Title:	Document Version:
Deliverable D3.1 **Design of the Basic IPv6/PLC Test-bed**	2.5

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

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
31/03/2003	03/04/2003	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:
Pedro M. Ruiz	ASSA	WP3

Authors (organizations):

Jean-Mickaël Guérin (6WIND), Antonio Beamud (ASSA), Sergio Fernandez (ASSA), Miguel A. Díaz, Álvaro Vives (Consulintel), Cesar Olvera (Consulintel), Jordi Palet (Consulintel), Chano Gómez (DS2), Antonio Gomez-Skarmeta (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 work has been organized in two different parts: Basic connectivity and advanced services. This deliverable describes the proposed design of the basic PLC network and discusses the different network design choices which have been considered and evaluated. The design of the advanced PLC network services like IP Multicast and QoS, although already started, will be reported in D3.2, which is due in month 15.

Keywords:

PLC network design, IPv6, network services, PLC bridges vs. routers, IPv6 prefix delegation, IPv6 multilink.

Revision History

Revision	Date	Description	Author (Organization)
v1.0	20/01/2003	Document creation, ToC and instructions for contributors	Pedro M. Ruiz (ASSA)
v1.1	07/02/2003	First contributions to topology discussions	Miguel A. Díaz, Álvaro Vives, Cesar Olvera (Consulintel)
v1.2	14/02/2003	Extraction of relevant points from the previous contribution, reshaping of the document and edition of the rest of sections except introduction and conclusions	Pedro M. Ruiz, Antonio Beamud, Sergio Fernandez (ASSA) Antonio Gomez-Skarmeta (UMU)
v1.3	20/2/2003	Improved the quality of some figures and general review and changes.	Álvaro Vives (Consulintel)
v1.4	28/02/2003	Added contributions regarding security	Pedro M. Ruiz, Antonio Beamud (ASSA)
v1.5	18/3/2003	Added contributions regarding routing.	Álvaro Vives (Consulintel)
v1.6	20/3/2003	Added Consulintel's network scheme	Álvaro Vives (Consulintel)
v1.7	21/03/2003	Added contributions regarding topology	Jean-Mickaël Guérin (6WIND)
v1.8	23/03/2003	Added contributions on addressing, routing and security	Pedro M. Ruiz (ASSA)
v1.9	28/03/2003	Added some address and external connection contents	Álvaro Vives (Consulintel)
v2.0	31/03/2003	Edition of every missing part, complete review, and finalization of the document	Pedro M. Ruiz (ASSA)
v2.1	31/03/2003	Editorial modifications, added description of Zaragoza test-bed, added architecture without router in customer side, added PLC autoconfiguration	Chano Gómez (DS2)
v2.2	31/03/2003	Final polishing of the document	Pedro M. Ruiz (ASSA)
v2.3	03/04/2003	Minor edits and template update	Jordi Palet (Consulintel)
v2.4	05/07/2003	Small error corrected	Jordi Palet (Consulintel)
v2.5	25/11/2003	Small error corrected	Jordi Palet (Consulintel)

Executive Summary

The design of IPv6 PLC networks has demonstrated to require special knowledge about the internal PLC functionality and implementation. The PLC operation is different to a BMA (Broadcast Medium Access) network, so the overall network performance may strongly depend upon the network design. Whereas in traditional Ethernet-like networks it is usually assumed a switched environment as the better access network design, these principles do not always hold in PLC networks. Hence, the large discussion about the use of PLC devices acting as bridges or routers between the Head End (HE) and the Customer Premises Equipment (CPE).

We have analyzed different alternatives for different user scenarios including home users, professionals and mixed scenarios. For these scenarios we have identified a suitable subset of network designs for each scenario being the best trade-off between efficiency, simplicity, facility to introduce and exploit IPv6 functionalities as well as low cost. For the different solutions we have discussed all the different network design aspects including among others topology, routing, addressing, autoconfiguration, security, etc.

This document present our findings in the design and deployment of basic IPv6 PLC networks whereas the design and implementation of advanced features will be addressed and included in D3.2 which will be due in month 15.

Table of Contents

Table of Figures

1. INTRODUCTION

The WP3 of the 6POWER project is in charge of the design, setup and operation of the PLC network to be used both for the internal and public trials. This first deliverable (D3.1) is devoted to the description of the first interim design of the PLC network. Thus, it is mainly focused on the description of the different design issues (e.g. topology, addressing, DNS, etc) regarding the basic network services, which have been analyzed in the first half of A3.1. The network design in A3.1 will continue in parallel with the implementation of the basic PLC network. Future outputs regarding the design of advanced PLC network services (i.e. multicast, QoS, etc.) will be incorporated into D3.2, which is due in month 15 (October 2003).

Much of the work described here, especially regarding the internal PLC network design, is strongly related to the internal operation of PLC devices. This operation is clearly described in WP2 deliverables D21 [1] and D2.2 [2]. These deliverables describe the MADBRIC architecture, which is one of the key inputs we have consider when taking internal PLC design decisions.

In general, the inter-PLC part of the network can be any IPv6 network based on different layer 2 technologies. The connections among PLC access networks will be done be pure layer 3 routing. We will have to take into consideration special properties of PLC access networks when designing that part of the network. Additionally, as described in [2], the PLC equipments, which will take part in the PLC access networks, will be the Head End (HE), Repeaters (RPT) and Customer Premise Equipments (CPE). HEs are point of access to the core IP network, RPTs are optional depending on the link capabilities between HE and CPE, and finally CPEs are the devices to which the customer's networks attach. These PLC devices, according to type C MADBRIC architecture can act both as bridges or routers. As we will show in the internal PLC design, only with a subset of these possible roles we can cover all the scenarios.

This document presents a top down approach in which relevant networking scenarios are identified before the technical analysis starts. This let us focus on relevant technical challenges instead of analyzing a wide plethora of technical problems, which may never appear in real PLC scenarios.

To reflect this top-down approach, the remainder of this document has been organized as follows: Section 2 describes and identifies real PLC networking scenarios. Section 3 deals with the design both of inter-PLC and internal topologies. Section 4 present the addressing plan design. The routing issues regarding our PLC network environment is explained in section 5, whereas section 6 describes the design issues regarding the basic networking services. Section 7 deals with the problematic regarding the interaction with external networks like Euro6IX and 6NET. Section 8 anticipates some of the design issues regarding multicast, QoS, etc. that we will have to face during the second phase of A3.1. The detailed design of the 6POWER PLC test-bed is described in section 9, and finally section 10 gives some conclusions, recommendations and future research issues to look at further.

2. BASIC NETWORKING SCENARIOS

To analyze the user's requirements in the different possible scenarios before providing technical solution, we will follow a top-down approach. We will start with an analysis of the requirements of these different possible scenarios, from which we will extract topology constraints, to be dealt with in the design phase. This approach will allow us to reduce the technical analysis to those topologies, which actually cover the user's requirements.

There will be mainly two types of users: home users and professionals (e.g. companies). The demands of these different kinds of users will be different. In fact, we will find these kinds of users in our 6POWER PLC trials. The partner's networks are in some sense professionals, while we will deploy public trials including home users.

Home users, whose scenario is depicted in Figure 2-1, are basically those who wish to use their connection at home during their leisure time usually do not have different terminals and do not provide services. However, future IPv6 trends indicate that each time more home users are having several devices, require the possibility to provide services (e.g. access to home networking device from outside home), etc. Some of the requirements for these users are:

- Connectivity to Internet for elastic applications (e.g. www, e-mail, etc).
- Audio/Video streaming with minimal QoS requirements.
- Real-time IP-based services like telephony, videoconferencing, etc, which usually require some QoS guarantees.
- Home network with no too many PCs (typical only one) and a few home-automation devices.

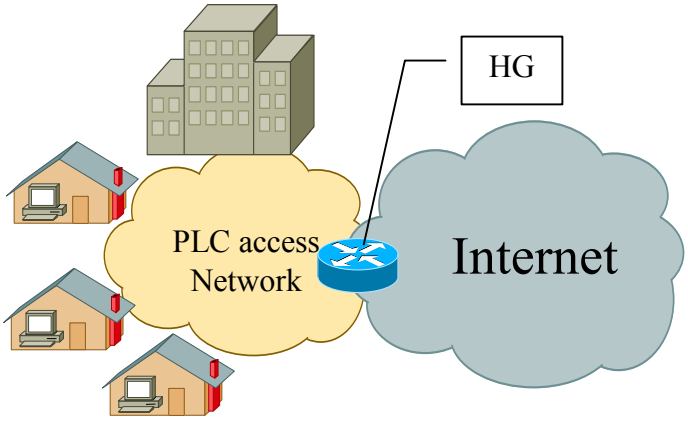

Figure 2-1: Home Users Scenario

Professional users usually have higher needs and requirements which require not only higher bandwidth but more complex network services and mechanisms. This scenario is shown in Figure. 2-2. These requirements may include among others:

- Internal network with multiple terminals connected, whose number will depend of course on the size of the company.
- The network may span over different parts of the building.
- Network applications are still required (i.e. www, e-mail, etc).
- Public services must be possible to be provided (e.g. web-server, DNS server, etc.).
- Bigger aggregated bandwidth both for real-time and elastic applications.

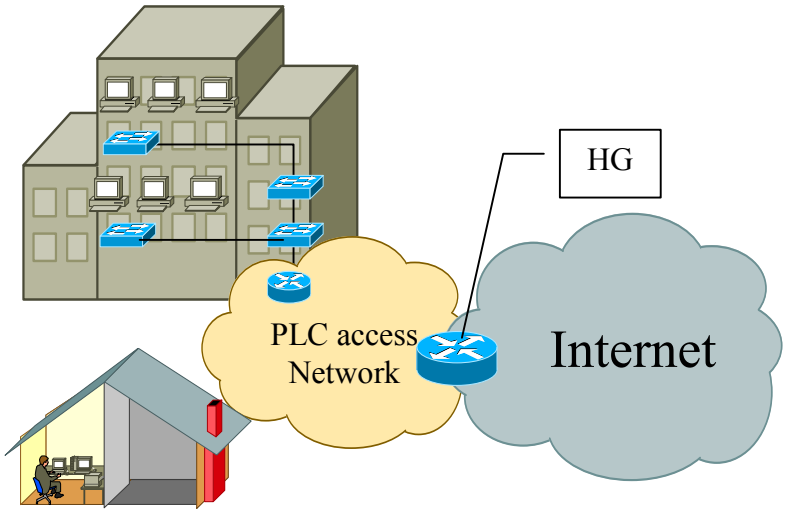

Figure. 2-2: Professional Users Scenario

The third possible scenario, which is depicted in Figure 2-3, is a mixed environment in which home users and professional users may share the same building.

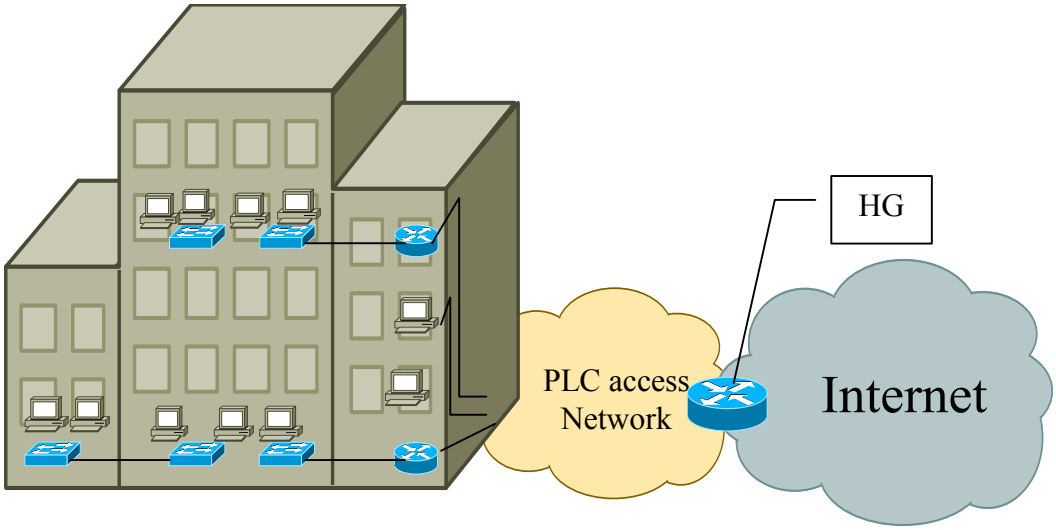

Figure 2-3: Mixed Users Scenario

The next section presents a discussion on the topology both for the interconnection of the different PLC access networks and the internal topology of the PLC access networks themselves.

3. TOPOLOGY OF THE BASIC PLC NETWORK

In this section, we discuss the different topologies to connect different PLC-access networks as well as the candidate internal topologies for the PLC access network in each of the different scenarios described above. We will focus our inter-PLC access network topology discussion at layer 3. The issue of the layer 2 technologies (e.g. WDM, ATM, PoS, etc.) to be used to interconnect different HEs is out of this deliverable as long as there aren't special requirements in PLC networks regarding this issue.

3.1 Inter-PLC Access Networks Topology and External Connections

The interconnection among different IPv6 PLC access networks is not different from the interconnection between different IPv6 access networks. In fact, PLC access networks are just another access technology as DSL, ATM, RDSI, or PSTN. At layer 3 a Core IP network will connect these access networks.

In the special case of our project, this core network will be based on IPv6. In addition, as many of the partners in the consortium are participating in Euro6IX or 6NET projects, we will use the European-wide core networks provided by these IST projects, as connectivity for our individual PLC test-beds. Partners not taking part on Euro6IX or 6NET consortiums will connect using IPv6/IPv4 tunnels to the rest of partners. Figure 3-1 shows the inter-PLC access network topology for the 6POWER PLC test-bed.

Euro6IX is going to be the "de facto" backbone to achieve interconnection between partners. This is because several partners are already connected to the Euro6IX network. This partners use some of the addresses allocated inside Euro6IX project. Partners that are no directly connected to Euro6IX, can both negotiate the direct connection or by means of an already connected partner. However, for simplicity we have established connections to partners, which are already part of Euro6IX.

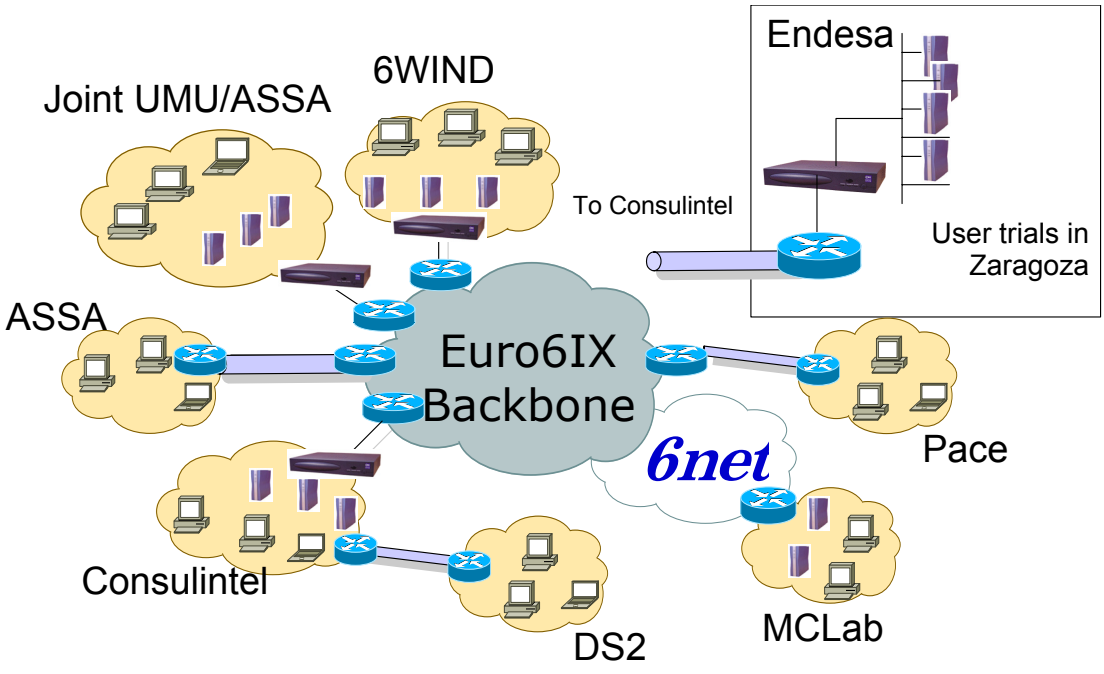

Figure 3-1: Interconnection Among 6POWER PLC Test-beds

Other partners (e.g. MCL) will be connected through the 6NET network, which is has already a peering agreement with the Euro6IX network. This scheme allows the IPv6 connectivity in an easy way, as it uses the already existent knowledge and infrastructure.

This topology facilitates the setup of the test-bed in the second phase of WP3. This is mainly because it resembles the distributed nature of the project, and facilitates the distributed management of each partner's test-bed. This will also facilitate the provision of other network services (e.g. security) as discussed in following sections.

3.2 Individual Test-bed Topology

The most important issue regarding the internal PLC access network topology is related to the router or bridge functionalities, which network devices can take. In subsequent diagrams these functionalities will be depicted according to Figure 3-2.

Figure 3-2: PLC Network Device Representation

In all the cases, the HE will act as a router, and the RPTs and CPEs may act as routers or bridges. RPTs are only used when there are long distances between HE and CPEs or the user's density is high. For the sake of generality, we will assume that RPT are always present in our scenarios[1]. In the following sections we analyze the different possibilities to get the better role for each of the devices in each of the three scenarios described in the previous section. In addition to the functionality and technical aspects, we will also take into account factors such as the costs of the equipments, etc.

In general, bridges are cheaper and have a high throughput. Routers usually have a little fewer throughputs and are more expensive. However, bridges can only work at the link layer whereas routers are more versatile and flexible. Our goal is to achieve a good trade-off to satisfy the user's requirements at the same time that we reduce the cost of the equipments and the operation costs.

In general, there are several combinations, which end up in severe technical issues, which are not solved in the Internet community so far. For example, having a HE-router, an RPT-router and a CPE-router (or even a customer owned one connected to its CPE-bridge) would require the support of a hierarchy of prefix delegations to be able to efficiently support autoconfiguration. This is a really difficult problem for which there is not a good solution now, and which becomes very complex especially when the prefix requirements from the customer changes, and these delegations need to be changed hierarchically. It is much simpler in the general case to have always an RPT-bridge connecting the HE-router to a CPE-router (or a customer router through a CPE bridge).

The only issue with having a RPT-bridge is that there might be too big broadcast domains in cases in which there are not intermediate routers between the HE and the user premises. However, this problem is much simpler than the previous one, and can be simply overcome just installing CPE routers in the end-user premises (i.e. as it is currently done with xDSL lines at the present moment).

[1] *Note that this assumption does not make us loss generality in our proposed solutions.*

There are some techniques that can be used for partially solving the problem of big broadcast domains that do not require the use of CPE or RPT routers. These techniques, that include layer-2 VLANs, effectively reduce broadcast traffic and are currently being used in power line access networks that are based on layer-2 devices.

In addition, as these final users might initially still use some IPv4 applications and services, it might be interesting to offer them some transition mechanism so that they can use during some time both IPv4 and IPv6. In that sense, as many of the transition mechanisms are based on routers (i.e. layer 3), it seems reasonable to do this mechanism automatically and near the user, so that our core network could be IPv6-only and the operation of the core could be reduced. This is also an argument in favor of placing a CPE-router whenever is possible.

Taking this into consideration, the number of possible topologies is clearly reduced. In fact, if we assume the HE-router and RPT-bridge, the only two cases are CPE-bridge or CPE router depending on the concrete scenario. We will analyze which option is better in each of the different scenarios.

In addition, we need to consider the case when CPE acts as a router and has more than one LAN interfaces. This case is common to both home users and professional scenarios.

3.2.1 Home Users Scenario

This basic scenario consists of end users accessing to the basic services like e-mail, web-browsing, etc. They do not manage their own web or mail servers, their own DNS, etc. Most of the services they access are provided outside the PLC network. Most of the configurations in the user's equipments and networks should be automatic, so that the network operator does not require big expenses in customer support. This would certainly reduce the costs and simplify the deployment, configuration and operation of the PLC access network.

These users will use one or several PCs without any internal network. These users do not have any special need for firewalling or internal routing or switching. For all these functionalities they rely on their ISP. Possible solutions in this case are the CPE being either bridge or router. For the customers' equipments to get autoconfigured, they need to receive a RA providing a /64 prefix. The best approach in this case is that the CPE acts as a router. Thus, the HE delegates a /64 prefix to the CPE which will announce it into the customers' LANs. This will easily support the automatic additions of more equipments by the customer without any the need to change anything in the configuration of the PLC network. This solution is shown in Figure 3-3.

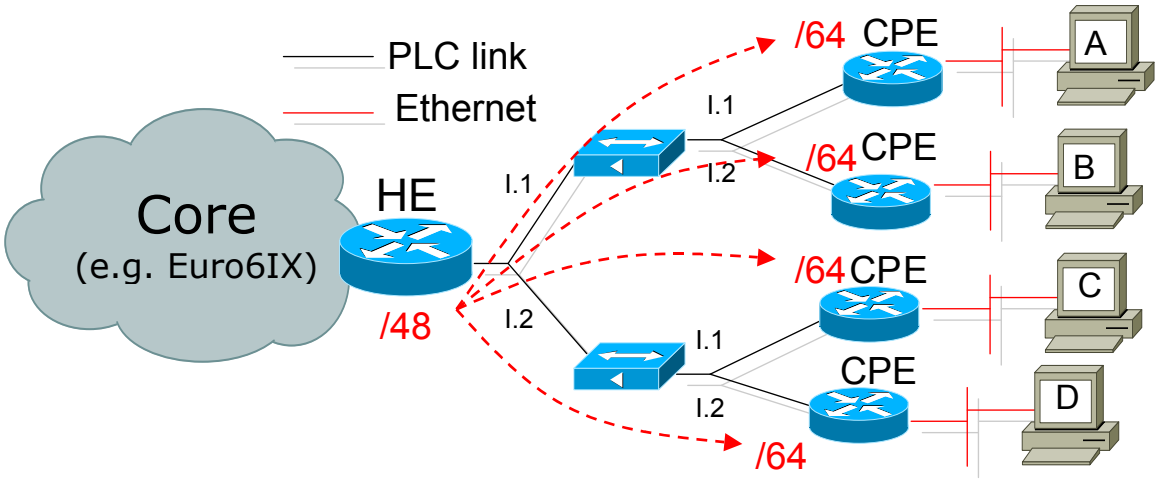

Figure 3-3: Proposed Topology for the Home Users Scenario

3.2.2 Professionals Scenario

This is the case in which customers can be entire networks and customers may even have their own routers, firewalls, etc. Given these requirements, and provided that using a CPE-router would cause the prefix delegations and other mechanisms to become extremely complex, it is much better to use CPE-bridges. In this case, the prefix delegation is performed from the HE to the router owned by the customer. This solution is presented in Figure 3-4.

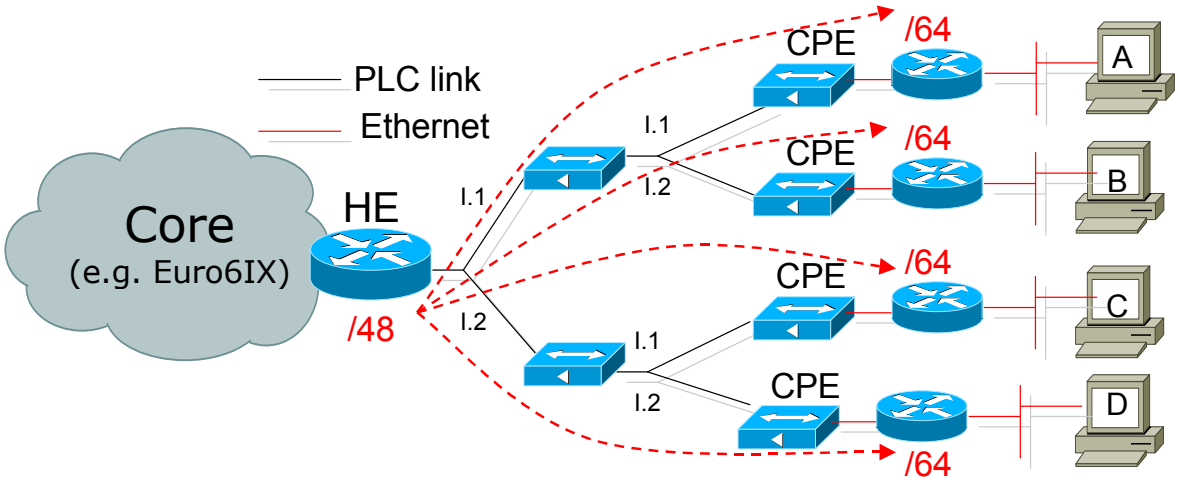

Figure 3-4: Proposed Topology for the Professionals Scenario

3.2.3 Mixed Scenario

There may appear both users and professionals. In fact, professionals are very likely to have their own networking equipments and internal networks (i.e. router, bridges, etc.). In that case, if the CPE acts as a router, we enter into the same problems of having hierarchical delegations. Thus, in that specific case, it is better to use CPE-bridges, connected to the user's router via Ethernet. The HE will delegate the corresponding prefix into the customer's routers (i.e. CPE for users, and customer-owned router for professionals). This perfectly works in this combined scenario as it is shown in Figure 3-5.

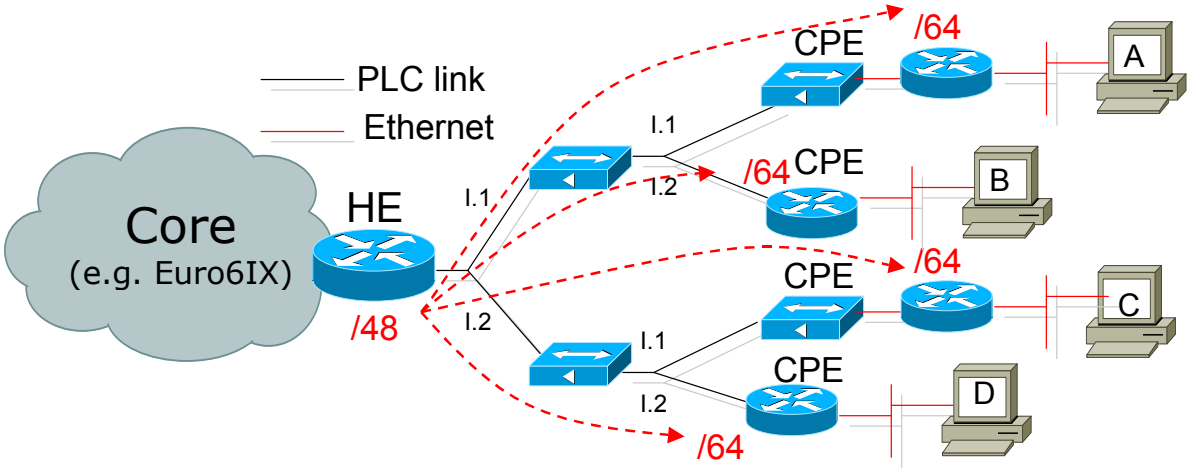

Figure 3-5: Proposed Topology for the Mixed Users Scenario

So we can extract the following general rule which offers a good trade-off, works with existing IPv6 mechanisms, and solves the different topology issues: ***In the internal PLC network***

topology the HE will behave always as a router, the RPT, if any, will behave as a bridge, and the CPE will behave as a router when there is no other router in the customer network or as a bridge, when the customer is using its own router.

3.2.4 CPE Router with Multiple LAN Interfaces

This scenario applies to both users and professionals, when there is a router, the one that belongs to customer behind CPE bridge, or CPE router itself. To allow customers' equipment to get autoconfigured, a RA must be advertised on each of the links attached to the router.

Two options are possible, depending on length of prefix delegated by HE to the customer.

HE delegates a prefix whose prefix length (pL) is lower or equal to 64. The router is able to subnet this prefix in order to build 2^(64-pL) /64 prefixes, pL <= 64. One built /64 prefix is required for each of its LAN interface for sending RA. For example, given a prefix P::/56, a router can build up to 256 prefixes, P:1::/64, P:2::/64, etc.

Therefore the number of /64 that the router can build is limited. Simple case is HE delegated one /64 (pL = 64) and the router has two interfaces. In this case HE must be configured to assign more than one prefixes to delegate to customer site.

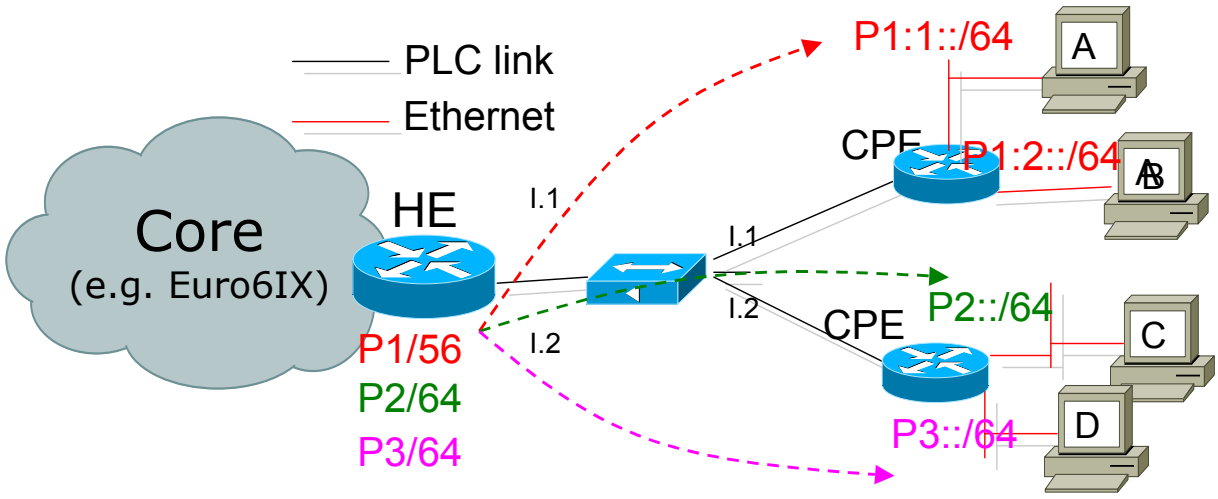

Figure 3-6: Proposed Topology for CPE Router with Multiple LAN Interfaces

In conclusion the router need to ask for as many as prefixes in order to be able to build a /64 prefix for each of its LAN interface.

In practice, the router in the customer's premises will rarely have more than ten interfaces, in particularly in Home Users scenario. That is to say one delegated prefix P::/60 per customer would be enough.

However it could be an administrative policy, on the delegating router, to assign /64 prefixes on demand.

3.2.5 CPE Bridge with no Router

This last scenario is maybe not optimal from a technical point of view, but it can become very common in power line access networks that were originally designed as layer-2 networks with IPv4 addressing and that were later upgraded to IPv6 without changing the user CPE.

In this scenario, the power line CPE is a legacy layer-2 bridge and the customer has one or more computers directly connected to the CPE. The customer can have a mixture of IPv4-only and dual-stack IPv6/IPv4 computers.

Customer's computers can get their IP addresses from the HE-router using IPv4 DHCP, IPv6 stateless autoconfiguration or DHCPv6.

In this scenario, the network operator would have a clear method to encourage users to upgrade their computers to IPv6: customers with IPv4-only would connect to the Internet through some type of NAT mechanism (so some services would have limited functionality) while customers with IPv6 addresses would have direct access to the Internet without translation mechanisms that interfere with their applications.

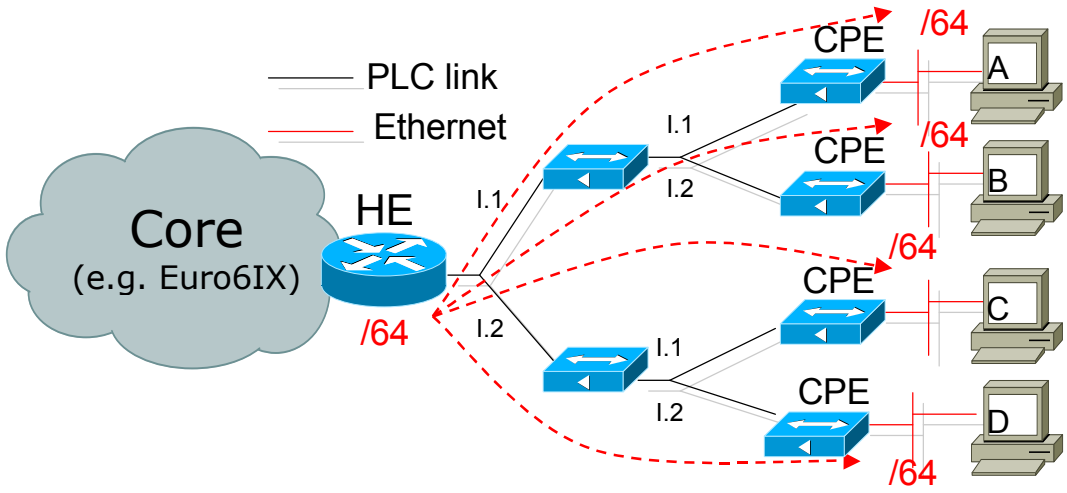

Figure 3-7: CPE Bridges with no Routers in the Customer's Network

4. ADDRESSING PLAN

There are different addressing requirements in different parts of the overall network. These parts are as follows:

- Inter-PLC networks addressing.
- Management of customer's addresses.

4.1 Inter-PLC Access Networks Addressing Plan

It is very important to separate what would be the addresses at both ends of the network connecting PLC access networks, from the addresses, which are used inside the access networks.

In general a big PLC operator, will generally have for their use a /32 prefix from their RIR (e.g. RIPE-NCC in Europe). This prefix will be used to offer addressing to our their customers. This does not mean that the IPv6 addresses of the internal network of the operator need to use this prefix. In fact, they could use any internal prefix (e.g. site-local) so that their network equipments could not be accessed from outside their internal network. Of course, access routers must use addresses from this /32 prefix (precisely from the sub-prefixes of this /32 prefix delegated to the specific customer) in the external interface to the customer's networks.

In the concrete case of the 6POWER project, most of the addressing decisions for the Inter-PLC Access Networks addressing are motivated from the use of the Euro6IX and 6NET projects, as a backbone network for the interconnection of our PLC access networks (i.e. 6POWER partners' networks). Thus, the overall prefixed will be those which are already allocated for the network of these projects. The addresses to be used in the external interface to the IPv6 core network for each of the partners are summarized in the next table.

	Home Gateway	Internal prefix
Partner	**IPv6**	**IPv6**
6WIND	3ffe:304:124:3600::36	3ffe:304:124:3600::/56
Consulintel	2001:800:40:2a0b::1	2001:800:40:2a0b::/64
DS2	2001:800:40:2a3a::12	2001:800:40:2A40::/62
MCLab	2001:620:204:500::1	2001:620:204:500::0/64
UMU/ASSA	2001:800:40:2c00::2	2001:800:40:2c50/60
Trial users	2001:800:40:2a3a::22	2001:800:40:2A44::/62

Figure 4-1: Inter-PLC Addresses

4.2 Customer's Network Addressing Plan

The internal addressing plan within each of the PLC test-beds is something that will depend very much on the specific topology and services to be offered. For example, having different subnetworks connected to the same HE, will require the prefix allocated for the HE to be delegated[4] to customers' equipments. Currently DHCPv6 [5] has been proposed to do that,

although it is still an open IPv6 issue. In addition, for customers attaching to the PLC network, autoconfiguration [3] of the addresses should be required.

Another option is the autoconfiguration of the internal PLC devices themselves. In that case, more advanced mechanisms [6-10] discussed in the IETF Zeroconf WG could be required. This kind of solutions will not be available in the basic PLC network, but it is something we will closely look at in future evolutions of the PLC network.

All these autoconfiguration ideas are further explained in our autoconfiguration section below.

Different PLC test-beds can have different addressing schemas (and even topologies). This would enrich the consortium's knowledge and expertise regarding the different available options. In the following sections we illustrate some of them.

4.2.1 Addresses in joint UMU and ASSA Test-bed

As it can be seen in the next figure, the prefix used by the joint UMU/ASSA test-bed is in the Euro6IX address space. In fact, it is a subrange of the UMU's IPv6 addresses in their Euro6IX test-bed. The range used for the 6POWER test-bed is 2001:800:40:2c50/60 and it is internally divided into several subnets with prefixes 2001:800:40:2c51/64, 2001:800:40:2c52/64, 2001:800:40:2c53/64 and 2001:800:40:2c54/64.

In case of any other 6POWER requiring an IPv6 tunnel to access the 6POWER IPv6 network, it can be easily provided a through the router labeled as 'Access Router'.

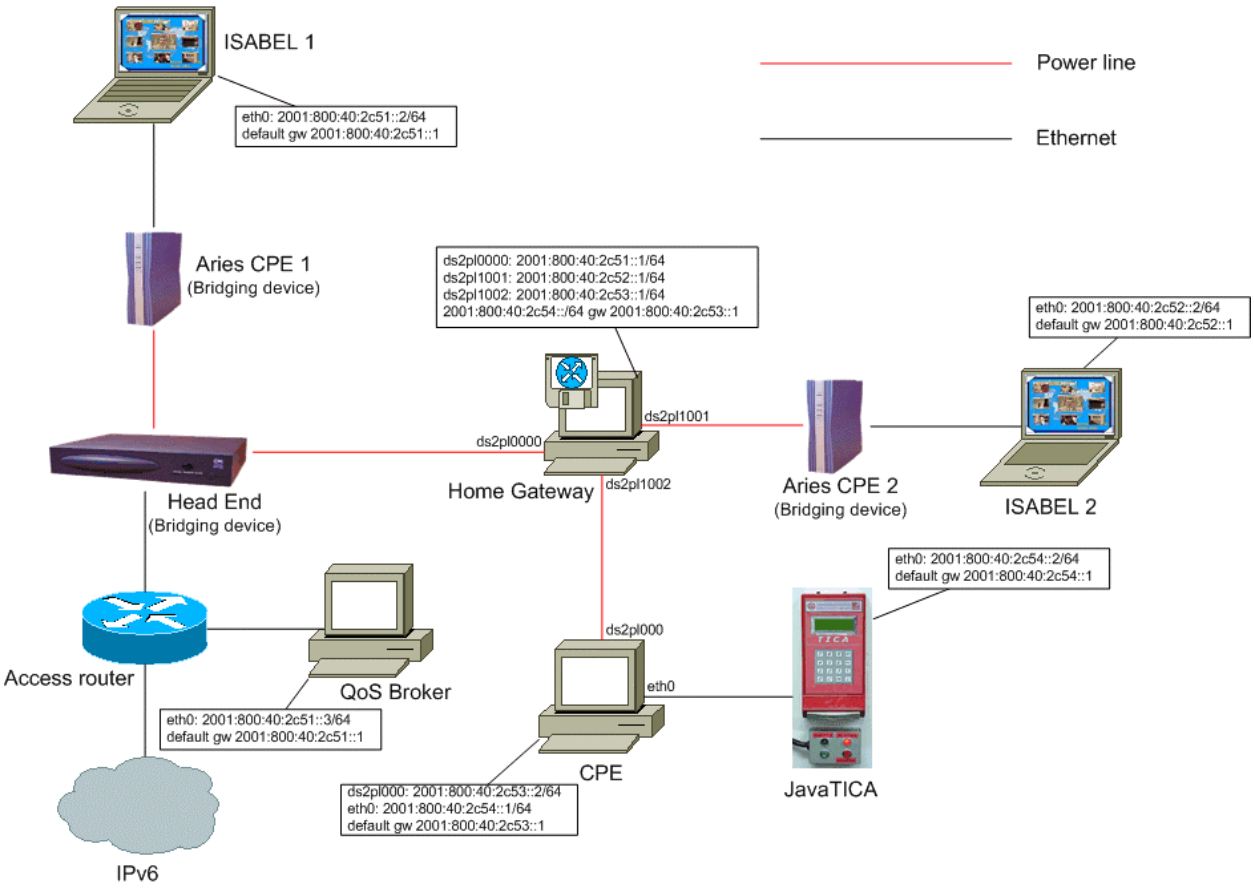

Figure 4-2: UMU's Test-bed

4.2.2 Addreses in Consulintel's Test-bed

We have designed our test-bed as being part of the Euro6IX network. So we have assigned addresses among the prefix we have received.

Also we had in mind the possibility of giving connection to another partner by means of an IPv6-over-IPv6 tunnel, allowing both the connection to our network and to Euro6IX backbone.

The following table and picture shows the addresses used and the network scheme.

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	80.81.115.132	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
Available	213.172.48.138	2001:800:40:2a3a::31/126	TBD	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

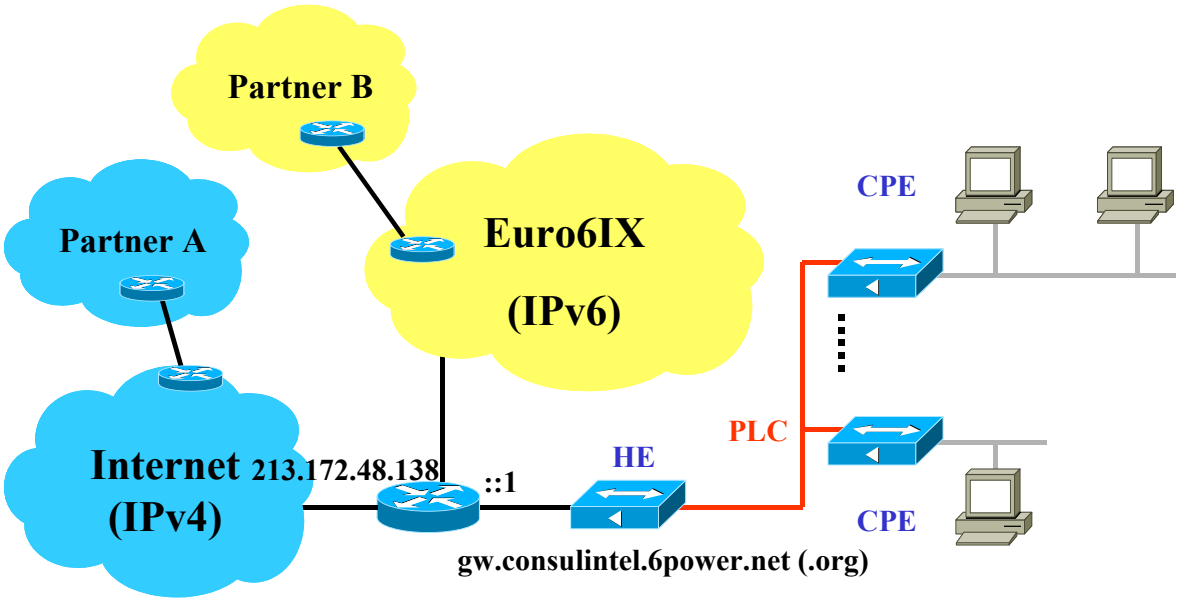

Figure 4-3: Consulintel's Test-bed

Partner A is a partner with IPv4 connectivity. It can makes a tunnel to Consulintel's premises, receiving the corresponding /62 prefix.

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

Also forward and reverse DNS lookups have been enabled for at least our router/gateway in the PLC-IPv6 network. This way gw.consulintel.6power.net (.org) could be used to test connectivity using ping6 and traceroute6.

5. ROUTING

Regarding routing issues we can divide the overall network in three domains, namely the user domain, the PLC-provider domain and Inter-PLC networks domain:

- The user domain includes the network from the CPE towards the user.
- The PLC-provider domain includes the network between the HE and the CPEs.
- The top-level domain includes the network that interconnects the HEs.

We will mainly focus in the last two.

5.1 Inter-PLC Networks Routing

The internal routing inside PLC Networks will be very simple because the PLC topology is very static. In this part of the network the routing will be only deployed in the scenarios in which some PLC equipments act as routers. In those cases, although routing protocols can be configured, it will usually be enough if we configure static routing due to the existence of single paths, and the static PLC topology.

5.2 Routing in Internal PLC-Provider Networks

The cases we are considering in this document are the basic ones, with the RPT being a bridge. In this cases the HE will be the responsible of managing the prefixes to be delegated to each CPE-router or to the user's router behind a CPE-bridge.

For each prefix assigned to customers, HE as delegating router will actually set dynamically a static route for this prefix through the (logical) interface from which the requesting router asks.

HE should perform reverse path forwarding (RPF) on logical interfaces to prevent not-assigned prefix spoofing or miss-configuration.

The mechanism for delegating the prefix to the routers is to be defined. Actually the DHCPv6[5] prefix delegation mechanism is a good candidate, as there are available implementations that could be used.

5.3 Routing in User Networks

Here the routing is achieved by means of the autoconfiguration.

In case of having a CPE-router, it will receive a prefix to announce to each of its subnetworks. If we have a CPE-bridge with a customer router connected to it, the user's router should have the ability of receiving the delegated prefix for each of its subnetworks.

The same ideas mentioned above applies to the way that the CPE-router or user's router obtains their prefixes.

Anyhow, the router in customer premises will set the default route to the upstream link, from where it would get the delegated prefix. It could use the link local address or the interface for this. As it can be seen the prefix delegation [5] will be a key piece to deploy in our PLC network

when ready. In the meanwhile, we will use statically configured default routes in the partners' routers so that a basic interconnection of the test-beds can be easily achieved. When the network equipment supports the prefix delegation we will introduce it.

6. BASIC NETWORK SERVICES

This section covers the design of the basic network services. Advanced services like network layer QoS and multicast are introduced in following sections, but the real design for those services will be presented in D3.2.

6.1 Domain Name Service (DNS)

DNS is one of the basic services to be deployed. In this basic network we will analyze the "basic" DNS ([11-14]). Issues like Dynamic DNS or DNSSEC could be considered in further designs, but the participating partners must agree on its deployment.

In this section is just addressed the design of the service. A configuration "cookbook" could be produced, from the know-how of related partners and the experience gained inside the project, for being used in deployment. Anyhow some practical guidelines will be given.

Regarding our design, the following issues must be taken into account:

- The DNS transport must be differentiated from the DNS resource records (RRs).
- We have got IPv4 and IPv6 DNS transport.
- We have got IPv4 (A, PTR) and IPv6 (AAAA, PTR) RRs.
- Nowadays there is no complete IPv6 DNS transport, from root to the desired domain.
- IPv6 RRs could be obtained using IPv4 transport and vice versa.

Based on this, the use of dual stack servers with both IPv6 and IPv4 connectivity is the best choice.

As it was shown in the topology section, we have a minimum IPv6 segment from the user to the WAN. There must be one IPv6 accessible DNS server within this IPv6 segment, but for recursive lookups that start from the root domain, IPv4 connectivity is a must.

The following figure illustrates the process of resolving a domain name that is neither in the zones nor in the cache of the DNS Local server. The user looks for www.6power.net and asks its DNS server. This one starts a recursive lookup from the root domain until it reaches the 6power.net server, which also has an AAAA RR for www.6power.net and returns it to the local server. The local server then returns the AAAA RR to the PLC/IPv6 user.

In the figure the red arrows represents IPv6 DNS transport and the blue ones represents IPv4 DNS transport.

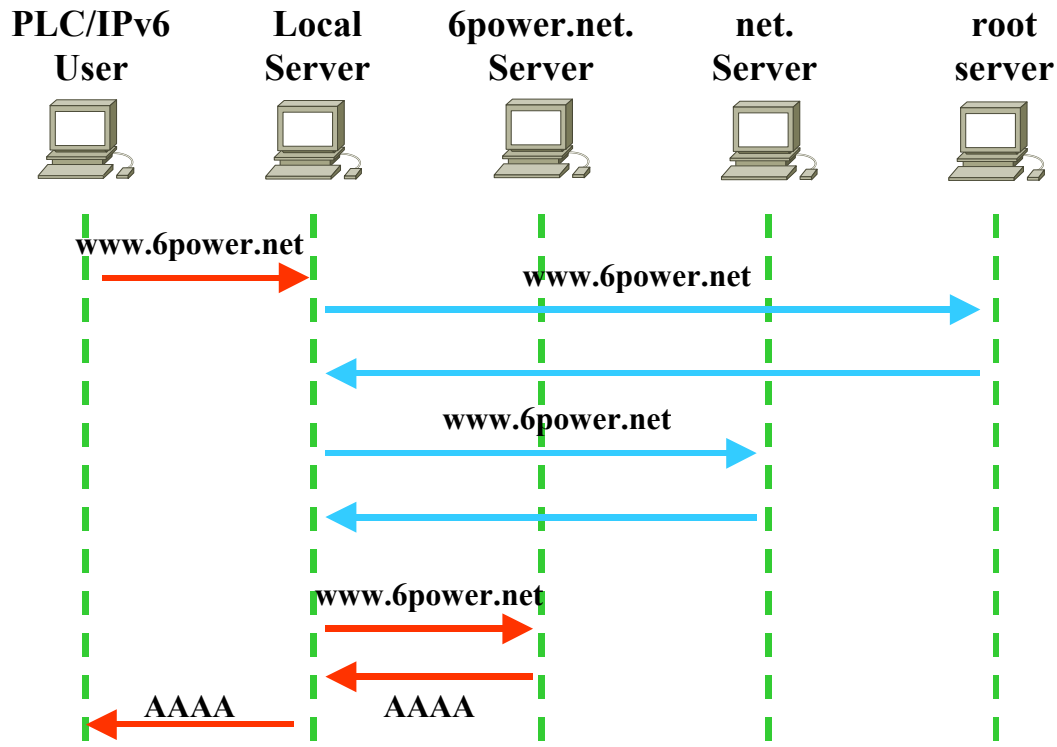

Figure 6-1: Mixed IPv4/IPv6 Resolution

Also, inside the PLC network (from the HE to the user) the DNS will be needed for easing management of devices. Even the domain hosting could be a service offered to the users.

Summarizing, the proposed design for the DNS service of the basic PLC/IPv6 network is based on the following premises:

- At least one DNS server (two or using other server as slave) per HE. More than one HE "under the service" of one DNS server is allowed, but only if the HEs are connected by the same IPv6 connect network .
- The DNS servers must be dual stack and have both IPv4 and IPv6 connectivity.
- Actually the recommended practice is to have AAAA RRs for direct lookups and PTR RRs under both IP6.INT and IP6.ARPA for reverse lookups.

According to this we would have the scheme showed in the following figure. We can see that our dual-stack DNS servers could be in the PLC network (green), on a native IPv6 network (yellow) or in the connect network which connects various HEs (orange) in Figure 6-2.

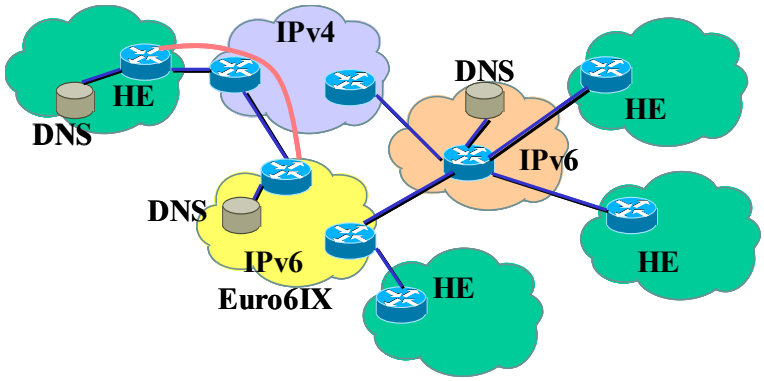

Figure 6-2: DNS Service Location

6.2 Security Plan

IPv6 is able to offer real end-to-end security thanks to the availability of globally routable addresses to every host as well as the requirement to each IPv6 compliant stack to support IPsec[16] which may provide authentication, by means of the authentication header (AH), and even confidentiality by means of the Encapsulating Security Payload header (ESP[17]). These headers can be used with IPSec either in transport mode or in tunnel mode. The main difference is that in transport mode the IPSec headers are used to authenticate and encrypt the contents of the IPv6 datagram whereas in tunnel mode, the full IPv6 datagram is included into a new IPv6 datagram containing the AH and ESP headers to authenticate and cipher the full original IPv6 datagram. The differences between these modes are shown in the next figure.

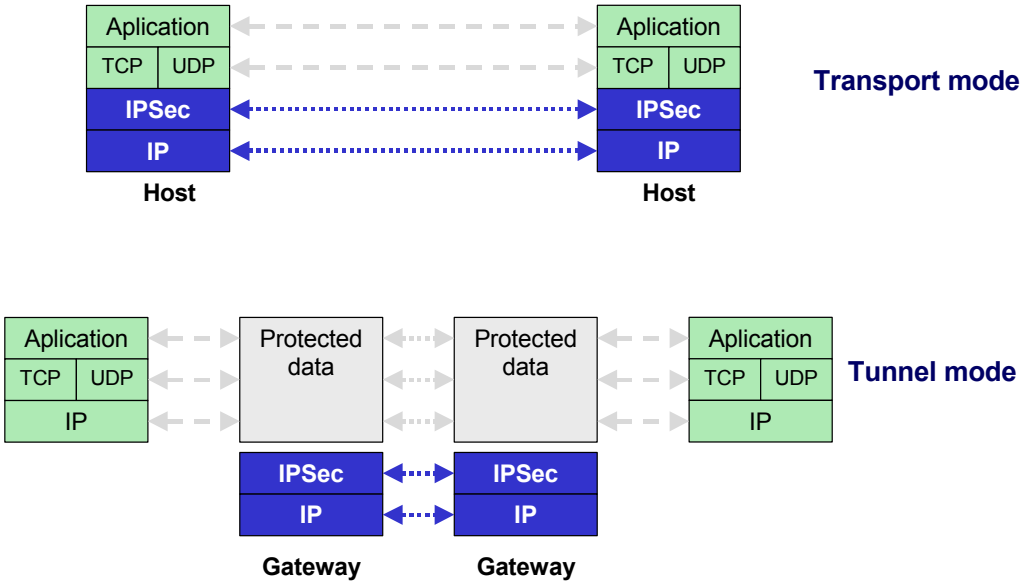

Figure 6-3: IPSec in Tunnel and Transport Mode

In addition to traditional access packet filtering (i.e. anti-spoofing and anti-smurfing filters in the access routers), the 6POWER PLC network will support the main security improvements provided by IPv6. IPSec [16] can be used to protect not only the access to the network, but also the network itself. In addition, the network infrastructure will be equipped to provide VPNs and IPSec-based security services. This will require:

- The configuration and deployment of a PKI service inside the 6POWER project.
- Analysis and study of solutions to provide these security services in transition scenarios.
- Establishment of static/dynamic VPNs between the different PLC test-beds.
- Probably the establishment of VPNs in end-host (in case of end-to-end IPSec security).

In the continuation of this PLC network design, we will address (if solutions available) mechanisms to avoid the different security attacks, which IPv6 is prone to, regarding the autoconfiguration and neighbor discovery mechanisms. These issues are currently under study in the IETF SEND WG, and are among others:

- **Malicious Last Hop Router**. An attacking node, on the same subnet as a host, is attempting to discover a legitimate last hop router, can multicast (or unicast as a response to a Router Solicitation message) legitimate-looking IPv6 Router Advertisement messages. If the entering host selects the attacker as its last hop router, the attacker can perform several attacks including the “man in the middle”. The attacker can always

ensure that it is elected as last hop router, multicasting a Router Advertisement with for the real last hop router having a lifetime of zero. In addition, when finished, the attacker can send redirect messages to these hosts towards the real last hop router, and disappear covering its tracks.

- **Good Router Goes Bad.** This is essentially the same attack, but in this case the attacker compromises the real last-hop router instead of acting as if it were the last hop router.
- **Neighbor Solicitation/Advertisement Spoofing.** An attacking node can cause packets (addressed both for hosts or routers) to be directed to a different link-layer address. This can be done sending either a Neighbor Solicitation with a new "Source Link-Layer Option" or sending a Neighbor Advertisement with a new "Target Link-Layer Option". The address could even be the subnet router anycast address, allowing the attacker to capture traffic to that address. This is caused because the Neighbor Cache of the nodes in the subnet is updated with this new link-layer address. In fact, that can be forced setting the "O" (Override) flag on. The attacker can decide how long the attack lasts, provided that it responds to the unicast Neighbor Solicitation messages which are generated as part of the Neighbor Unreachability Detection (NUD). If the attacker does not respond to these messages, the attack may last between 30 to 50 seconds (according to standard NUD timers).
- **Spoofed Redirect Message**. The attacker uses the link-local address of the first-hop router to send a Redirect message to a legitimate host. Since the host identifies the message by the link-local address as coming from its first hop router, it accepts the Redirect. As long as the attacker keeps on replying to NUD-probes, the redirect will remain being effective.
- **Bogus On-Link Prefix.** An attacking node can send a Router Advertisement message indicating that some prefix (of arbitrary length) is "on-link". If a sending host thinks the prefix is on-link, it will never send a packet addressed to an IPv6 address within that prefix to its first hop router. Instead, it will try to perform address resolution within its subnet. As no one will answer those requests, this produces a Denial of Service (DoS) attack to that host. The attacker can use an arbitrary lifetime on the bogus prefix advertisement. In fact, if the lifetime is infinity, the attacked host will have its service denied until it losses the state in its prefix list (e.g. rebooting or receiving an announcement of the same prefix with lifetime zero).
- **Bogus Address Configuration Prefix.** An attacking node can send Router Advertisement messages specifying an invalid prefix to be used by a host for address autoconfiguration. A host executing the autoconfiguration algorithm will use that prefix to build an address even if this address is not valid for the subnet. As a result, all the IPv6 packets using that IPv6 autoconfigured address will never get an answer. In addition, this DoS attack has the potential to propagate if the attacked host performs a dynamic DNS updating its AAAA or A6 Resource Record (RR), causing other nodes receiving this DNS answer to fail to communicate with the host. To avoid that, well-written applications should try each of the different IPv6 addresses received in an RRSet after a DNS query.
- **Duplicate Address Detection DoS Attack.** In an autoconfigured scenario, an attacking host could launch a DoS attack by responding to every Duplicate Address Detection (DAD) attempt by an entering host. If the attacker claims the address, then the host will never be able to obtain an address.
- **Neighbor Discovery DoS attack.** An attacker node (from outside of the attacked subnet) starts fabricating addresses within the attacked subnet prefix and continuously sending packets to them.. The last hop router is obligated to resolve these addresses by sending Neighbor Solicitation messages. A legitimate host trying to enter the subnet may not be

able to get a Neighbor Discovery service from the last hop router because it will be already busy trying to resolve all these other solicitations.

- **Parameter spoofing.** An attacking node could send out a legitimate-looking Router Advertisement that resembles a legitimate Router Advertisement from any of the routers except that the included options (parameters) are filled so that legitimate traffic is disrupted. For example, the Current Hop Limit can be set to zero or another low value so that the packets from the nodes on the link are dropped before reaching its destination. Another example would be setting on the 'M' and/or 'O' flags to make the nodes go to a DHCP Server to get additional autoconfiguration information. The attacker can set up a bogus DHCP server and control the parameters which hosts in the subnet autoconfigure just sending its own bogus replies.

6.3 Autoconfiguration

IPv6 knows both stateless and stateful autoconfiguration.

- **Stateful autoconfiguration** is what was known as DHCP in IPv4. Work towards a specification of DHCPv6 is being done within IETF [5], but at the moment it still be in draft state.
- **Stateless autoconfiguration** [3] is new in IPv6 and allows hosts to obtain its address without any configuration. Neither is necessary the configuration of a dedicated server (like in DHCP). The key element is the router, which will be present somewhere in our network.

Both mechanisms seen above just allow **host autoconfiguration**. Actually there is no standardized **router autoconfiguration** mechanism. We will try to argument the need of the last issue.

Based on this we can consider autoconfiguration of the user's hosts and of the PLC-network provider's routers.

6.3.1 User's Hosts Autoconfiguration

The autoconfiguration is achieved by means of **Router Advertisements** (**RA**) sent by a router. So we have to guarantee that in each user's LAN segment there are RAs sent.

With the information received within the RA the host obtains one or more network prefixes with which it can construct its IPv6 address. Also the host receives the address of the router, which will act as its gateway.

As a first analysis of the basic cases considered in this document we could differentiate the following configurations:

- The **CPE is a router:** In this scenario the CPE have to make the RA's. How the corresponding prefix to be announced reach the CPE is more related to the network provider network configuration. In a simplistic case we can consider the CPE to be manually configured.
- The **CPE is a bridge**: In this scenario a router behind the CPE should send the RAs. This implies that this router have to be able to receive the delegated prefixes in whichever the way it is done.

6.3.2 Network Routers Autoconfiguration

As said above, there are no standardized solutions to this issue.

A zerouter BOF has been organized. Its work is focused on IP router autoconfiguration for unadministered networks (i.e. the SOHO market) and would provide solutions to auto-configure IP addressing (IP-AC now on), unicast and multicast IP forwarding and to detect and recover from inevitable addressing collisions (see [6] to [10]).

New prefix delegation (PD now on) protocols, auto-configuration of arbitrary router parameters, transit networks or services would be specifically out-of-scope for the group.

What we will try here is to identify the required mechanisms for our network, in order to ease the deployment and management of the IPv6 PLC network provider's part of the network.

As we are considering the simple network topology, only HE and CPE would be routers. In the mean time a PD mechanism would be needed. As said above, the mechanism for delegating the prefix to the routers is to be defined. Actually the DHCPv6 [5] prefix delegation mechanism is a good candidate, as there are available implementations that could be used.

Also the interfaces of the network devices should have an IPv6 address for managing purposes. These addresses must be accessible from the Network Operation Center (NOC), wherever it was.

6.3.3 PLC Devices Autoconfiguration

Currently, the layer-2 link between PLC devices is not autoconfigured. Actually, in order to establish a link between a PLC master and a PLC slave, the MAC address of the slave has to be registered in the master, using any of the available methods (manually or remotely using SNMP).

This has been identified as a serious problem for the deployment of large PLC network, and will be solved during this project. PLC autoconfiguration capabilities (which will complement IPv6 autoconfiguration features) will be developed and tested in the trials performed in the project.

7. FUTURE ENHANCEMENTS OF THE BASIC NETWORK DESIGN

As we have commented before, this deliverable only describes the basic network design and D3.2 will describe the design of advanced network services like QoS and Multicast. This section describes the specific aspects, which we will look at, and our tentative ideas, which will be fully studied and investigated in the next phase of A3.1.

Regarding QoS, what we have identified is that currently layer 3 approaches cannot be generalized to cover QoS at the PLC layer. We will have to analyze and propose solutions to the provision of QoS in PLC networks taking into consideration the network as a whole instead of a set of standalone PLC links. Hence, the key aspect in our future network design will be the provision of a simple mapping of Applications requirements and application signaling to network layer QoS provision as well as a mapping between these network layer QoS provision and any specific QoS provision at the PLC layer. This general approach to be investigated and the relation in terms of QoS among the different parts of the PLC network are illustrated in Figure 7-1.

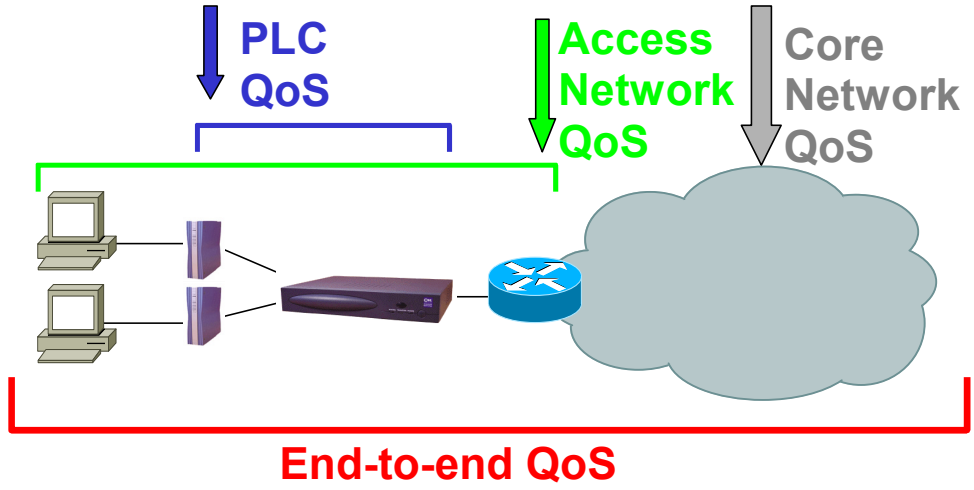

Figure 7-1: Different QoS Components to Evaluate

Regarding multicast, the approach is somehow similar. While the IP Multicast model [18] is currently widely accepted and deployable in a PLC bridged scenario, it is not clear which is the best network design to get the better performance due to the internal PLC operation. Most of the IP Multicast operation is based on the IGMP [19] (MLD [20]in IPv6)protocol, combined with some routing protocols like PIM-SM [21].

Due to the specific PLC broadcast support, we will have to analyze different alternatives to increase layer2 multicast performance while preserving IPv6 multicast compatibility. We will analyse among others IGMP/MLD snooping [22] and IGMP/MLD proxying [23] approaches.

8. DESCRIPTION OF THE TEST-BED TO BE SETUP

The most important test-bed to be setup will be located in the existing power line access trial currently maintained by Endesa in Zaragoza, Spain. This trial is, basically, a hybrid network containing Gigabit Ethernet rings, Medium Voltage power line links and Low Voltage power line links. The network is based on a bridged architecture, with VLANs being used to reduce broadcast domains. The network currently provides Internet and VoIP service to more than 2000 customers, and is totally based on IPv4.

One of the main rules that we have followed when designing the test-bed for the 6POWER projects is that adding IPv6 support should be as little disruptive as possible to the existing users of the network. At the same time, the new IPv6 service should not add significant complexity for the network operator. This was a very important concern: if the staff at Endesa that is running the network thinks that managing an IPv6 network is more complex than managing the existing IPv4 network, they would delay migrating the network to the new protocol, and would try different options (i.e.: NAT) instead of switching to IPv6 in case they run out of IPv4 addresses.

A simplified diagram of the initial trial network is included in Figure 8-1. It shows a layer-2 network, with a single IPv4 router that connects all customers (grouped by VLANs) to the IPv4 Internet.

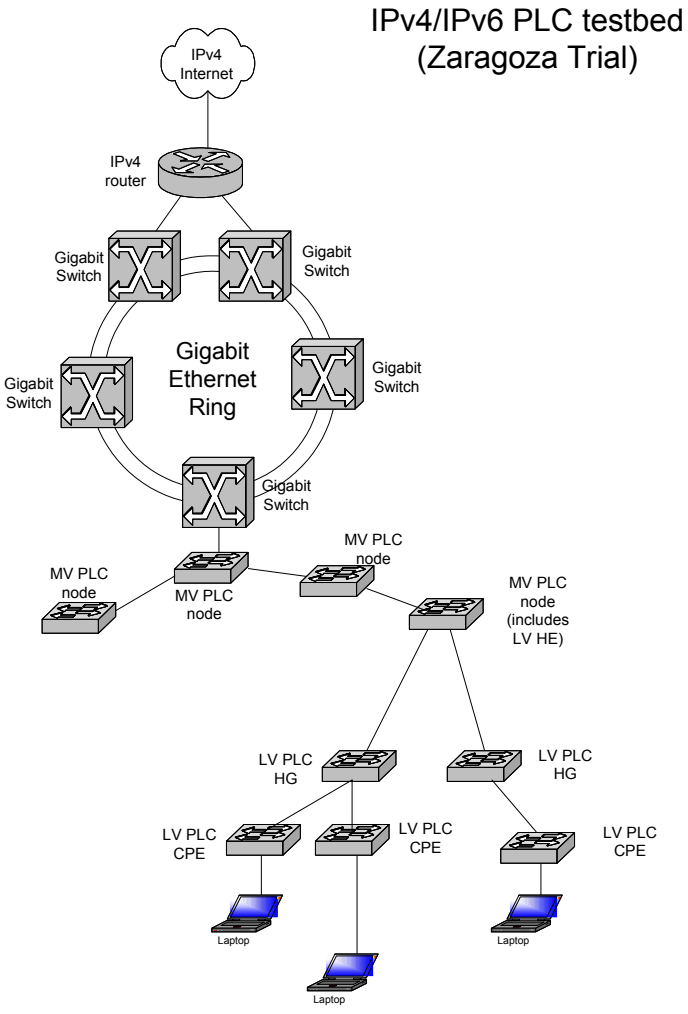

Figure 8-1: Original Trial Network Architecture

Figure 8-2 shows the basic modifications that are needed for adding IPv6 support to a group of customers that hang from the same transformer. Basically, the following devices are added:

- A Router HE is installed in the transformer. This router provides IPv6 services downstream and provides IPv6 Internet connectivity through an IPv6 tunnel.
- A variety of routing devices are installed in the house of the customers. We will try several options: a) an integrated CPE router, b) a split architecture with a layer-2 CPE connected to a router, and c) a layer-2 CPE that connects the end-user computer directly.

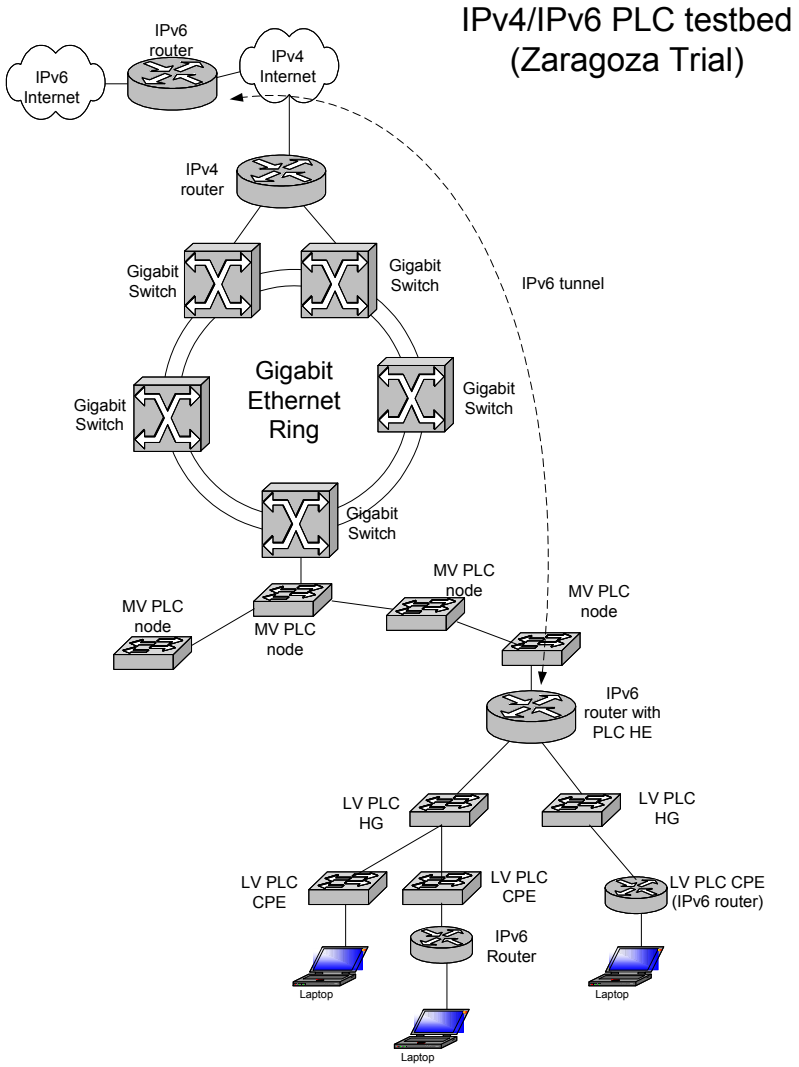

Figure 8-2: Proposed Architecture to Include IPv6 Support in the Original Test-bed

According to the internal project schedule, an integrated HE router will not be ready for the intended trial date, so a split solution was designed, in which both an IPv6 router and a layer-2 PLC HE are installed in the transformer. The router and the PLC HE would be connected through Fast Ethernet. This architecture is shown in Figure 8-3.

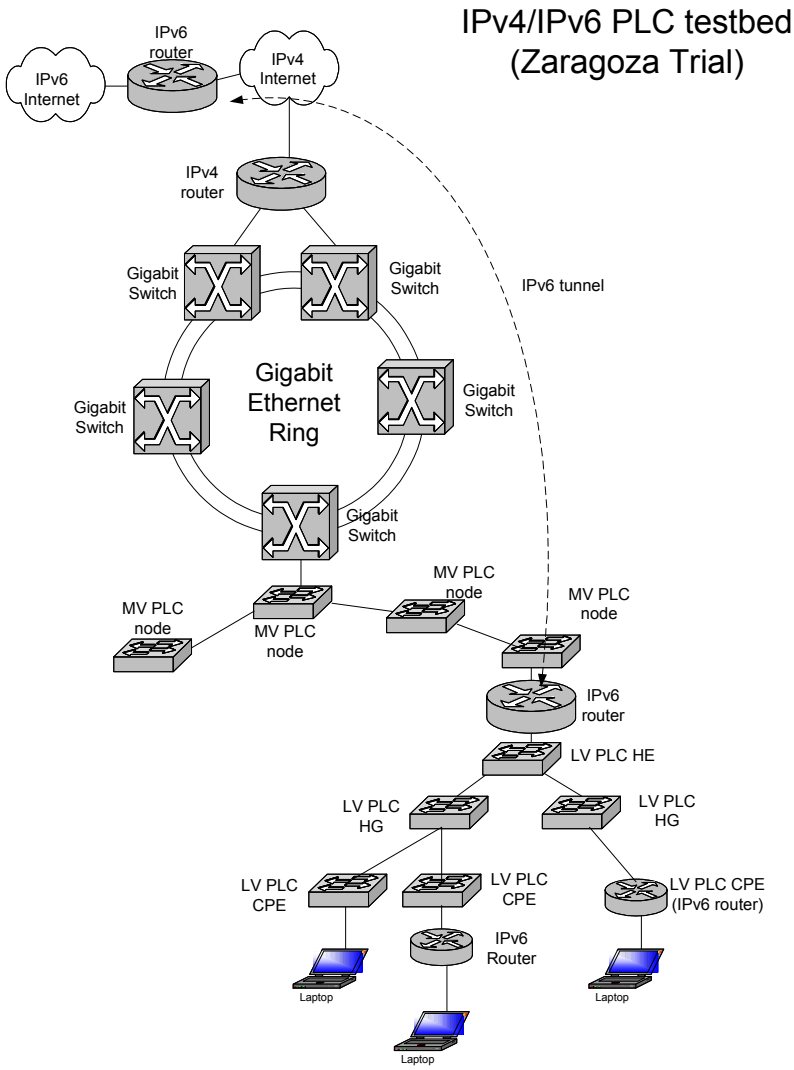

Figure 8-3: Architecture with Split IPv6 Router and Power Line Head End

Some partners proposed a further optimization, to the one showed in Figure 8-3. Why restricting the possibility of providing IPv6 service only to one transformer? If we move the IPv6 router up in the network, it can provide IPv6 service to even more customers, with no extra cost to the project. Even more, if initial tests were successful, Endesa could provide basic IPv6 service to the whole network (>2000 customers) with no extra equipment. This was not a project objective originally, but could happen if the trial results shows that IPv4/IPv6 service can be provided easily to power line customers with no extra complexity for the network provider. This last architecture is shown in Figure 8-4.

A dedicated VLAN is established between the test-bed transformer and the IPv6 router. While the rest of customers connect to the Internet through the original IPv4 router, customers in the transformer test-bed use the IPv6 router as a gateway to the Internet. By changing the VLAN configuration appropriately, more customers can be easily migrated to the IPv4/IPv6 trial network.

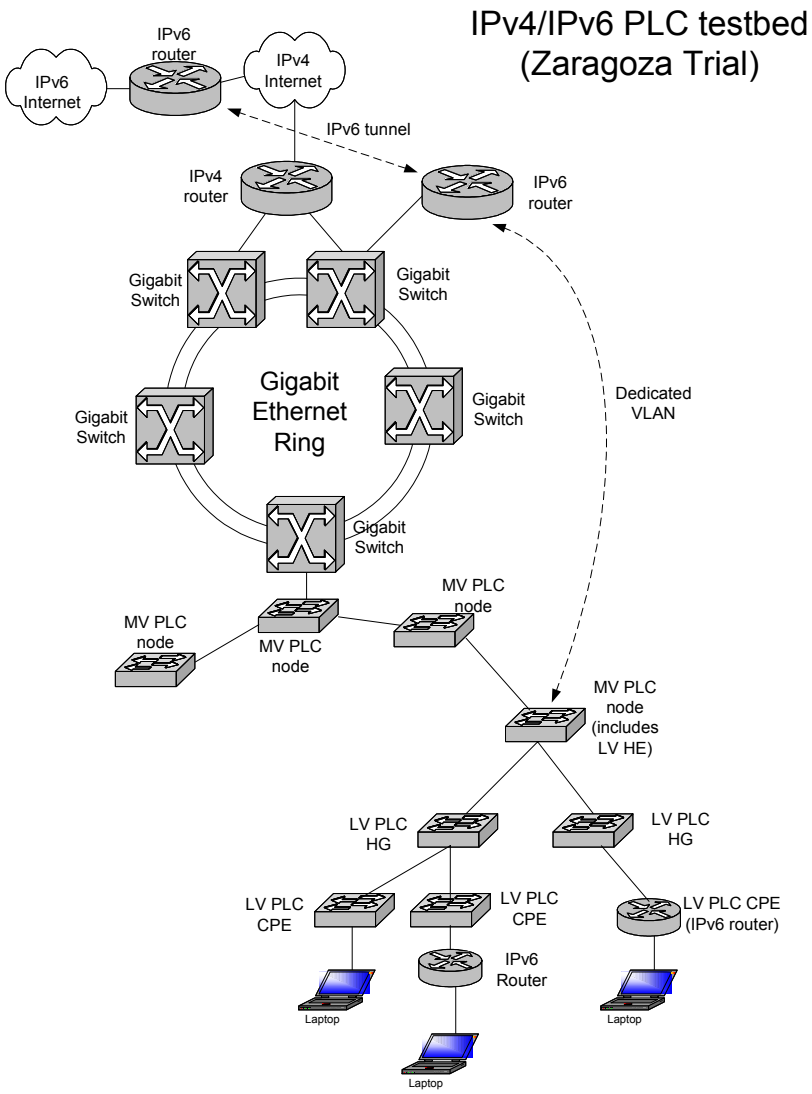

Figure 8-4: Final Architecture with IPv6 Router in the Core Network

9. SUMMARY AND CONCLUSIONS

We have presented our network design proposal for the setup of the basic PLC networking services in the framework of the 6POWER project. We have analyzed and proposed a design taking into consideration many aspects like topology, identification of candidate scenarios, routing, security, naming service, etc.

Much of the work has been devoted to the decision of using PLC bridges or PLC routers in which parts of the networks. This issue has come up as one of the most important factors affecting the overall PLC network throughput. From the complete set of alternatives there are some of them, which are directly workable, whereas others require specific functionalities, which are not already available in IPv6 equipments (e.g. multilink support). For each user scenario we have been able to find an immediate solution with specific combinations of PLC bridges and routes being a good trade-off between efficiency and ready deployment. The solutions are presented in the topology section.

In addition, we have designed the PLC network using Euro6IX and 6NET as the interconnection networks among different partners. The connection details were agreed with these projects to avoid any problem with their internal policies. An inter-partner IPv6 network has been designed and specified.

Furthermore, we have analyzed important aspects like autoconfiguration, DNS setup, security and other important basic network services, which will be deployed in the network. The proposed network design will be used as the basis for the basic PLC network deployment within the A3.2 activity.

As future work we plan to address the design of advanced network services like QoS and multicast in the continuation of A3.1 until month 15. In addition, the input from our initial A3.2 network deployment during these months will be very valuable, and it will be widely used to refine our basic design if necessary.

10. REFERENCES

[1] "Report on IPv6-over-PLC relevant issues", Deliverable 2.1, 6POWER Project (IST-2001-37613), September 2002.

[2] "IPv6-over-PLC interface specification", Deliverable 2.2, 6POWER Project (IST-2001-37613), January 2002.

[3] "IPv6 Stateless Address Autoconfiguration", S. Thomson, T. Narten, RFC-2462. December 1998.

[4] draft-ietf-ipv6-prefix-delegation-requirement-00.txt - Shin Miyakawa - November 2002.

[5] "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", R. Droms (ed.), J. Bound, Bernie Volz, Ted Lemon, C. Perkins and M. Carney. Internet-Draft, Work in progress, November 2002. (http://www.ietf.org/internet-drafts/draft-ietf-dhc-dhcpv6-28.txt)

[6] draft-haberman-ipngwg-auto-prefix-02.txt - B. Haberman, J. Martin - February 2002.

[7] draft-chelius-router-autoconf-00.txt - G. Chelius, E. Fleury, L. Toutain - Internet-Draft, Work in progress, June 2002.

[8] draft-linton-arcp-00.txt - J. Linton – Internet-Draft, Work in progress, October 2002.

[9] draft-white-zeroconf-subnet-alloc-01.txt - A. White, A. Williams - Internet-Draft, Work in progress,October 2002.

[10] draft-white-zeroconf-uiap-01.txt - A. White, A. Williams - Internet-Draft, Work in progress,October 2002.

[11] "Domain Names - Concepts and Facilities", P. Mockapetris, November 1987.

[12] "DNS Extensions to support IP version 6", Thomson, S. and C. Huitema, RFC 1886, December 1995.

[13] "Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)", R. Bush, A. Durand, B. Fink, O. Gudmundsson, T. Hain, RFC 3363, August 2002.

[14] "Tradeoffs in Domain Name System (DNS) Support for Internet Protocol version 6 (IPv6)", R. Austein, August 2002.

[15] draft-ietf-ipv6-multilink-subnets-00.txt – D. Thaler, C. Huitema - Internet-Draft, Work in progress , June 2002.E. Kaufman, A. Newman, "Implementing IPsec", John Wiley & Sons, 1.999

[17] S. Kent and R. Atkinson. IP Encapsulating Security Payload (ESP). RFC 2401, November 1998

[18] S. Deering, “Multicast Routing in Datagram Internetworks and Extended LAN”. Ph., D. dissertation. Stanford University, December 1991.

[19] Fenner, W.: “Internet Group Management Protocol, Version 2”. RFC 2236, November 1997.

[20] Deering, S., Fenner, B. and Haberman, B."Multicast Listener Discovery (MLD) for IPv6",RFC2710, October 1999.

[21] Estrin, D., Farinacci, D., Helmy, A., Thaler, D., Deering, S., Handley, M., Jacobson, V., Liu, C., Sharma, P. and Wei, L.: “Protocol Independent Multicast Sparse Mode (PIM-SM): Protocol Specification”. RFC 2362, June 1998.

[22] Frank Solensky, Morten Christensen, Karen Kimball, Considerations for IGMP and MLD Snooping Switches, draft-ietf-magma-snoop-06.txt. Internet-Draft, Work in progress.

[23] Bill Fenner, IGMP/MLD-based Multicast Forwarding ('IGMP/MLD Proxying'), draft-ietf-magma-igmp-proxy-02.txt. Internet-draft. Work in progress.