Title: **Deliverable D2.1.4** **Report of 4th Deployment Case Study**	**Document Version:** 1.3

Project Number:	**Project Acronym:**	**Project Title:**
223794	6DEPLOY	IPv6 Deployment Support

Contractual Delivery Date:	**Actual Delivery Date:**	**Deliverable Type* - Security**:**
28/02/2010	21/10/2010	R – PU

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

Responsible and Editor/Author:	**Organization:**	**Contributing WP:**
Alvaro Vives	Consulintel	WP 2

Authors (organizations):

Jordi Palet (Consulintel).

Abstract:
This document is a case study intended for ISPs in developing regions considering the deployment of IPv6.

It is based on an actual case, but no details are disclosed that would compromise issues of security or confidentiality for the ISP.

Keywords:

IPv6, deployment, ISP, case study

Disclaimer

Executive Summary

This report describes the first steps towards an IPv6 deployment within an ISP in a developing region. Due to the fact that the ISP has not yet started operating, the implementation and the information are under a NDA. Therefore, this document generalizes the information and refers to a generic ISP. However, the information contained here is considered valuable for other ISPs in a similar situation.

This report is based on the conclusions obtained from an initial evaluation of the ISP's network and the subsequent IPv6 implementation plan.

The recommended solution for the IPv6 deployment was to deploy dual-stack IPv6 services, i.e. so that IPv6 capabilities will become available on the existing infrastructure that supports IPv4.

The different parts of the network and the technologies used are described, showing the points that should be taken into account when considering a similar deployment scenario.

Table of Contents

Figure Index

Introduction

ISPs have been urged to implement IPv6 on their networks in advance to anticipate user demand, avoid future problems due to IPv4 address depletion problem, and be ready for the future applications that will certainly require the use of IPv6.

All the RIRs (Regional Internet Registries) have made announcements supporting IPv6 deployment and urged the Internet stakeholders to start implementing IPv6. For example, AfriNIC's "Advice to Operators for Immediate Action on IPv6", dated 25th July, 2007 below:

"Internet Protocol version 4 (IPv4), the protocol used today to run the Internet for more than 20 years now has started showing its limits with mainly the running out of number resources associated to it, known as Internet Protocol addresses (IP addresses). This is essentially due to the steady growth of Internet usage during the past few years. Only 18% of the total IPv4 space is now available and at the rate of actual consumption despite the very strict evaluation measures implemented by all regional Internet registries, this would not last longer than till 2010-2011.

Soon (within three to four years), AfriNIC will not be able to continue to allocate IPv4 addresses to Network Operators with a guarantee for aggregation. It is our responsibility, to avoid such a situation where the development of our region's network infrastructure is drawn back by the unavailability of these version 4 addresses, to urge Network Operators in the Africa region to take clear actions toward implementing Internet Protocol version 6 (IPv6) in their Network Infrastructure in cohabitation with IPv4. While the time is not for panic, it is rather important that action be taken NOW to avoid a situation of urgency later.

IPv6, the protocol designed and defined as a standard by the Internet Engineering Task Force (IETF) since the late 90s, allows the availability of Billions of Billions of IP addresses with an improvement of several embedded features of the protocol as the result of lessons learned and experiences gained from IPv4 deployment and usage. It is a fact that the long term solution and strategic move for emerging economies like in our region is to not struggle with IPv4 only network deployment any more, but rather deploy IPv6-Ready infrastructure as from now on.

Since 2005, AfriNIC has launched a campaign to introduce IPv6 to Operators and Policy Makers around the African continent. This campaign has taken us for training sessions in more than 12 countries with more than 500 people trained and informed about IPv6.

The AfriNIC Board has approved a plan to intensify this campaign by reaching out to every country and operator across the continent by the end of 2010. This includes giving training on various transition mechanisms for the smooth deployment of IPv6. This decision also implies the use of different means of communication to reach the majority of stakeholders by the targeted date.

Since advanced planning is a key factor for a successful and affordable transition, we are hereby urging operators in the AfriNIC region to take immediate action."

At the time of writing this document, the NRO (Number Resource Organization), has announced that the available stock of IPv4 addresses at the IANA (Internet Assigned Numbers Authority) pool, is now below 5%, versus the 10% that was available at the beginning of 2010. This means that in less than one year, IANA will not be able to provide more IPv4 addresses to the RIRs.

The ISP which has been the basis of this document, decided to follow AfriNIC's recommendation and started with the necessary first steps towards IPv6 implementation, i.e. training of its staff, analysing its network (including devices, services, etc.), and creating an implementation plan (including addressing plan, elements to be updated or changed, etc.).

This document is based on this implementation plan.

1. OVERVIEW

The first step was to evaluate the ISP's network(s) and produce recommendations regarding the deployment of IPv6 on its data network. As a result of this evaluation, 6DEPLOY partners helped to make an inventory and analyse the network, identify its architecture and its elements, the technologies used, and the current IPv6 support, if any, of those elements.

Using the results of the evaluation, the next step was to generate a roadmap, and identify the main tasks to be carried out.

The following scheme shows these main steps:

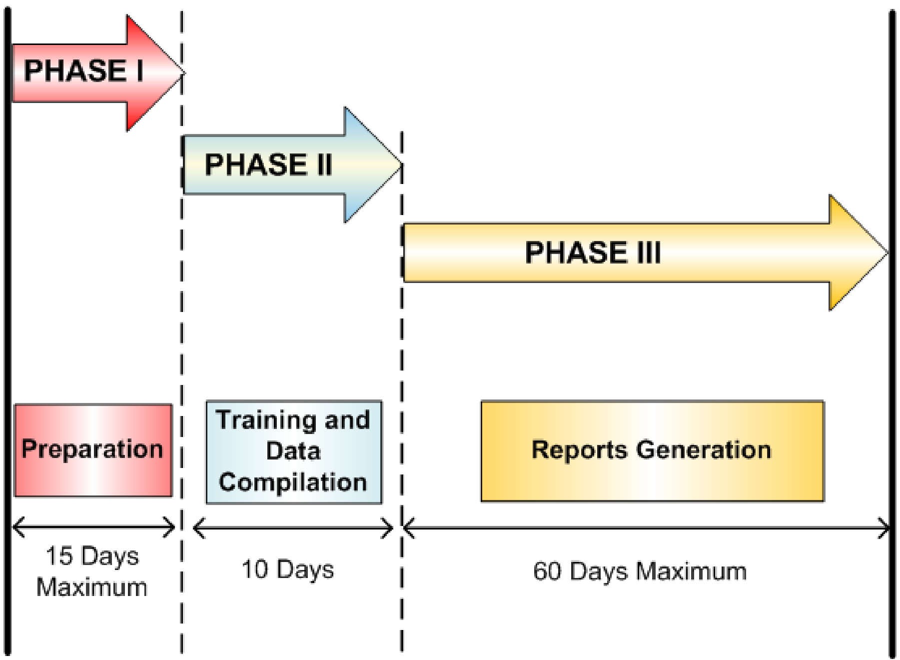

Figure 1-1: First steps towards IPv6 deployment

2. DATA COMPILATION

In-house data compilation was necessary to generate the inventory of devices, firmware/software versions used, services offered, the layout of the existing network, understand the foreseen network evolution, future changes, and learn about security measures and management practices.

A top-down approach was used: first a global scheme of the network was obtained, and then details were obtained given for each part of the network. An overview of the compiled data is as follows:

2.1 Network layout

The following figure shows the different technologies used in the ISP's network. This ISP mainly used wireless technologies to offer services to its customers and even for its internal links.

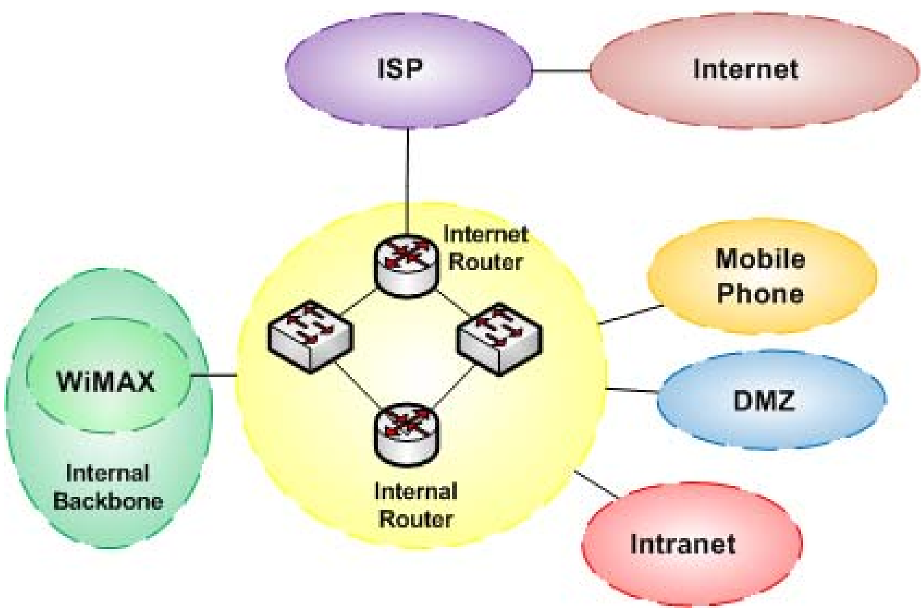

Figure 2-1: ISP's Network Layout

The ISP's network is composed of a core network, to which different access technologies are connected. The core network is connected to the Internet through an upstream provider.

The different access technologies used are WiMAX, cellular phone infrastructure and Ethernet. The different networks that use these technologies are WiMAX for clients, an internal backbone (that uses the WiMAX infrastructure as well) used as a distribution network, a DMZ, ISP Intranet, and the cellular phone data network.

Each of these different technologies had its own equipment to be inventoried, firmware/software versions to be checked, and technology issues to be considered when IPv6 must be deployed.

Important information collected in this phase was the number of users/devices connected to each service, and how they are expected to increase (or decrease). This information was used for defining the addressing plan.

The following are some considerations of each of the main parts of the network analyzed.

2.2 Core

The main elements analyzed, and summary results were:

- **Routing protocols used**: No dynamic routing protocols were used, only static routes.
- **Internet connectivity**: The ISP's network is connected to a single upstream provider that did not provide IPv6 connectivity. A list of alternative IPv6-capable service providers was created.
- **Network devices**: The routers, firewalls, and switches were quite new and updated. This resulted in a good support for the needed IPv6 features.
- **"Special" devices**: A traffic shaper is used that does not support IPv6. There were no load balancers, content inspection, lawful interception, proxy, or other devices to be considered.
- **Addressing**: Both private and public addresses were provided to end-users. The number of delegated IPv4 addresses and the tools/mechanisms for managing them were also analyzed.

2.3 Backbone

The ISP also had an internal backbone network used as a distribution network; mainly for internal use. This backbone network uses microwave links. The following figure shows a schematic representation:

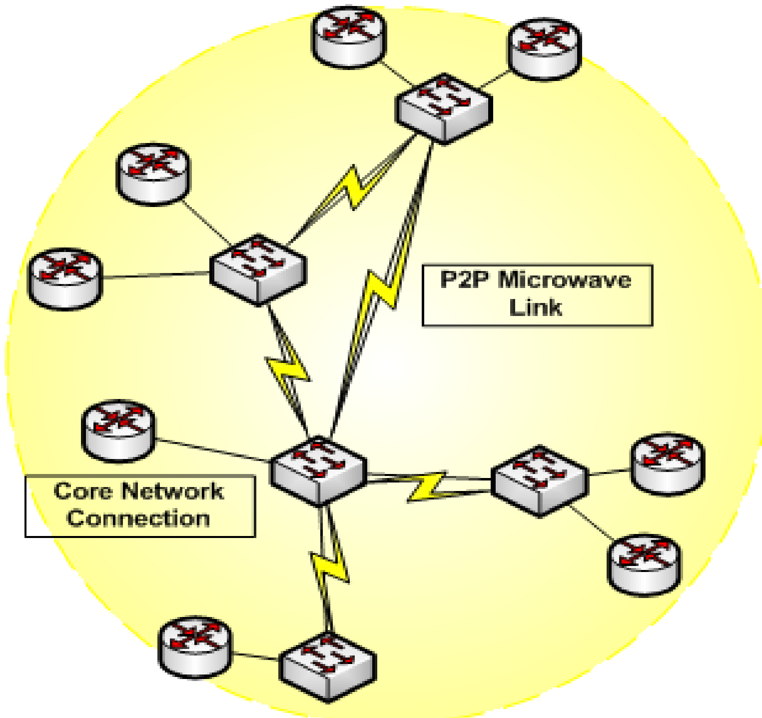

Figure 2-2: Backbone Network

A majority of the routers in this network already supported IPv6, and the others just needed a software update. It was required that the routers support dynamic routing over IPv6, in preparation for its possible use in the future.

2.4 Intranet

This network is used by the ISP's employees, and is mainly based on Microsoft applications both for the clients and for servers. They also used VoIP internally.

The Windows OS's used supported IPv6 with no problems, and some of the services too, but there were two main missing IPv6-capable elements: a proxy (Microsoft-based) and the VoIP infrastructure.

2.5 WiMAX

The WiMAX network also uses the microwave links used by the backbone network to reach the end users. There are two types of users; those using just a router to connect to the WiMAX service and those using both a router and a PC to connect to the WiMAX service. The following figure shows a schematic representation:

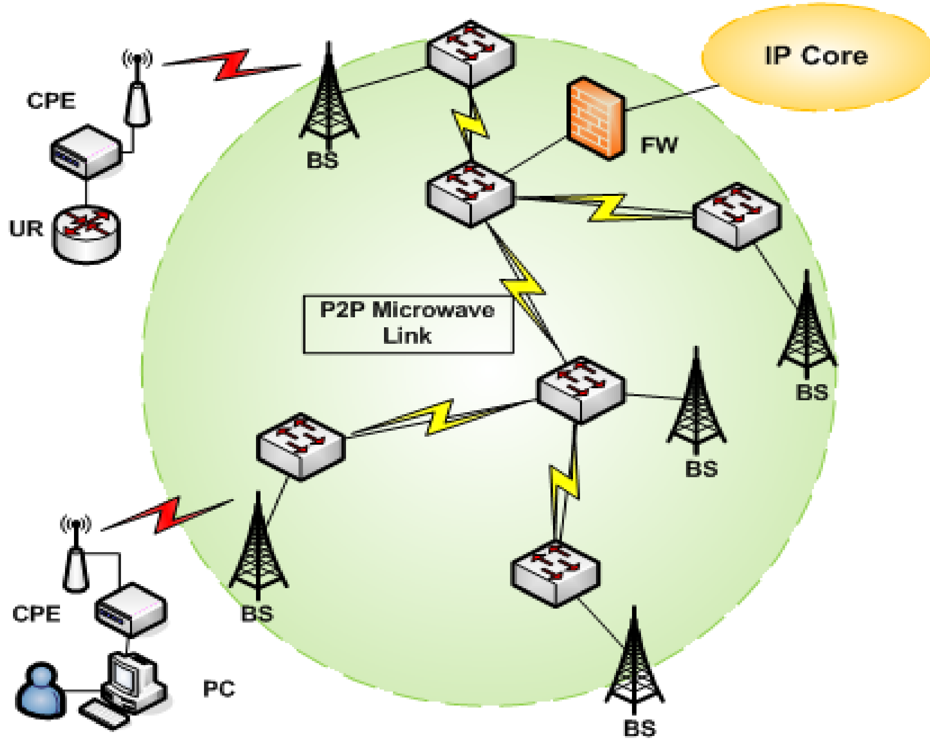

Figure 2-3: WiMAX Network

As seen in the figure above, the Base Stations (BS) are connected to the backbone, which is based on microwave links. Users connect to the BSs using a WiMAX CPE that provides Layer 2 connectivity to a PC or a User's Router (UR).

The vendor of the WiMAX equipment has not confirmed if they support IPv6, but from the standard it is supposed to support IPv6 and treat it as Ethernet traffic. It has been recommended to make some tests to be sure that the WiMAX radio links provide IPv6 connectivity.

The vendor management software for all the WiMAX devices is proprietary and does not support IPv6. There is also no IPv6 support in the firewall used to connect the WiMAX Access Network to the Core, for which the replacement of this device would be the best solution.

Both public (static) IPv4 addresses and private (using DHCP) IPv4 addresses are provided to end-users.

2.6 Cellular phone network

The cellular phone network is heterogeneous in the sense of having different vendor equipment and offering services under different evolutions of the technology. The network has a GSM (Global System for Mobile communications) part that uses 2G radio access (GERAN – GSM Radio Access Network) based on TDMA (Time Division Multiple Access). In addition, there is a part based on the UMTS (Universal Mobile Telephony System) standard that uses 3G radio access (UTRAN – UMTS Terrestrial Radio Access Network) based on WCDMA (Wide band Code Division Multiple Access). GPRS (General Packet Radio Service) is the packet service used in both the GSM and UMTS networks. In this document we use the terms "2.5G" to refer to the GSM network with packet service support, "3G" to make reference to the UMTS cellular phone network with GPRS data support [TS23.060] and "IMS" (IP Multimedia Subsystem) [TS23.228] as defined in Release 5 (Rel-5) of the 3GPP (Third Generation Partnership Project) [3GPP] standard.

The following figure shows a generic scheme of the cellular phone infrastructure. It is not the objective of this document to explain this infrastructure, therefore, the description provided is not extensive.

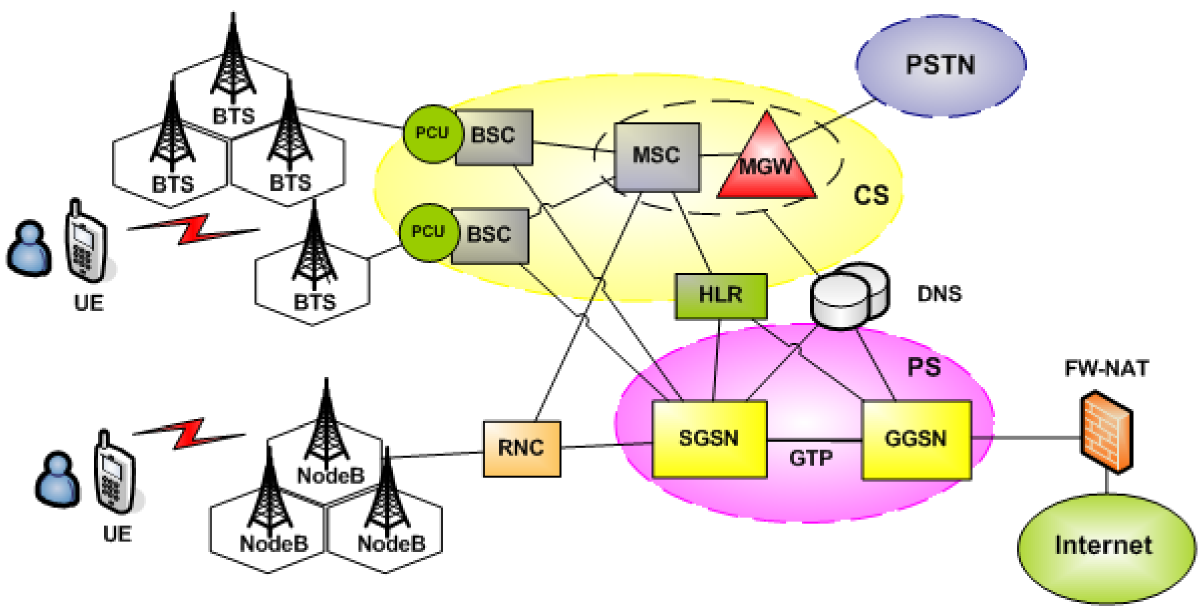

Figure 2-4: Cellular Phone Network

The cellular phone network is composed of both 2.5G and 3G data networks, sharing the common elements like the GGSN (Gateway GPRS Support Node), SGSN (Serving GPRS Support Node), MSC (Mobile Switching Center), MGW (Media Gateway), HLR (Home Location Register) and DNS (Domain Name Server) for the GPRS data service.

Each UE (User Equipment) uses a PDP (Packet Data Protocol) context that connects the UE with the GGSN, which provides data connectivity to the UE. Both IPv4 and IPv6 are supported, but only one of the protocols could be used in one PDP context. It is defined by 3GPP/IETF that each PDP context receives a /64 IPv6 prefix, to ease the autoconfiguration process on the UE. This was taken into account for the addressing plan.

The main problem with this ISP was that almost all the devices of the cellular phone network were from one vendor, who had very little information about IPv6 support and configuration. In general they were supposed to support IPv6 with a software update, but due to missing information, it was not known for certain if this was the case and therefore only general steps could be planned in advance.

2.7 Services

Some basic internal services were analyzed too:

- **E-mail:** Different e-mail servers and proxies are used, but the support of IPv6 is missing in all of them. The best solution would be to update or replace all the software used, but at the moment this would be difficult.
- **DNS**: The servers (linux-based) and software used (BIND) for the DNS service support IPv6 with no problems (DNS transport, forward and reverse resolution).
- **NTP**: The device used for NTP service does not support IPv6. The solution would be to update/replace it.
- **Web**: The servers (linux-based) and software used (Apache 2.x) for web service support IPv6 with no problems.
- **Management**: The NOC uses a lot of different software to monitor the network. Most of these applications are from the hardware vendors and consequently proprietary, with no IPv6 support.

3. IPv6 Implementation Plan

Based on the description of the network shown and the IPv6 support, or lack of it, this section provides a summary of the proposed actions for each relevant item to be taken into account when deploying IPv6.

3.1 Addressing plan

For the addressing plan, the number of users attached to each type of access technology and network were taken into account, including the predicted evolution. This number was then multiplied by the decided IPv6 prefix assigned to each type of user. In this way the required IPv6 prefix to be delegated by the RIR was assessed.

The prefix length for each type of user or element in the network was determined to be as follows:

- Point-to-point links and internal LANs: /64
- WiMAX users: /48
- Cellular phone networks: /64 for each PDP context
- Intranet LANs: /64

After this evaluation, the conclusion was that a /32 prefix would be sufficient for the ISP, considering the current and forecasted number of customers.

3.2 Core

The recommended steps were:

- Enable IPv6 in both the Internal and External facing routers. Both type of routers support IPv6, but the feature has to be enabled.
- Configure IPv6 in the LANs, by configuring IPv6 address(es) in the LAN interfaces.
- Configure the routing - in this case static routing - as used for IPv4.
- Configure eBGP in order to announce the assigned IPv6 prefix.

- Bypass the packet shaper for IPv6 traffic, because it does not support IPv6. In a later stage, the traffic shaper should be replaced, by one with dual-stack support.

3.3 Backbone

Layer 2 switches and Layer 3 routers compose the backbone network. The switches do not need any re-configuration to allow IPv6 traffic. The routers, that have IPv6 support (the majority), only have to be re-configured to enable IPv6, pass IPv6 addresses on the interfaces and have the static routes configured ,(in the same way as for IPv4).

For the routers that do not have IPv6 support, the only additional step is to update the software to add the required IPv6 support.

3.4 Intranet

The Intranet network is composed of different elements, such as PCs, servers, proxies, routers, VoIP devices, etc. The following were the main issues to be considered:

- VoIP: The used equipment does not support IPv6. Since renewing is not considered possible, this service should be implemented over IPv6 in a future phase.
- Clients: All OSs are from Microsoft starting with XP SP2 and newer, i.e., basic IPv6 support exists. In case of the need of using DHCPv6, then Windows Vista and newer are necessary. The needed step is to enable IPv6 on the clients with XP OS. For Windows Vista and newer, IPv6 support is enabled by default.
- Enable IPv6 in servers and services that support it. Assign static IPv6 addresses to the servers.
- Enable stateless autoconfiguration for clients using Router Advertisements.
- One missing element is the support of IPv6 in the proxy used for some parts of the users' Intranets. The ISP needs to change the proxy to provide IPv6 support.

3.5 WiMAX

The WiMAX network has to be checked to ensure that the equipment follows the standards and is able to deliver IPv6 traffic, considered as Ethernet traffic. The vendors say their equipment does not support IPv6, however, according to the standard, IPv6 support should be present.

If the evaluation is a successful test is done, then the following should be done:

- Use vendor management software over IPv4, as it lacks IPv6 support.
- The firewall should be replaced by one with IPv6 support.
- Routers on the user premises should be checked to have a list of IPv6-ready ones to facilitate the availability of IPv6 under request. The OSs on the user premises are a matter for the users, but the most probable case is that they will support IPv6.

3.6 Cellular phone network

Regarding the cellular phone network, little information was received. However, the things that are certain are:

- IPv6 support exists in both the GGSN and SGSN, but a software update is needed.
- The existing HLR software supports IPv6.
- IPv6 prefixes of length 64 should be assigned to each end user terminal/PDP context.

In summary, the IPv6 deployment in the cellular phone network should be postponed until information is received about IPv6 support in the different elements used, and configuration information is available from the vendor.

3.7 Services

The services to be considered in a first deployment phase are DNS and web servers. Their configuration is straightforward and a great deal of information is available on how to achieve this.

4. CONCLUSIONS

This document describes the aspects to consider for an ISP IPv6 implementation in a developing region. So far only the first steps have taken place, namely training, network analysis, and the creation of a draft plan for the implementation. The information given in this document has, for confidentiality reasons, been made as anonymous as possible.

The main problems in this - and other similar deployments - are related to the lack of IPv6 support on some devices, and the lack of information from some vendors. Also the management software IPv6 support was generally non-existent.

The proposed implementation plan is based on a phased approach, starting in the core network, then the connection to the IPv6 Internet, and then spreading network-by-network outwards until all the access networks have been completely covered. This means that the barriers on some current access technologies could be solved in future phases.

In a first overall view, the implementation phase of IPv6 on the core, backbone, Intranet, Internet connection, and basic services is feasible. This is expected to be also the case in similar ISP scenarios.

5. REFERENCES

[3GPP] Third Generation Partnership Project: http://www.3gpp.org

[6DEPLOY] The 6DEPLOY project, http://www.6deploy.eu

[TS23.060] 3GPP TS 23.060 V5.13.0 (2006-12): General Packet Radio Service (GPRS); Service description; Stage 2 (Release 5)

[TS23.228] 3GPP TS 23.228 V5.15.0 (2006-06): IP Multimedia Subsystem (IMS); Stage 2 (Release 5)