

Max In:1712.0 b/s (0.0%) Average In:672.0 b/s (0.0%) Current In:1488.0 b/s (0.0%)
Max Out:864.0 b/s (0.0%) Average Out:624.0 b/s (0.0%) Current Out:824.0 b/s (0.0%)

`Weekly' Graph (30 Minute Average)

Figure 5-4: Consulintel's Test-bed Traffic Statistics Example


SmokePing Latency Page for UMU-ASSA (2001:800:40:2c00::2) - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Last 3 Hours
Seconds
120 m
100 m
80 m
60 m
40 m
20 m
0
09:00 09:20 09:40 10:00 10:20 10:40 11:00 11:20 11:40
RRDTOOL / TOBI OETIKER
Last 30 Hours
12:00 18:00 00:00 06:00
SMOKE•PING
Built on Tobi Oetiker's RRD TOOL

Select Target:

- IPv6 World
  - 6POWER
    - 6WIND
    - Consulintel
    - DS2
    - MCL
    - PACE
    - Trial-Users
    - UMU-ASSA
  - Asia

Maintained by:
Alvaro Vives

Created using
Tobi Oetiker's
SmokePing-1.20

UMU-ASSA (2001:800:40:2c00::2)

```
Median Ping RTT (avg 33.6 ms) ( 🟩 0  🟦 1/20  🟦 2/20  🟪 3/20  🟪 4/20  🟪 10/20  🟥 19/20 )  avg pkg loss: 1.53 %
Probe: 20 ICMP Echo Pings (56 Bytes) every 300 seconds               created on Tue Nov 11 11:47:29 2003
```

```
Median Ping RTT (avg 33.2 ms) ( 🟩 0  🟦 1/20  🟦 2/20  🟪 3/20  🟪 4/20  🟪 10/20  🟥 19/20 )  avg pkg loss: 1.15 %
Probe: 20 ICMP Echo Pings (56 Bytes) every 300 seconds               created on Tue Nov 11 11:47:29 2003
```

Figure 5-5: Consulintel's Test-bed Smoke Ping Statistics Example

5.3 Endesa Test-bed

Endesa´s test-bed is, in fact, the part of the present network assigned to the public IPv6 trial. As right now Endesa is involved in a commercial launching, part of the network (about 30 users) will be assigned to research and development general and particular features regarding corporative purposes. Some of these users will be involved in 6POWER project. In this sense, it is interesting to check Section 2.1 of this document for further information of final scenarios to be deployed.

As a first step of the final public trial, an IPv6 tunnel from Endesa to UMU has been established. One PC in Endesa´s network is connected to one UMU´s router using the prefix 2001:800:40:2c91::/64. The PC is a Linux box running SuSE, supplied by Endesa and configured by UMU. The final users are IPv6 connected through dedicated 6POWER VLAN. There are three PC:

- Linux server: 2001:800:40:2c91::100
- Windows XP: 2001:800:40:2c91::101
- Windows XP: 2001:800:40:2c91::102

The PCs belongs to "Colegio San Valero", which is connected to Substation Z01141 in Zaragoza, through FO. From the TC, there are three repeaters connected in a low voltage branch. Linux box is connected to the second repeater, and Windows XP boxes are allocated in an office connected to third repeater. These last modems are also providing VoIP service with a IPv4.

The following picture shows the final layout.

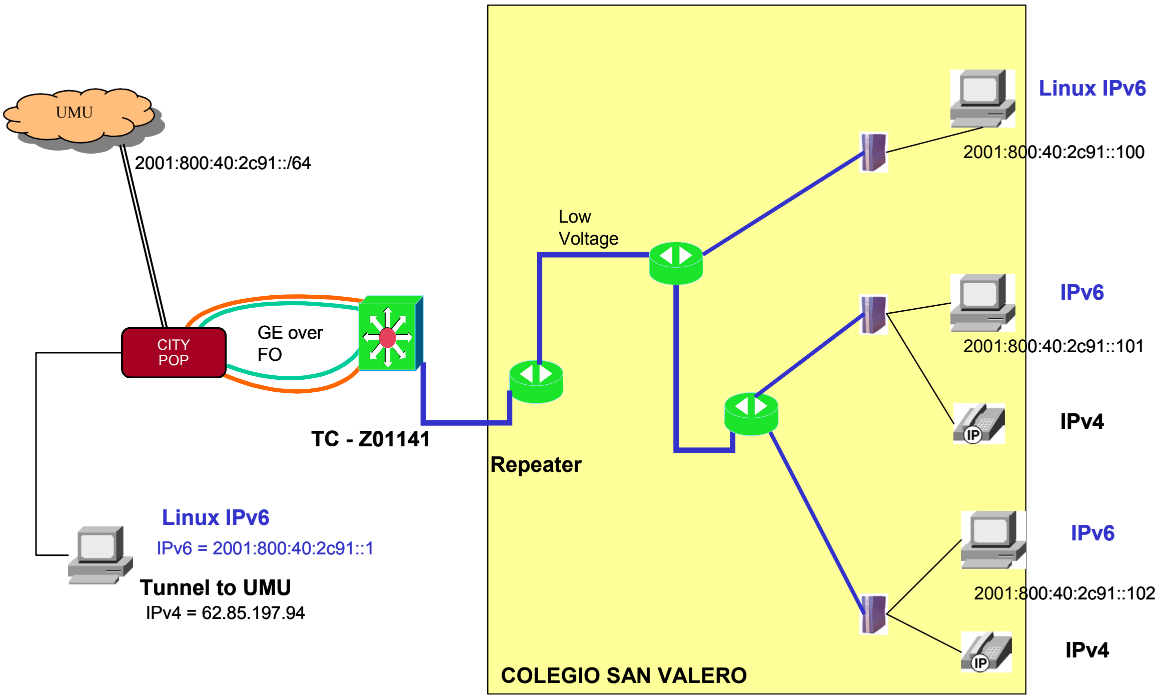


Figure 5-6: Endesa's Test-bed

5.4 6WIND Test-bed

DMZ segment is numbered 2001:660:3008:1950::/64. One PC runs services:

- OS - FreeBSD4.5 release
- DNS - bind 9.2.1

- WEB - apache 2.0.44

Second PC on DMZ is the IPv6 radius server

- OS - Linux 2.4.18
- Radius - FreeRadius + UMU patch for IPv6 transport

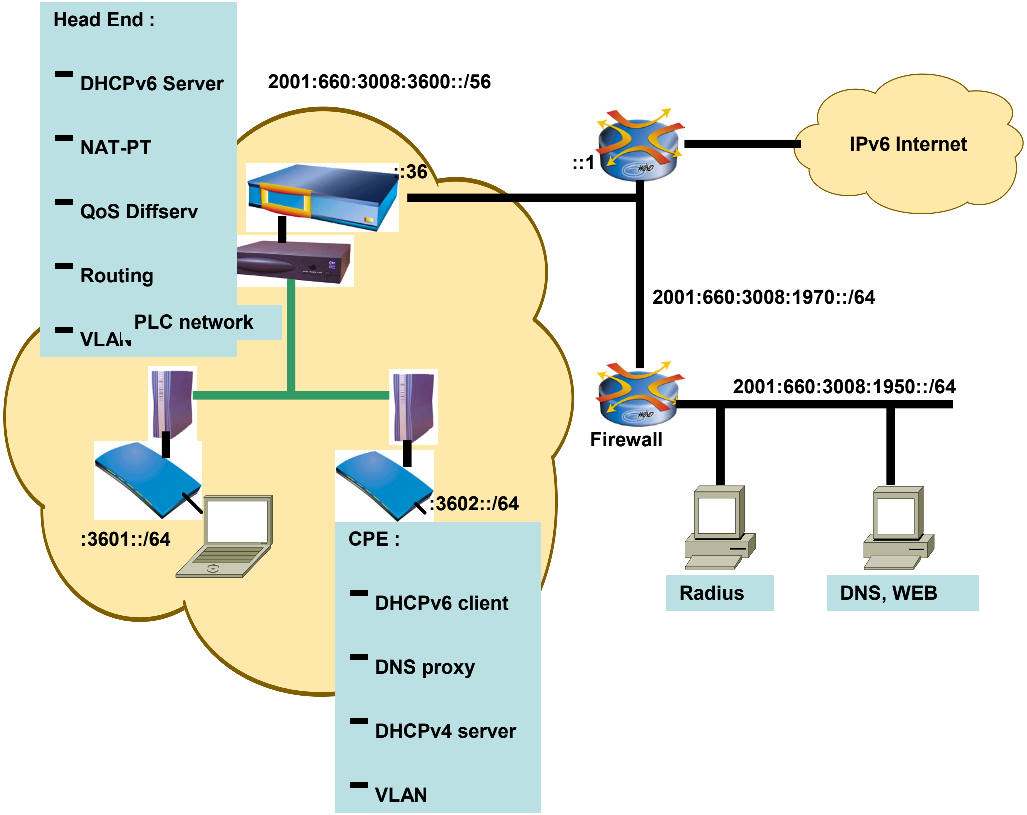


Figure 5-7: 6WIND's Test-bed

PLC network belongs to 2001:660:3600::/56 prefix. The Head End is divided into 2 pieces cross-connected on Ethernet:

- Router: 6WIND Edge.
- PLC/Ethernet modem which is a PC under Linux 2.4.18.

Two CPEs (2001:660:3601::/64 and 2001:660:3602::/64) are also two equipments:

- Router: 6WIND Gate.
- PLC/Ethernet modem which is a PC under Linux 2.4.18.

Laptops are running different operating systems: Windows XP, Linux, FreeBSD.

5.5 DS2 Test-bed

The basic DS2 test-bed is composed of the following parts:

- 2 PLC user modems (CPE).
- 1 PLC head-end (HE).
- 2 hosts running Windows applications.
- 1 host running Linux, performing routing and tunneling.

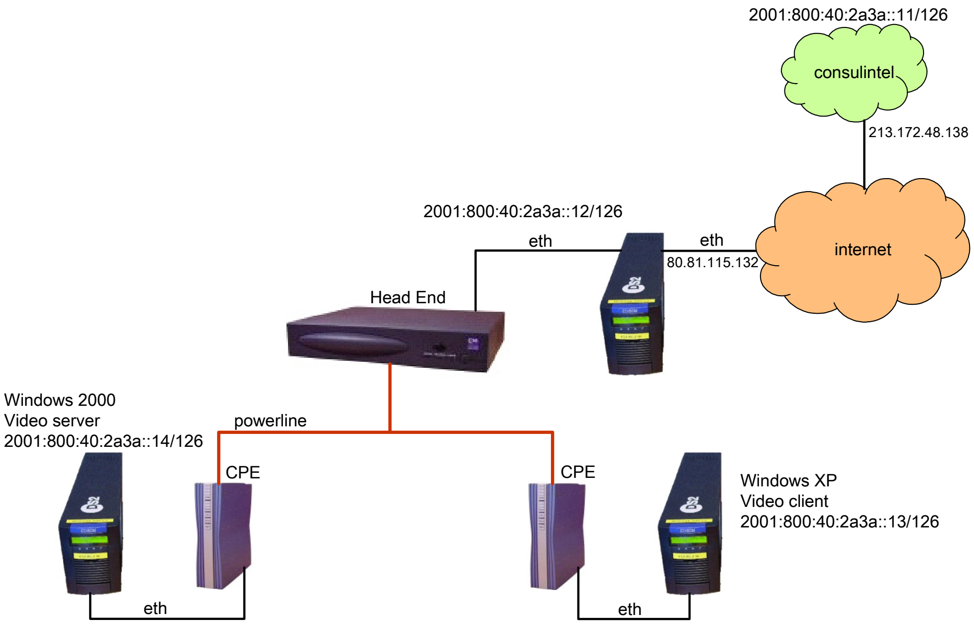


Figure 5-8: DS2 Test-bed

The whole network is connected to the IPv6 world through a tunnel with the network of Consulintel. DS2 has been assigned the IPv6 prefix 2001:800:40:2a3a::/126. Three IPv6 addresses were used for the three hosts mentioned above. On the IPv4 side, one public Internet address assigned to DS2 was used.

The test-bed is not permanent, as part of the equipment is sometimes used for other building demos of DS2 products not related to the 6POWER project.

The test-bed allows us to validate basic IPv6 functionality and also the advanced QoS features developed in the project. For specific tests, like subjective VoIP quality tests, we have temporally increased the size of CPEs, in order to stress the system. For other types of test (for example, PLC-level autoconfiguration) we have added more repeaters and CPEs in order to have a more complex topology.

5.6 MCL Test-bed

So far there are configured the following DNS entries here at MCL for the domains mcl.6power.org and mcl.6power.net.

- Dns: 2001:620:204::10
- Ping/ping6: 2001:620:204::12
- Gate: 2001:620:204::1
- Www: 2001:620:204::12

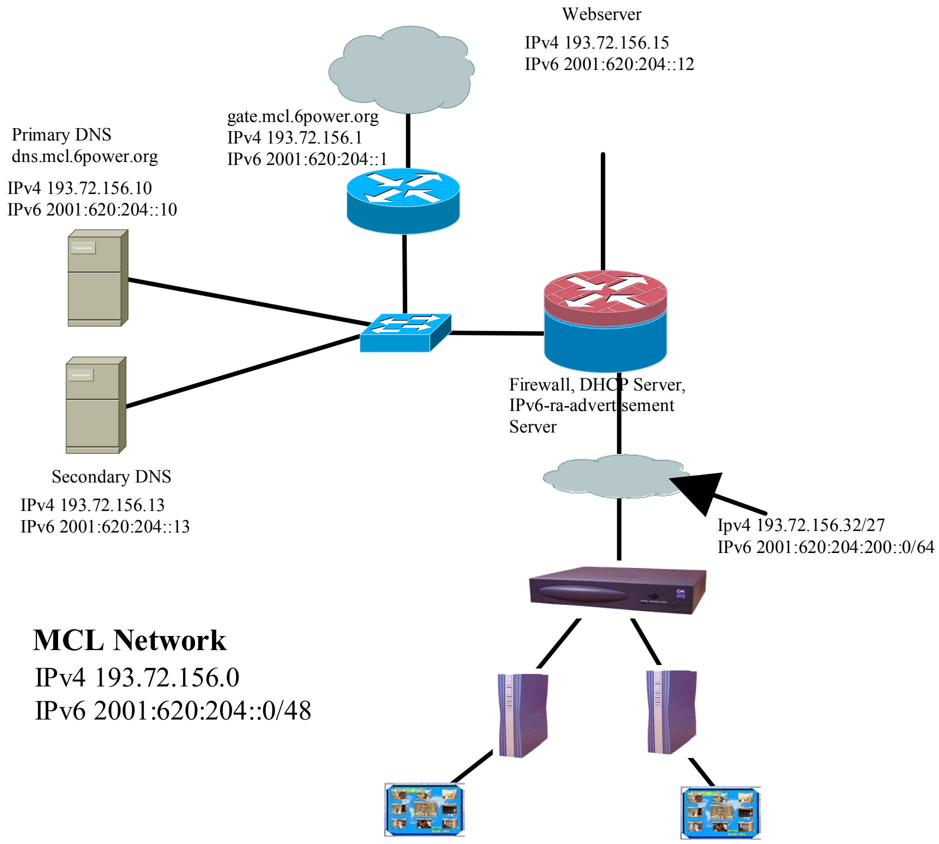


Figure 5-9: MCL's Test-bed

5.7 PACE Test-bed

The master IPv6 network in Pace is the **Saltaire** one. The connections come in from Consulintel (as shown in Section 2.2) straight to the Saltaire IPv6 gateway and from there you can access IPv6 hosts in Saltaire and **Cambridge**.

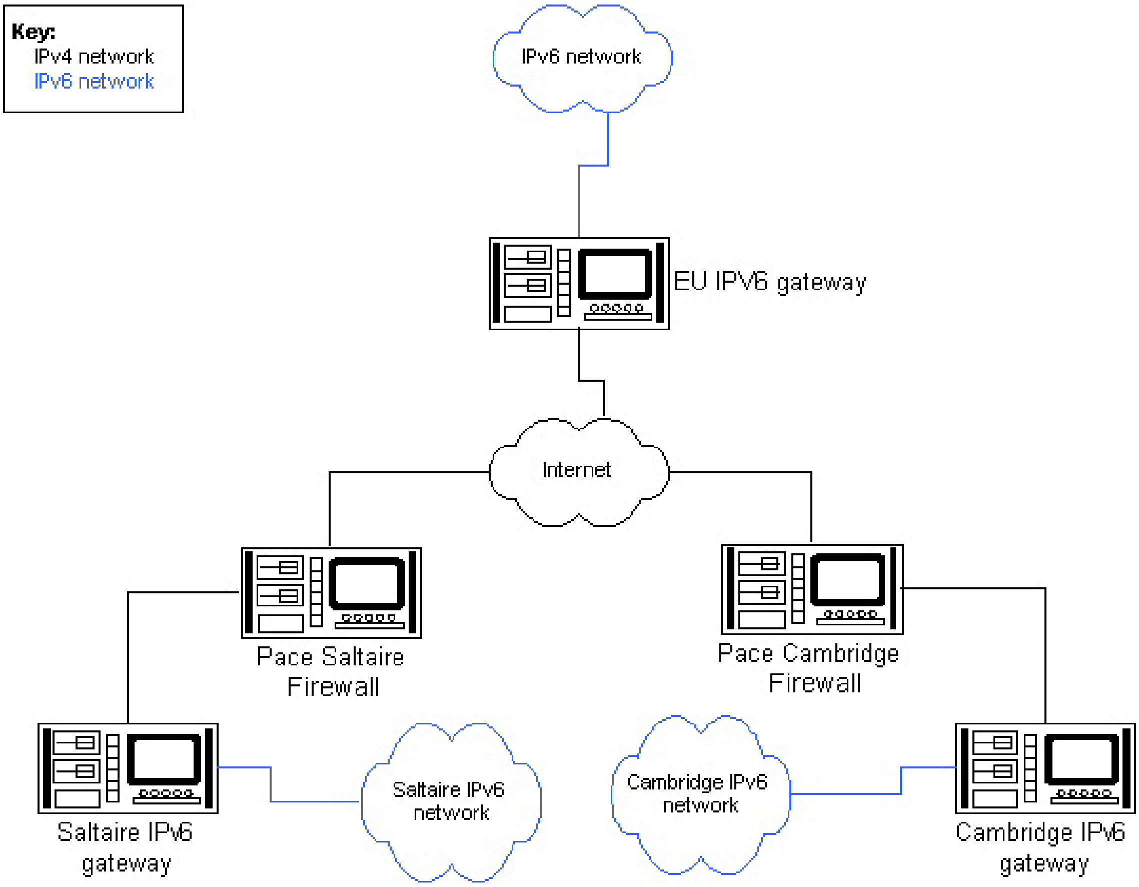


Figure 5-10: PACE's Test-bed

The Cambridge connections go out from the Saltaire gateway over the Internet and back in the Cambridge Firewall to Cambridge IPv6 gateway.

The connectivity between the three IPv6 networks is handled by encapsulating the IPv6 traffic, through the IPv4 corporate network (and the internet) and then using gateways to the IPv6 networks. This is done using IP protocol 41.

6. SUMMARY AND CONCLUSIONS

The study that was initiated in D3.1 regarding the network setup has been completed in this document, with the design and installation of several test-beds in different sites (one in each partner, typically). The planned interconnection over IPv6 between them has been a success, thanks to the possibility brought to us by Euro6IX and 6NET.

Those partners with no possibility of direct connection to any of those networks have been aided by other partners using IPv6 over IPv4 tunnels, so the establishment of a “global” test-bed in the project is now a reality. Of course, PLC is used in most partners, so as a general idea, this document proves the feasibility of our approach.

Not only represents this a big step towards our ultimate goal, but all this work can be seen as a prelude of the final public trial in Zaragoza, with real residential users, of which some hints were also given in this deliverable.

Although the results of the intensive testing of the tools installed in each test-bed will be part of a future deliverable, we covered here the details of the operation of the tools in each test-bed, and some of them gave initial results. Again, this is only the preparation of a full-fledged demonstration of the suitability and appropriateness of using IPv6 over PLC in commercial networks.

7. REFERENCES

[6POWER_D3.1] Design of the Basic IPv6/PLC Test-Bed, Deliverable 3.1, 6POWER Project (IST-2001-37613), April 2003.

[RFC3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney. “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”. RFC 3315. July 2003.

[IETF_PREFIX] O. Troan, R. Droms. “IPv6 Prefix Options for DHCPv6”, draft-ietf-dhc-dhcpv6-opt-prefix-delegation-05, October 2003.

[IETF_DNS] A.K. Vijayabhaskar. “The Name Service Search Option for DHCPv6”, draft-ietf-dhc-dhcpv6-opt-nss-00, October 2003.

[RFC2462] S. Thomson, T. Narten. “IPv6 Stateless Address Autoconfiguration”, RFC 2462, December 1998.

[IPComp] A. Shacham, B. Monsour, R. Pereira, M. Thomas. “IP Payload Compression Protocol (IPComp)”. RFC 3173. September 2001.

[Oakley] H. Orman. “The OAKLEY Key Determination Protocol”. RFC 2412. November 1998.

[SKEME] H. Krawczyk. "SKEME: A Versatile Secure Key Exchange Mechanism for Internet", from IEEE Proceedings of the 1996 Symposium on Network and Distributed Systems Security.

[ISAKMP] D. Maughan, M. Schertler, M. Schneider, J. Turner. “Internet Security Association and Key Management Protocol (ISAKMP)”. RFC 2408. November 1998.