Title:	Document Version:
Deliverable D2.3 **IPv6 transition technologies**	1.0

Project Number:	Project Acronym:	Project Title:
297239	GEN6	Governments ENabled with IPv6

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
30/01/2012	30/01/2012	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:
Jordi Palet Martínez	Consulintel	WP2

Authors (organisations):

Alvaro Vives (Consulintel), Anastasios Zafeiropoulos (GRNET), Irene Gioxi (Intelen), Carsten Schmoll (FHG)

Abstract:

This deliverable presents possible approaches for the transition of existing IPv4 infrastructures to either dual-stack (medium term) or IPv6-only (long term), in order to support connectivity with both dual-stack, IPv4-only and IPv6 only networks.

Keywords:

IPv6, Governments, IPv6 Transition Mechanisms, Transition and Coexistence.

Revision History

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

Revision	Date	Description	Author (Organization)
v0.1	01/07/2012	Document creation	Jordi Palet (Consulintel)
v0.2	22/01/2013	Added Content	Alvaro Vives (Consulintel)
v0.3	29/01/2013	Added Content	Alvaro Vives (Consulintel)
v0.4	04/02/2013	Added Content	Anastasios Zafeiropoulos (GRNET), Irene Gioxi (Intelen)
v0.5	06/02/2013	Added Content	Carsten Schmoll (FHG)
v1.0	06/02/2013	Document revision	Alvaro Vives (Consulintel)

Disclaimer

Executive Summary

This deliverable presents possible approaches for the transition of existing IPv4 infrastructures to either dual-stack (medium term) or IPv6-only (long term), in order to support connectivity with both dual-stack, IPv4-only and IPv6 only networks.

The document is divided in four parts:

- Some generic scenarios are presented to be used in further discussions.
- Transitions mechanisms overview
- Transition and coexistence options using the considered scenarios and already seen transition mechanisms
- Information about transition strategies and mechanisms used in real public organization networks

Table of Contents

Figure Index

Table Index

1. INTRODUCTION

The background of this document is common to all data network today, the need of deploying IPv6. This is something that is getting really urgent because of the scarcity of IPv4 public addresses. This introduces two issues:

- **It gets difficult to get more IPv4 public address**, that are needed to connect to the IPv4 Internet and being visible publishing services or content. This is resulting in the use of translation mechanisms, using even several levels, that offers a degraded service to the end user. See, for example for NAT444 (two levels of NAT for IPv4), some scenarios [RFC6264] and some tests performed in real content providers [I-D. donley-nat444-impacts].
- **IPv6-only networks are appearing**, what results in the need to be visible over IPv6 to allow users on those network to access to our content. In other words, if we do not publish our services over IPv6 will get invisible, or at least blurred, to an increasing part of Internet.

The transition to IPv6 is something that have been taken into account from the beginning, when the new Internet Protocol was designed. The initial idea was that both protocols will coexist for several years and things should be done with enough time in advance. Nowadays there is an added issue, the IPv4 address space exhaustion, which introduces urgency and lack of public IPv4 addresses.

In this context, we will cover in this document the most relevant transition mechanism because of their utility, availability on vendor's products or real use in networks around the world.

After a brief description of theses transition mechanisms and transition approaches, suggestions will be given of possible approaches for the transition of existing IPv4 infrastructures to either dual-stack (medium term) or IPv6-only (long term), in order to support connectivity with both dual-stack, IPv4-only and IPv6 only networks, in order to warrantee the access to those infrastructures in all the possible scenarios.

This document ends with information about transition strategies and mechanisms used in real public organization networks.

2. CONSIDERED SCENARIOS

We will describe two generic scenarios to be used to illustrate further discussions.

2.1 Scenario 1

The first generic scenario we will describe is the smallest one, where the public administration network is not very big nor expands over a big geographical area. These kinds of networks are usually served by another bigger public organization, that in some cases are dedicated to provide the connectivity service.

Example of this scenario could be a University that has its own campus network, but connectivity is obtained through commercial ISPs or a NREN (National Research Network).

The following figure shows this scenario:

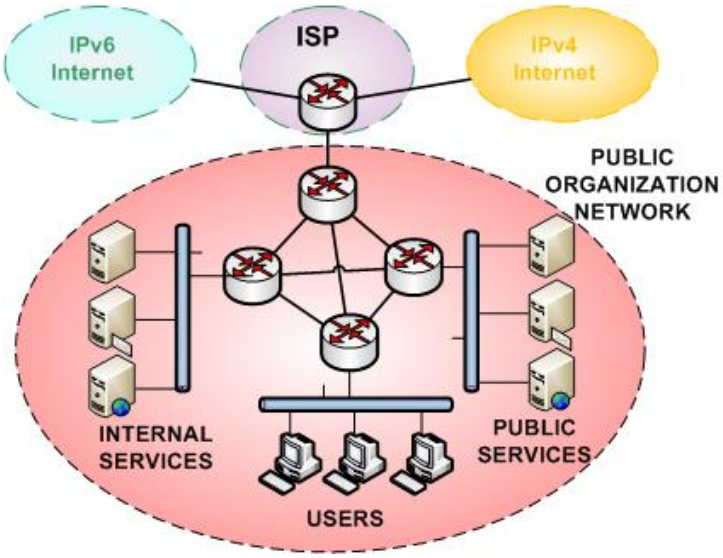

Figure 2-1: Scenario 1 scheme: small public organization

The public organization network is connected to both the IPv4 and IPv6 Internet through the ISP. The services published by the public organization could be divided in two types, for internal use only and also for public access.

2.2 Scenario 2

The second generic scenario is a network of a big public organization that expand over a big geographical area that could cover a whole country. This network could be used for the organization own needs or could be used to provide connectivity to other, usually smaller, organizations.

Example of this scenario could be a NREN (National Research Network) used to connect

educational and research institutions all over a country, or a government network used to give connectivity to local institutions all over a country.

The following figure shows this scenario:

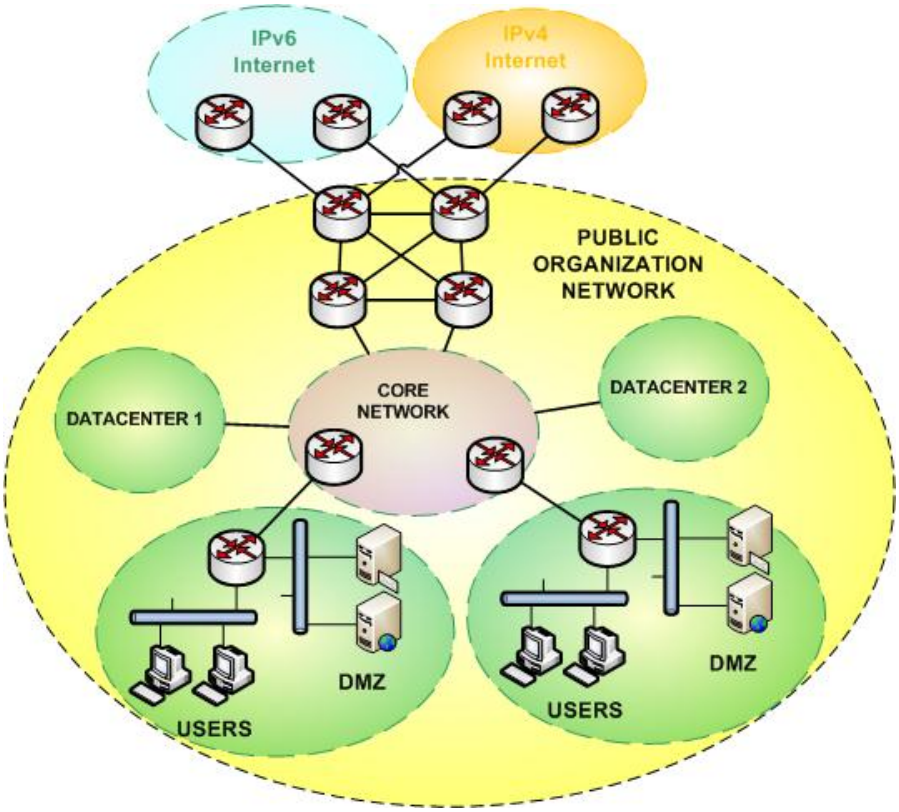

Figure 2-2: Scenario 2 scheme: big public organization

The public organization network is connected to both the IPv4 and IPv6 Internet.

3. TRANSITIONS MECHANISMS OVERVIEW

A public organization network could deploy three types of networks, not incompatible:

- **IPv4-only**: This makes sense with old technologies that being removed, networks where the effort or cost of implementation is too high or it's not possible because lack of vendors support.
- **IPv4 and IPv6**: The preferred option because coexistence of both protocols allows gradual and friendly transition from IPv4 to IPv6.
- **IPv6-only**: In some cases it makes sense to deploy IPv6-only networks to avoid further transition work. A mechanism is needed in order to allow access to the IPv4 Internet.

As stated above, the scope of this document is the last two options: dual-stack and IPv6-only.

Transitions mechanisms used to implement IPv6 in a network could be classified into three main groups, in order of preference:

- **Dual-stack**
- **Encapsulation-based transition mechanisms (Tunnels)**
- **Translation-based transition mechanisms**

Transition mechanisms within these three groups are not incompatible, so they can coexist in the same network depending on the needs and characteristics of the network.

3.1 Dual-Stack

Dual-stack strategy [RFC4213] is based on adding IPv6 capabilities to the network stack of IP devices, making them able to process IPv4 and IPv6 packets at the same time. This way, both protocol versions work in parallel in the same network. All operating systems that are currently in widespread use on PCs, servers, smart phones and tablet computers, already support IPv4/IPv6 dual stack operation. Even though, the set of supported functionalities does sometimes differ (e.g. mobile phones often support IPv6 only on the WiFi interface, not across 3G data networks). IPv6 support for software applications varies widely and needs to be checked for the used version. The detailed behavior of a computer system with regards to IPv6 depends on multiple parts together: Network, operating system, application and current settings.

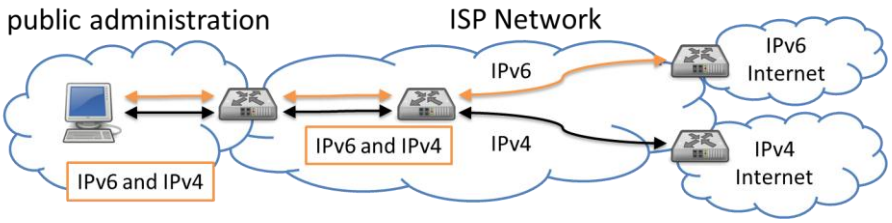

Figure 3-1: Dual-stack networking

For dual stack operation on the end-to-end path between software applications and their remote users, it is necessary for the IT infrastructure to provide full support for IPv4 and IPv6 on the IP Layer (Layer 3). This means that existing functions of IPv4 networks must also be available for IPv6, including:

- IP addresses and IP address management
- IP packet forwarding
- IP routing (where applicable)
- IP packet filtering (in firewalls and end systems)
- Application-specific gateways (also termed: application-level gateway – ALGW)
- An exception are transparent IPv6-over-IPv4 tunnels, which can traverse network paths that by themselves do not support IPv6.

A move towards dual-stack operation requires well-planned procedures for existing networks to avoid the compromising of existing functionality. Due to dependencies, the order of the migration process of the various mentioned systems must be planned and monitored carefully.

A detailed technical overview of IPv4/IPv6 dual stack operation and related transition techniques can be found in RFC4852: "IPv6 Enterprise Network Analysis IP Layer 3“ [RFC4852]. This document also explicitly describes the starting situation and the need for a graded systematic planning for introducing IPv6 in existing IT infrastructures.

The advantage of dual-stack approach is that it is a long term solution, because the work done to implement IPv6 on the network will be "forever", with no need to change things. This is why this is the recommended option if it's possible to implement it. Using dual-stack approach, services could be made available to users smoothly and in a transparent way. Using DNS, application will choose which protocol version to use. Native IPv6 could be offered at the same time as IPv4 connectivity using public or private addresses, using NAT.

The disadvantages are that it depends on the IPv6 support in network devices, that it affects all network devices used for data and services over IPv6, and it introduces an overload on the network management (for IPv4 and IPv6). It also usually requires adding memory to routing devices, and sometimes adding hardware or software updates.

Other problem detected is that dual-stack clients with bad IPv6 connectivity, when accessing a dual-stack server available over both IPv4 and IPv6, could have a bad experience because of the delay of the application on switching from the non-working IPv6 to IPv4. To solve this problem there are already implementations on web browsers and operating systems of the *happy-eyeballs* solution [RFC6555][RFC6556].

In the medium/long term, there could be parts of the network that could used IPv6-only in order to minimize the disadvantages. It's also expected that as the IPv6 traffic grows, IPv4 traffic decreases.

3.1.1 Option: Use of VLANs for handling IPv4 and IPv6 in the Intranet

Using VLANs (VLAN tags), one can separate different logical networks. Considering IPv6, it would be an option to setup separate VLANs for the IPv6 traffic only, and to keep existing IPv4-only VLANs as is. A precondition for this operational model are certain technical features in the existing infrastructure, such as VLAN functionalities according to IEEE 802.1Q on all affected switches in the infrastructure.

This technique is described in detail in [RFC4554]. It is based on the idea of distributing all IPv6 traffic in an Intranet across newly spanned Layer 2 VLANs. Switches must be configured as a VLAN-based Layer 2 “overlay” network. This is schematically shown in the following figure:

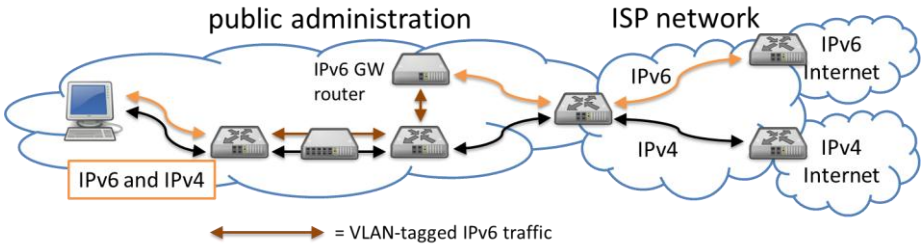

Figure 3-2: IPv6 over VLANs in the Intranet

However, in general, a complete modernization of dual-stack-capable routers, switches and security devices should be preferred. In this VLAN-based solution, the different processing and routing of the two versions of IP packets leads to the risk of having different latencies plus complex errors in the network if one of the two protocols fails. This partially originates from the fact that the VLAN-based solution leads to different routes in the Intranet for IPv4 and IPv6 traffic.

Overall, this solution should not be deployed when it is planned to introduce native IPv4/IPv6 dual stack operation (or even IPv6-only subnets) in the near future. In that case, it would only induce a substantial amount of extra work for a non-sustainable intermediate solution.

3.2 Encapsulation-based transition mechanisms

Where, for any reason, it is not possible to implement dual-stack, encapsulation-based transition mechanisms could be used. Basically what they do is to encapsulate traffic of one version of the IP protocol into the other version packets, IPv6 into IPv4 or IPv4 into IPv6. Tunnels could be static (manually configured [RFC4213][RFC2784] or using a tunnel broker [RFC3053][RFC5572]) or automatic/dynamic.

In the last years different solutions appeared to provide IPv6 connectivity over an IPv4-only network using tunnels. In the following table the most common, used or successful are briefly described and analyzed:

Mechanism	Features	Advantages	Disadvantage
Static / Tunnel Broker	- Static establishment - Supports authentication	- Good scalability - NAT Traversal (with TSP [RFC5572])	- No good management - Tunnel service discovery configured manually - Doesn't support well client's IPv4 change - Poor performance if other tunnel endpoint is far
Teredo	- Automatic establishment - Usually from host to router Generates signalling traffic to get information about used NAT and obtain an IPv6 address Encapsulates IPv6 in UDP/IPv4	- Works well through NAT - Very good scalability - Automatic tunnel service discovery	- Poor security - Difficult to manage - IPv6 Prefix defined for clients - Asymmetric model - Not reliable
6to4	- Automatic establishment - Usually from router to router	- Very good scalability - Automatic tunnel service discovery - Good support on commercial platforms	- Poor security - Difficult to manage - Client needs a public IPv4 - IPv6 Prefix defined for clients - Asymmetric model - Not reliable
Softwires	- Automatic establishment - No new protocols defined, use existent ones - Based on L2TPv2 or L2TPv3 - All elements are under control of the ISP	- Good security - Good management - Good scalability - Works through NAT - There's good support of needed protocols - From the users and IPv6 Internet point of view, looks like a native IPv6 network	- Tunnel service discovery is configured - CPE's software need to be updated - New network element needed: SC (Softwires Concentrator)
6RD	- Automatic establishment - Based in 6to4 but inside an ISP and with some changes - Anycast IPv4 addresses	- Security supported (same as for IPv4) - An ISP own prefix could be used - Very good scalability - Automatic tunnel service	- Sit needs a software change in the CPE - A new element is needed: 6RD relay, by now not too mucho support by vendors although improving

	used to announce internally in the ISP 6RD relays - All elements are under control of the ISP	discovery - ISP's IPv6 prefix used for clients From the users and IPv6 Internet point of view, looks like a native IPv6 network Supports implementation of multiple relays, it's scalable and robust - Works with public and private IPv4 for the user	
6PE	- Automatic establishment - Works over an existent MPLS network - Medium implementation complexity	- Only border routers (PE) need to be configured - Use the benefits of MPLS	- Need a previous working MPLS/IPv4 infrastructure
6VPE	- Automatic establishment - Works over an existent MPLS network - Configuration and mechanisms used similar to 6PE to provide IPv6 VPN (L3VPN) using the same IPv4/MPLS network - Medium implementation complexity	- Only border routers (PE) need to be configured - Use the benefits of MPLS - Supports IPv4 at the same time as IPv6	- Need a previous working MPLS/IPv4 infrastructure

Table 3-1: Tunneled Transition mechanisms

In summary, from the transition mechanisms showed in the table, **Teredo** [RFC4380] and **6to4** [RFC3056][RFC3068] could be discarded because of management problems and poor quality control. However, as these transition mechanisms are activated by default in current operating systems, specifically Teredo (if the user has a private IPv4 address) or 6to4 (if the user has a public IPv4 address), it could be useful in case of having a big network, to do what some ISPs are doing, implement 6to4 and Teredo relays, to avoid users' bad experiences.

Static tunnels could be used temporarily and in a small number, because it's not a solution that scales. There are some commercial solutions that make all the process automatically, but as this is a temporal solution, it could make the costs not affordable, as you will have to implement native IPv6 in the future.

The other solutions like **Softwires** [RFC5571], **6RD** [RFC5569][RFC5969], **6VPE** [RFC4659] y **6PE** [RFC4798] could be considered as an interesting option to be used, having always in mind that they are temporary.

Softwires and 6RD could give IPv6 connectivity in the parts of the network where dual-stack

couldn't be implemented, with the condition of being able to find the necessary equipment that implements the solution.

The following figure illustrates softwires solution (AAA mechanisms not included), where the SI (Sofwires Initiator) establishes a tunnel with the SC (Softwires Concentrator):

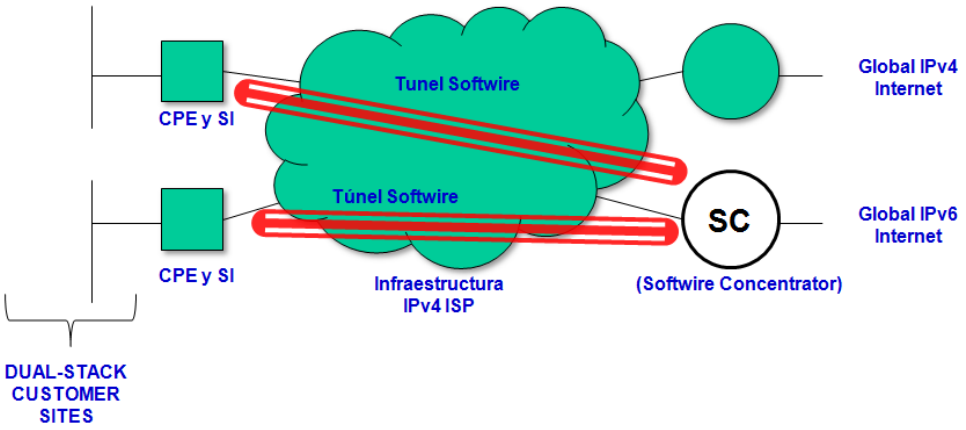

Figure 3-3: Softwires Scheme

The following figure shows a simplified 6RD scheme:

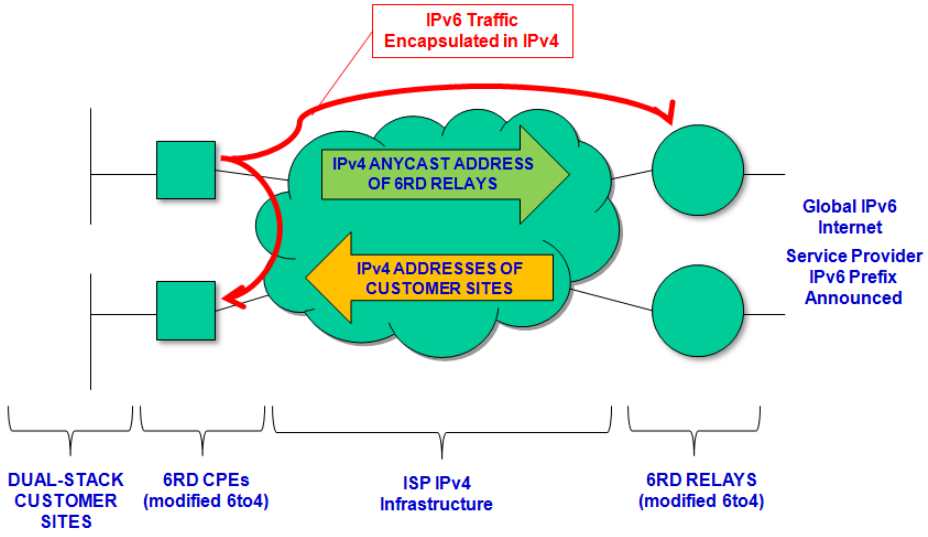

Figure 3-4: 6RD Scheme

Another mechanism is **6PE** that allows for IPv6 connectivity using an existent IPv4/MPLS infrastructure. Actually is the only scalable solution to have MPLS with IPv6, in other words, there is no vendor support to implement an IPv6-only MPLS network. The next figure shows some details about 6PE.

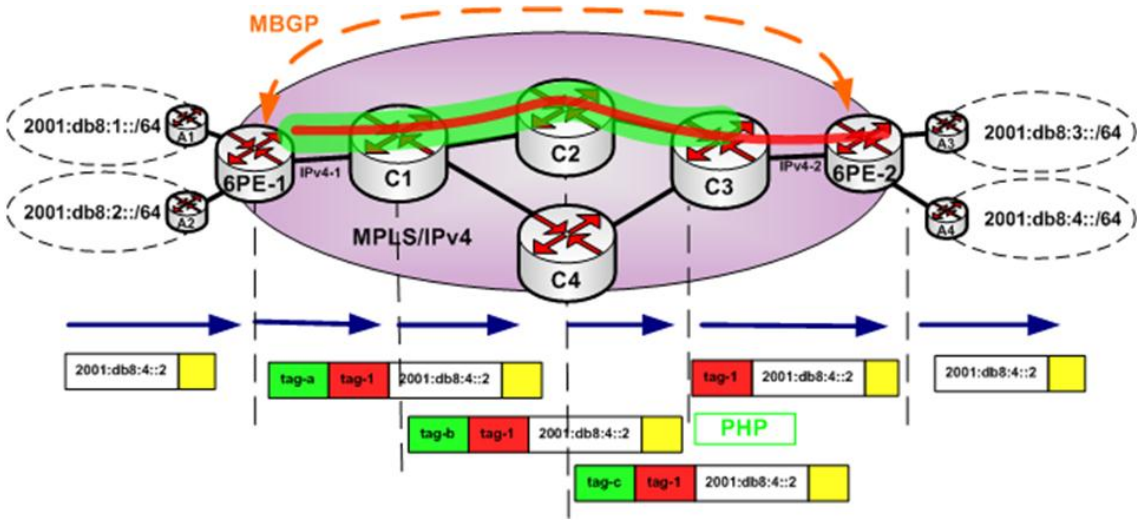

Figure 3-5: 6PE Details

In the figure there are 4 IPv6 prefixes distributed between the same number of access routers (A1-A4). 6PE-1 and 6PE-2 establish an MBGP session between them to announce the known prefixes using the mapped-IPv4 address created from an IPv4 address of the MPLS/IPv4 network (::FFFF:IPv4/128). A tag is associated to each prefix announcement. In addition to announce their prefixes, 6PE routers learn each other routers prefixes from the MBGP session. In the figure, for example, 6PE-1 learns from 6PE-2 the following:

```
Prefix              Next-Hop         IPv6- Tag
2001:db8:3::/64    ::FFFF:IPv4-2     tag-2
2001:db8:4::/64    ::FFFF:IPv4-2     tag-1
```

When a node in 2001:db8:2::/64 subnetwork sends a packet to the 2001:db8:4::/64 subnetwork, when reaches 6PE-1, it adds to labels. The label inside is the IPv6 label announced by 6PE-2 and the outer label is the IPv4/MPLS label (in the figure the PHP - Penultimate Hop Popping - technique is used to eliminate the MPLS label in the penultimate hop). The IPv6 packet reaches 6PE-2 only with the IPv6 label that is used to quickly send it to the correct interface with no label.

A similar behavior has the mechanism called 6VPE (use of IPv6-VPNs over an IPv4/MPLS network) where the VPN-IPv6 address family is used in the access routers to the IPv4/MPLS network. VPN-IPv6 routes are distributed using MBGP. At a logical level, 6VPE could be seen as multiple layers of 6PE, where each layer has its own routing table and its data traffic.

3.3 Translation-based transition mechanisms

Transition mechanisms based on translation could be used to enable communication between devices that only support one version of the IP protocol and devices that only support the other

version of the IP protocol. This is needed because both versions of the IP protocol are not compatible. Translation could be done in network, transport or application layer.

Translation could be used to allow IPv4-only devices communicate with IPv6-only devices. For this purpose mechanisms like **NAT-PT** (at network level) and **TRT** (at transport level) were designed, but were deprecated as standard long time ago and are not recommended at all [RFC4966].

ALGs (Application Level Gateways) could be useful in some scenarios and for some protocols, for example as web and e-mail proxies.

In the group of ALGs we could include a solution that some content providers are using by means of load balancers and server farms. This is a quick solution that allows a gradual and transparent transition of the servers infrastructure. A web content provider, for example, could use load balancers in two ways as transition mechanisms:

- **IPv4 Client - IPv6 Server**: Domain name of the web servers resolve only to IPv4 addresses, which are configured in the *public* face of the load balancers. Load balancers redirect requests towards the server farm where some have IPv4 and others have IPv6. This way, IPv6 support could be added gradually to the server farm.
- **IPv6 Client - IPv4 Server**: Domain name of the web servers resolve to IPv6 addresses (or to both IPv4 and IPv6) that are configured in the public face of the load balancers. Load balancers redirect requests towards server with IPv4 addresses inside the server farm. IPv6 servers could be introduced gradyally and start attending requests from load balancers. This scenario need that the content provider has a good IPv6 connectivity and changes in the DNS to add IPv6 addresses associated to the served webs.

Translation, in the context of solutions for the transition and coexistence we are in, should be the last resort, because they are complex, do not support all the protocols, use some tricks, and of course, they are not a long term solution. An exception, because of it cost/ease of implementing/offered service rate are proxies serving as load balancers.

Translation could also be used to allow communication from IPv6-only with IPv4-only devices. Actually this is being used in real tests in mobile phone operators and there are several implementations available of the mechanism called **NAT64/DNS64** [RFC6144-RFC6147, RFC6052], that is similar to NAT-PT but improved.

NAT64 allows that multiple IPv6-only nodes share a public IPv4 address to access the IPv4 Internet. It has been defined that only supports TCP, UDP and ICMP. Implementation of IPv6-only network will be something common in the mid-term as IPv4 addresses continue to exhaust and IPv4-to-IPv4 translation techniques become more expensive than implementing IPv6.

The following figure shows the packet flow for web access using NAT64 to an IPv4-only web site (www.example.com):

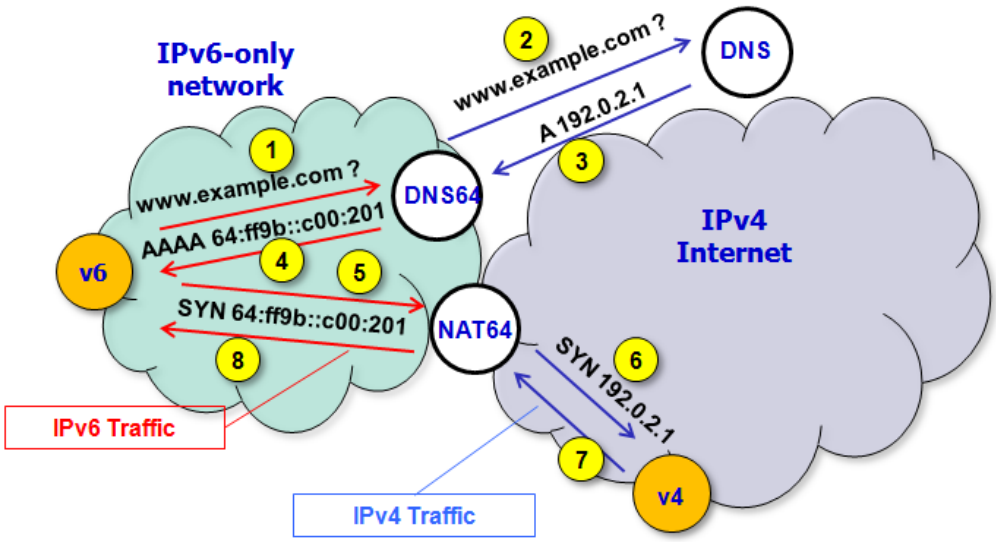

Figure 3-6: NAT64/DNS64 example

It's known that there are things that don't work:

- Everything out of TCP, UDP, or ICMP: Multicast, Stream Control Transmission Protocol (SCTP), the Datagram Congestion Control Protocol (DCCP), and IPsec.
- Applications that carry layer 3 information in the application layer: FTP [RFC6384], SIP/H323.
- Some applications: online gaming, skype, etc.

Recently, **NAT66** [RFC6296] has been standardized. Some reason for this could be seen in [RFC5902]. Again, this mechanism is not recommended, as any other based on translation.

4. TRANSITION AND COEXISTENCE OPTIONS

Basing the discussion on the considered scenarios and already seen transition mechanisms there will be different options we can consider in a public organization network.

4.1 Option 1: Native Dual-stack

The objectives will be:

- **Provide dual-stack connectivity to users**: Users should be able to connect using native IPv4 and IPv6 to internal services and to Internet.
- **Publish services in dual-stack**: Services publicly available over both IPv4 and IPv6, and properly announced in the DNS.
- **Carry IPv6 traffic natively inside the public organization network,** in addition to native IPv4.

The following figure illustrates the scenario for the small public administration network, with dual stack connectivity.

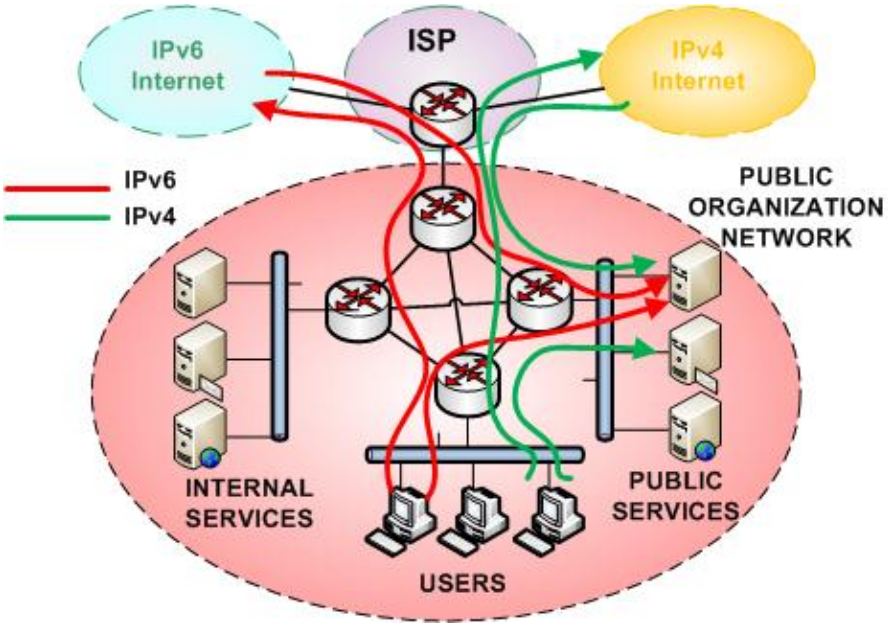

Figure 4-1: Dual-stack: small public organization network

The following figure illustrates the scenario for the big public administration network, with dual stack connectivity.

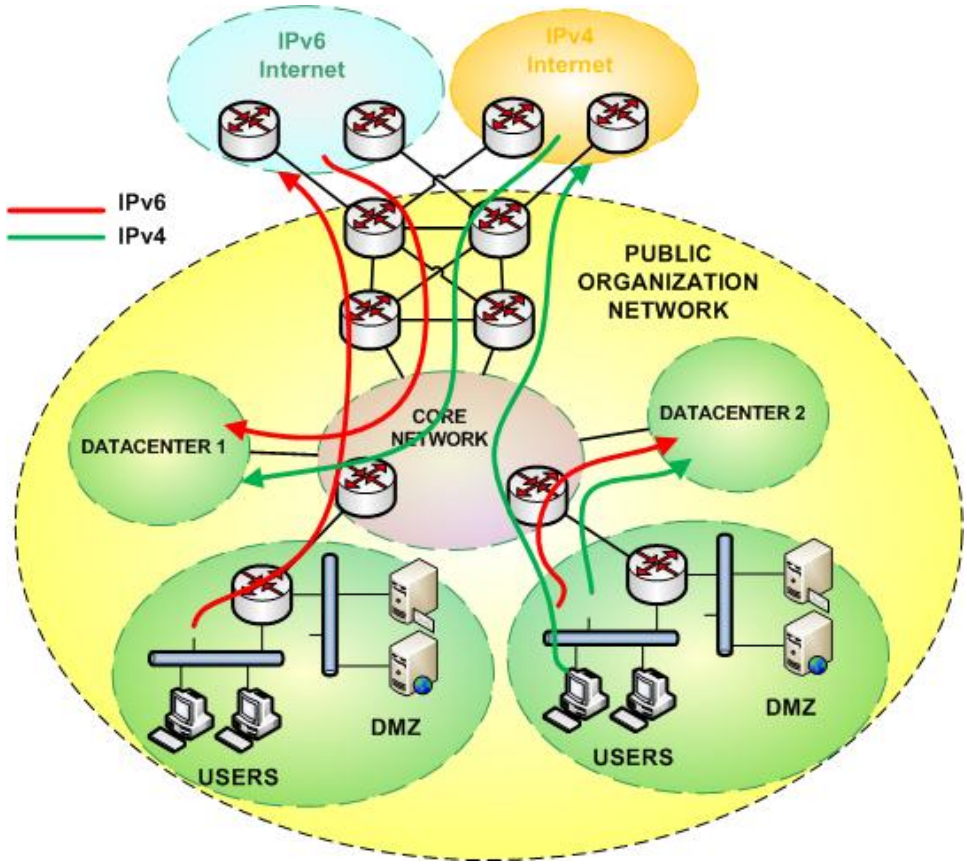

Figure 4-2: Dual-stack: big public organization network

In both scenarios, IPv6 and IPv4 packets flow natively through the whole network; they are not encapsulated in, nor translated to, other version of IP. If all users have IPv6 connectivity, and internal and public services are available over IPv6, then it's expected that internally the users will use only IPv6, i.e., the only need for IPv4 for internal users would be IPv4-only services in Internet.

4.2 Option 2: Mixed scenario

The following scenario shows a mix of native and encapsulation-based transition mechanisms. This is a very common scenario. The objectives will be:

- **Provide dual-stack connectivity to users**: Users should be able to connect using native IPv4 and IPv6 to internal services and to Internet. From their point of view, they are using a native dual-stack network. In other words, final users' LAN should be native dual-stack independently of the mechanism used for that.
- **Publish services in dual-stack**: Services publicly available over both IPv4 and IPv6, and properly announced in the DNS.
- **Carry IPv6 traffic inside the public organization network**: If native dual-stack is not available for any reason, an encapsulation-based mechanism should be used.

The objectives illustrate the idea that connectivity to IPv6 internet and users' final LAN should

be native dual-stack. Encapsulation-based transition mechanisms could be used inside our network. The only exception, that should be solved as soon as possible, is the connectivity to IPv6 Internet, that could use a tunnel in case our service provider doesn't support native IPv6 yet.

The following figure illustrates the scenario for the small public administration network. The native IPv4 traffic will flow as shown in previous section figure, only IPv6 is depicted.

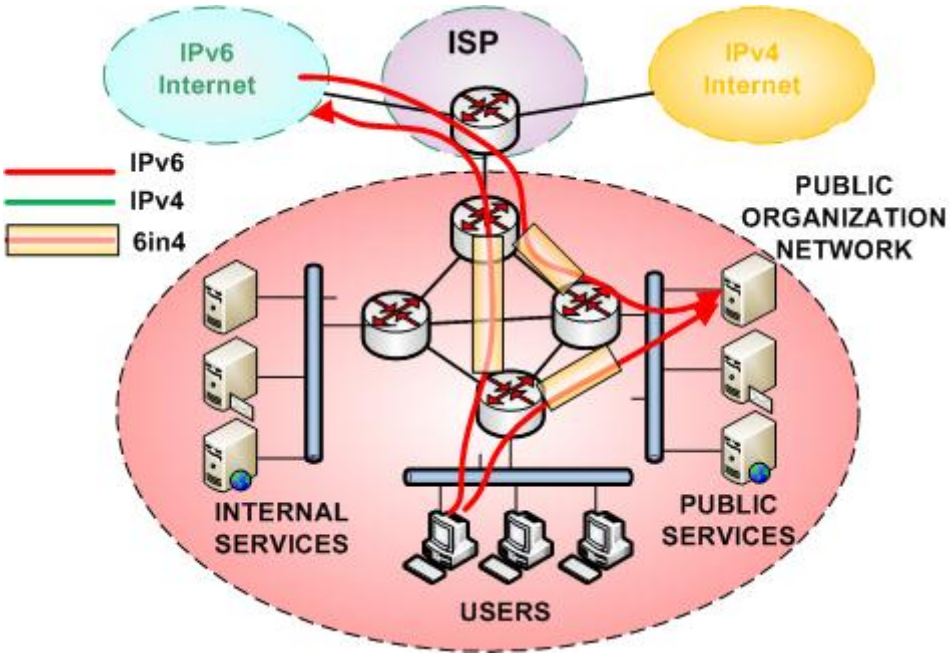

Figure 4-3: Mixed Scenario: small public organization network

The following figure illustrates the scenario for the big public administration network. The native IPv4 traffic will flow as shown in previous section figure, only IPv6 is depicted.

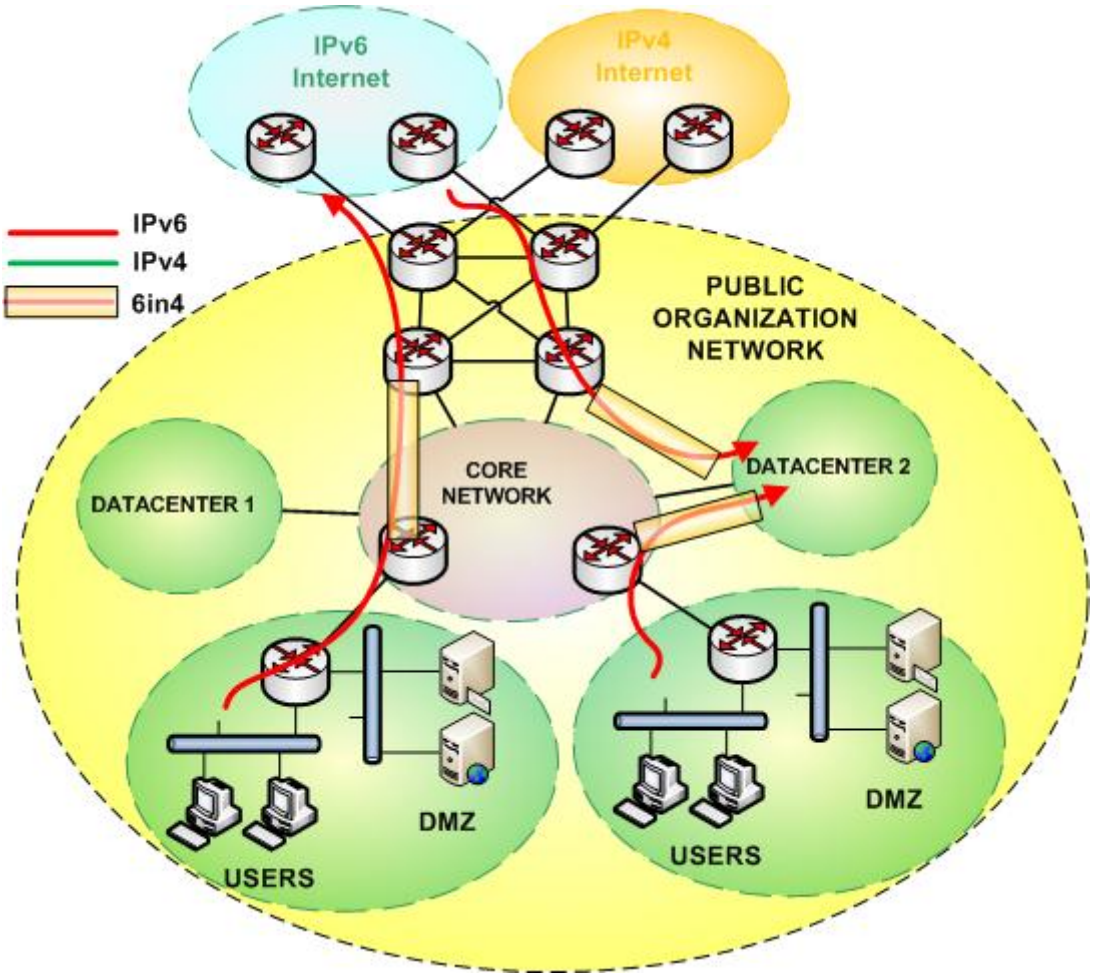

Figure 4-4: Mixed Scenario: big public organization network

Figures show only how IPv6 traffic flows in the public organization network being encapsulated into IPv4 (6in4) to cross the core of the network. This could be accomplished, for example, using static tunnels between shown routers. Remember that static tunnels are not a scalable solution.

Other transitions mechanisms could be used, for example:

- In the small public organization network: Dynamic mechanisms like 6RD could be used between the router that connects to the ISP and all the other routers inside the network. This way, any new router for any new or existent network, should configure 6RD, and will be able to provide IPv6 connectivity to the LANs it serves.
- In the big public organization network: If the core network used MPLS, then 6PE or 6VPE could be used. In some cases layer two VPNs, like VPLS, could be used because they are IP-agnostic, i.e., they doesn't matter about the IP version of packets flowing through the MPLS cloud.

4.3 Option 3: IPv6-only

The last option is to implement an IPv6-only network and configure a mechanism to allow users

to connect to the IPv4 Internet. This is shown for the whole network, but could be used only in one part. This is a mid-term scenario, to be used when there are really no more IPv4 public addresses and the content and services available over IPv6 are the majority.

The objectives will be:

- **Provide IPv6-only connectivity to users**: Users will see an IPv6-only network.
- **Provide a mechanism allowing our IPv6-only users to connect to the IPv4 Internet content**.
- **Publish services in dual-stack**: Services should be made available to both the IPv4 and IPv6 Internet
- **Carry native IPv6 traffic inside the public organization network**: Traffic within the public organization network will be IPv6-only.

The following figure illustrates the scenario for the small public administration network. The native IPv6 traffic will flow as shown in Native Dual-stack section figure, only connectivity to/from IPv4 Internet is depicted. There will be no internal IPv4 traffic in the public organization network.

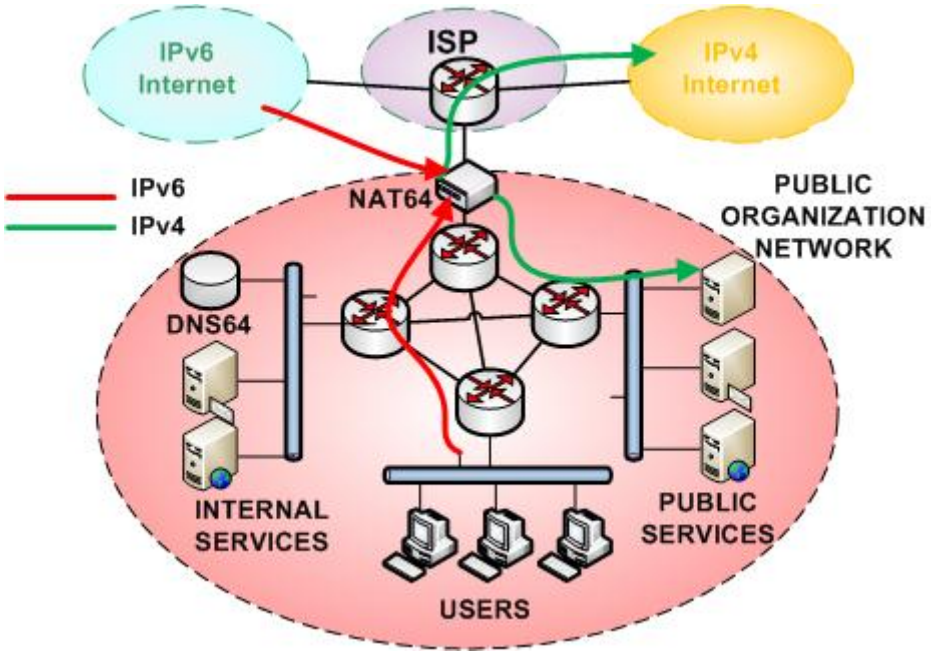

Figure 4-5: IPv6-only Scenario: small public organization network

The following figure illustrates the scenario for the big public administration network. The native IPv6 traffic will flow as shown in Native Dual-stack section figure, only connectivity to/from IPv4 Internet is depicted. There will be no internal IPv4 traffic in the public organization network.

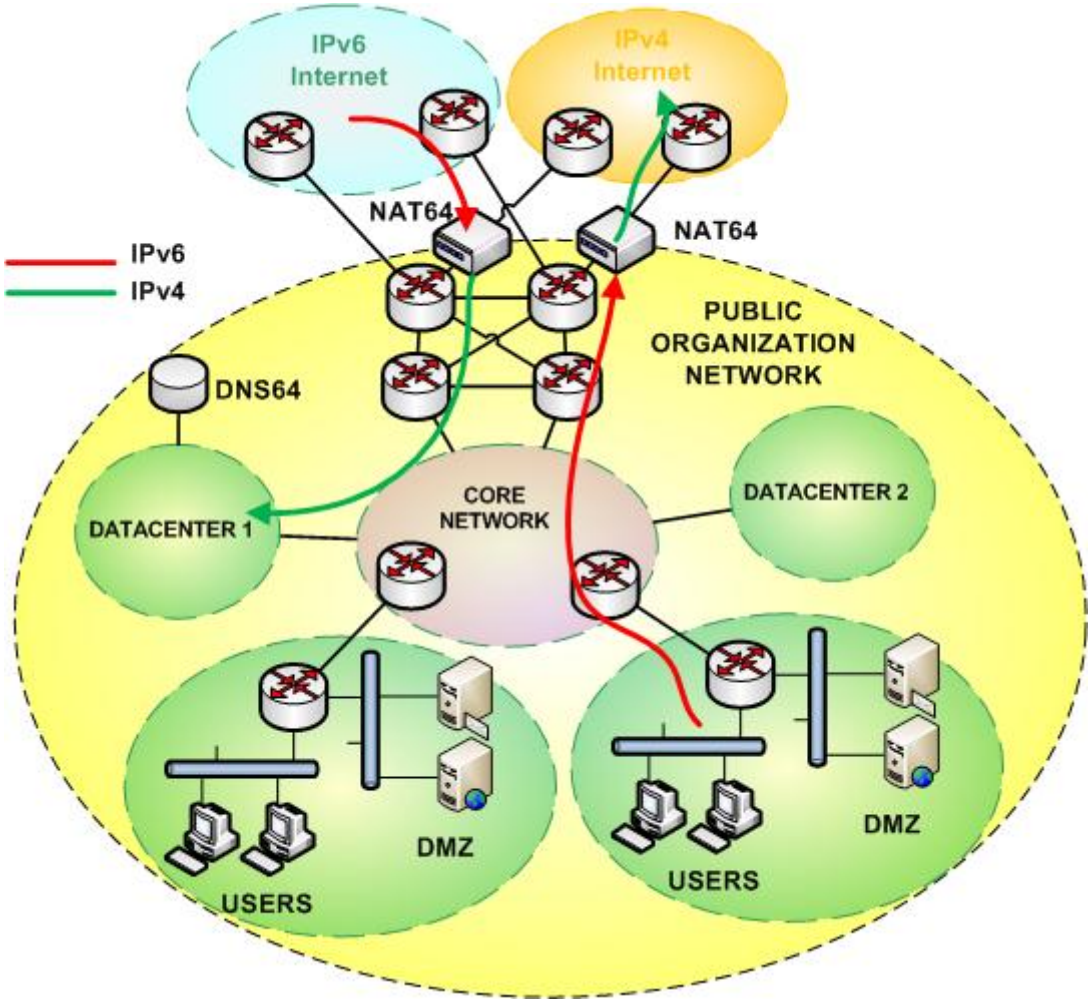

Figure 4-6: IPv6-only Scenario: big public organization network

In both figures we could see two new elements, the DNS64 and the NAT64. The DNS64 is used by internal users as the DNS server, with the difference that in case of resolving a domain name to only an IPv4 address, it automatically generates an IPv6 address using the obtained IPv4 address and an internally well known prefix (usually 64:ff9b::/96). The internal users will always think that they are connecting to IPv6 addresses associated with the domain names.

The NAT64 box is the one in charge of doing the translation, in the figure it's used in two ways:

- **Connect my IPv6-only network to the IPv4 Internet**: This is called stateful NAT64, and is based on the NAT64 boxes receiving all the traffic directed to the internally well known prefix (for example, 64:ff9b::/96), and translating the packets from IPv6 to IPv4 when going out, keeping the state of the translation done, and reversing the translation when a response come back.
- Connect the IPv4 Internet to my IPv6 servers (not recommended): This is usually called stateless NAT64, and in case of already having internal IPv6, it would be better to offer the service over IPv6. In case this is not possible or having a servers farm, IPv6 requests could be received and translated to IPv4 before being sent to the server. In this solution,

a 1 to 1 translation is done between IPv6 and IPv4, and the public DNS domain name should be configured to resolve to the appropriated IPv6 address that will be translated to an IPv4 one.

It should be clearly stated that the NAT64 mechanisms has several drawbacks and should not be considered as a long term solution.

5. EXAMPLES

In the following sections, information about transition strategies and mechanisms used in real public organization networks is shown.

5.1 Greek Example

IPv6 Transition planning for SYZEYXIS-II: The public network SYZEYXIS-II is planned to become a multi-service platform for interconnecting 34 thousands public sector organisations and providing advanced services to public servants in Greece for the fiscal years 2014-2017. The public network SYZEYXIS-II will be based on Internet technologies and protocols, while IPv6 support will be considered for the provision of advanced services.

Due to the IPv4 address depletion problems, the public network today extensively uses private IPv4 addresses by using NAT gateways. Therefore, multiple technical challenges have to be addressed that increase the management overhead as well as the risk of service disruption. The network SYZEYXIS-II has to target to offload as much as more traffic to IPv6 from the day one of its operation. This can be achieved through the establishment of dual stack networking infrastructure and the provision of dual stack services. Dual stack connectivity in the backbone network as well as basic networking services (e.g. DNS, ACLs, etc) have to support IPv6 functionality from day one. In addition, the network SYZEYXIS-II has to target to enable IPv6 protocols in the access network, either over lease lines or broadband connections. If existing equipment is going to be (re)used, the IPv6 services has to be provided on case-by-cases basis, even by manually configured tunnels or through other possible alternatives. Existing services have to be upgraded to support IPv6 with appropriate software and hardware upgrades. Some of the existing services may not need to be upgraded to IPv6 due to high CAPEX/OPEX costs, and using instead alternative translation services via load-balancers or other well-proven technologies. Initially, an addressing plan has to be designed taking into account the backbone network and the network interconnecting the different ministries and organizations. Transition use cases have to be specified taking into account the need for dual stack support per region or per type of agency, the interconnection of governmental data centres and the need for IPv6 support in the provided services.

Dual stack IPv4/IPv6 support in the Greek pilot in GEN6: As stated in the deliverable D2.2 of the GEN6 project, the Greek School Network (GSN) and the Greek Research and Technology Network (GRNET) support both IPv4 and IPv6 into their backbone networks. Furthermore, tunnelling services are provided from GRNET for customers that want to acquire IPv6 access into their networks for testing purposes.

In the Greek pilot within GEN6 (see Figure below), the core and access network is IPv6 enabled

including the smart energy metering devices. Intelen's infrastructure implements dual stack architecture, as it functions both over IPv4 and IPv6 over the GSN's and GRNET's network. Intelen's Advanced Metering Infrastructure (AMI - via i-box) has IPv6 bidirectional communication to send and receive both data and remote management commands to Intelen's Master Data Management (MDM) infrastructure. The AMI infrastructure can function over either IPv6 or IPv4, while the default communication option is over IPv6. As long as the MDM is concerned, the dual stack architecture ends at the entrance point of Intelen's cloud, which is a set of load balancers that operates over both protocols. At the moment an 'IPv6 only' scenario is feasible and functional, provided that the communication network between AMI components and MDM is functional. Currently, in the deployed infrastructure, IPv6 support in the i-box is enabled by default while i-box IPv6 auto-configuration mechanisms are also active.

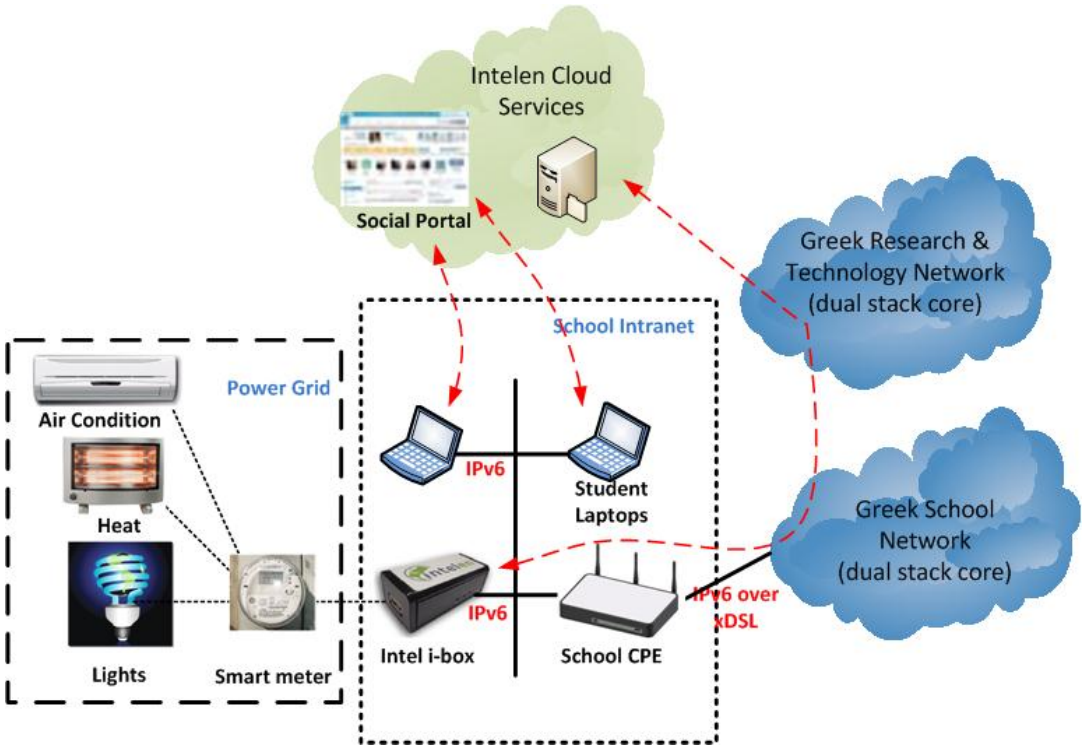

Figure 5-1: Greek pilot interconnection scheme

6. CONCLUSIONS

The transition mechanisms and strategies to be used in a public organization network are different and there are several options. We have shown some of them and classified them in three categories, clearly stating that a native dual-stack approach should be the preferred one. any other solution, should be seen as a temporary solution, that will eventually be eliminated from the network.

7. REFERENCES

[I-D. donley-nat444-impacts]	C. Donley, L. Howard, V. Kuarsingh, A. Chandrasekaran, V. Ganti, "Assessing the Impact of NAT444 on Network Applications", draft-donley-nat444-impacts-05 (work in progress), October 2012
[RFC2784]	D. Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, "Generic Routing Encapsulation (GRE)", March 2000
[RFC3053]	A. Durand, P. Fasano, I. Guardini, D. Lento, "IPv6 Tunnel Broker", January 2001
[RFC3056]	B. Carpenter, K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", February 2001
[RFC3068]	C. Huitema, "An Anycast Prefix for 6to4 Relay Routers", June 2001
[RFC4213]	E. Nordmark, R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", October 2005
[RFC4380]	C. Huitema, "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", February 2006
[RFC4554]	T. Chown, "Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks", June 2006
[RFC4659]	J. De Clercq, D. Ooms, M. Carugi, F. Le Faucheur, "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN ", September 2006
[RFC4798]	J. De Clercq, D. Ooms, S. Prevost, F. Le Faucheur, "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE) ", February 2007
[RFC4852]	J. Bound, Y. Pouffary, S. Klynsma, T. Chown, D. Green, "IPv6 Enterprise Network Analysis - IP Layer 3 Focus", April 2007
[RFC4966]	C. Aoun, E. Davies, "Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status", July 2007
[RFC5569]	R. Despres, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) ", January 2010
[RFC5571]	B. Storer, C. Pignataro, Ed., M. Dos Santos, B. Stevant, Ed., L. Toutain, J. Tremblay, "Softwire Hub and Spoke Deployment Framework with Layer Two Tunneling Protocol Version 2 (L2TPv2) ", June 2009
[RFC5572]	M. Blanchet, F. Parent, "IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP)", February 2010
[RFC5902]	D. Thaler, L. Zhang, G. Lebovitz, "IAB Thoughts on IPv6 Network Address Translation", July 2010
[RFC5969]	W. Townsley, O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification", August 2010
[RFC6052]	C. Bao, C. Huitema, M. Bagnulo, M. Boucadair, X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", October 2010
[RFC6144]	F. Baker, X. Li, C. Bao, K. Yin, "Framework for IPv4/IPv6 Translation", April 2011
[RFC6145]	X. Li, C. Bao, F. Baker, "IP/ICMP Translation Algorithm", April 2011
[RFC6146]	M. Bagnulo, P. Matthews, I. van Beijnum, "Stateful NAT64: Network Address and Protocol

	Translation from IPv6 Clients to IPv4 Servers", April 2011
[RFC6147]	M. Bagnulo, A. Sullivan, P. Matthews, I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", April 2011
[RFC6264]	S. Jiang, D. Guo, B. Carpenter, "An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition", June 2011
[RFC6296]	M. Wasserman, F. Baker,"IPv6-to-IPv6 Network Prefix Translation", June 2011
[RFC6384]	I. van Beijnum, "An FTP Application Layer Gateway (ALG) for IPv6-to-IPv4 Translation", October 2011
[RFC6555]	D. Wing, A. Yourtchenko, "Happy Eyeballs: Success with Dual-Stack Hosts", April 2012
[RFC6556]	F. Baker, Testing Eyeball Happiness, April 2012