Transition Strategies from IPv4 to IPv6: The case of GRNET

C. Bouras[1,2], P. Ganos[1], A. Karaliotas[1,2]

[1]Research Academic Computer Technology Institute, Patras, Greece
[2]Department of Computer Engineering and Informatics, University of Patras, Greece
e-mail: bouras@cti.gr

Abstract

In this paper we describe the results that came out from the project of employing the IPv6 protocol over the Greek Research & Technology Network (GRNET). In the way of this process one of the big issues that had to be considered was the transition strategy that would be deployed. The main goals of a transition strategy are to be smooth enough and therefore to put the less of configuration overhead to the end users and the network administrators.

Keywords

Networks, Protocols, IPv6, Transition mechanisms,

1. Introduction

The IP protocol and its current version, IP version 4, is the most widely used protocol in computer networks in our days. The big change that happened to the character of the Internet, from a rather academic network with low demands on resources to a commercial network with a variety of intensive applications running over it – considering also the integration of other communication services on it e.g. VoIP – showed the weakness of the fourth version to support the new networking applications. The reasons that led the Internet community to adopt the development of a new IP version are summarized in the following.

Lack of Addresses: The address space of IPv4 is 2^{32}. This space is decreasing because of the sub netting procedure and the dedicated areas in the IP space for several operations like private networks and multicasting. The IP space that has been left is running out. There are new demands for IPs, while new devices tend to connect to the IP networks, such as home devices and mobile phones.

Performance-Manageability: The lack of hierarchy levels in IP addresses results the existence of too many -hard to manage- routing entries to the routers. Also, several applications demand for Quality of Service (QoS) support from IPv4 and this shortcoming is overleaped by the use of protocols in higher levels with uncertain results.

Security: Considering the wide spread of Internet and its use for several transactions, like financial ones, the security is an issue that has to be supported by the IP protocol, which must be able to provide reliable and efficient security mechanisms.

Automatic Address Assignment: The configuration procedure in IPv4 hosts is complex and requires human interference. Users would prefer a procedure of type “plug and play”. When a computer is plugged to the IP network, the connection parameters may be configured automatically without the human interference. This capability is suitable enough for mobile users.

The new version of IP protocol, IP version 6, seems to be a satisfactory solution of the above limitations (Deering and Hinden, 1998). It is foreseen that the deployment of IPv6 is probably inevitable and it is only a matter of time to see exactly when ipv6 will become the basic internetworking protocol. Since the number of network applications that currently IPv4 supports, is enormous and the porting procedure will cost much in terms of money and time, the only applicable solution that will lead to a global dominance of IPv6 is the coexistence of IPv4 and IPv6 for a quite large period of time. In a mixed situation, where both protocols co-exist communication between IPv4 hosts over an IPv6 network, IPv6 hosts over an IPv4 network and IPv6 host and an IPv4 host must be achievable.

2. Transition Mechanisms

The transition mechanisms are considered as a toolset to enable the smooth transition to the new version of the IP protocol. These mechanisms are divided into three (3) main categories depending on their operation and the way of their implementation: Dual Stack Mechanisms, Tunneling Mechanisms and Translation Mechanisms.

2.1. Dual Stack Mechanisms (DSM)

This mechanism is the deployment of a quite simple idea. Any host that desires to participate both in IPv4 and IPv6 networks has to maintain both stacks on its network interface(s). It enables a full IPv4 end-to-end communication between a dual stack host within an IPv6 only network and an IPv4 only host. The DST mechanism is based on tunneling mechanism using a dynamic tunnel interface combined with temporary IPv4 address assignment provided by a DHCPv6 server.
The Dual Stack Transition Mechanism (DSTM) is based on the usage of a DHCPv6 server, which assigns temporarily global IPv4 addresses to IPv6 hosts that wish to communicate with an IPv4 only host (Tsirtsis, 2000). The IPv4 packets are encapsulated into IPv6 packets through a DTI interface and are transferred within the IPv6 network to the Border Router, which interconnects the IPv6 network with the IPv4 network.
One critical issue for the implementation of the DST mechanism is the support of the Domain Name Service (DNS) and the impact of this service to the preference of a host to the IPv4 and/or the IPv6 protocol (Gilligan and Nordmark, 2000). In order a network host to be capable to communicate with other hosts by the use of both protocols, this host has to dispose the appropriate libraries and to ask the DNS for the address of IPv4, IPv6 and IPv4/IPv6 hosts. This means that the libraries have to be able to handle both A records (IPv4) and AAAA/A6 records (IPv6). It is concluded that the DNS support in DST mechanisms is a parameter that affects the network performance.
The operation of the DSTM is bi-directional, which means that the initialization of the communication may take place either from the IPv6 host side or the IPv4 host side. This is a major advantage of DTSM compared to other mechanisms, which allow the initialization of the communication only from the IPv6 host side. The DSTM requires the usage of a DHCP server and optionally the usage of a DNS server for the dynamic import of the temporary IPv4 address into the DNS database. Thus, the implementation of the DSTM matches more to small and medium network sizes that already use a DHCP server for the sharing of global IPv4 addresses. The main limitation for the implementation of DSTM focuses on the non-availability of a DHCPv6 server, because the standardization process has not been completed yet.

2.2. Tunneling Mechanisms

The tunnelling mechanisms may be used for the IPv6 communication over the existing IPv4 infrastructure and vice-versa. They are based on the encapsulation of IPv6 packets into IPv4 packets and the transmission over the IPv4 network. The two endpoints of the tunnel need to be dual stack routers or hosts.

The tunneling mechanisms are mainly divided into two main categories according to the way they are created: either by direct configuration on the endpoints of the tunnel or by coding of the address of the endpoint into the IPv6 address.

The first category supports the following two (2) mechanisms:

Configured Tunneling Mechanism: The term "Configured Tunnel" refers to the explicit definition in each endpoint of the tunnel of the IPv4 address of the opposite endpoint. According to this mechanism the IPv6 packets are encapsulated into IPv4 packets. The destination address of the IPv4 packets has been indicated in the creation of the tunneling interface on the router, while the source address is the IPv4 address of the interface. By this way routers build point-to-point links over the IPv4 infrastructure and these links are used for the transmission of the IPv6 packets. The implementation cost of the Configured Tunneling Mechanism is low because it allows the parallel development of the IPv6 infrastructure without the usage of separate physical links.

Tunnel Broker Mechanism: Tunnel Broker is a mechanism designed for users that want to participate to the IPv6 network but they are isolated from any native IPv6 network or for users who wish an early IPv6 adoption (Durant, Fasano et al, 2001). It provides quick connectivity to the IPv6 network in addition to the low administration cost. The tunnel broker assigns an IPv6 address to the Dual Stack host, which returns along with its DNS name and client configuration information. The main components of this mechanism are the tunnel broker entity and the tunnel broker server. The tunnel broker entity is used for the registration of the user and the tunnel activation for the connection to the IPv6 network. The tunnel broker server is an IPv4/IPv6 router connected to both networks.

The tunnel broker mechanism is targeted to the connectivity to the IPv6 network of remote users and small sites. However, it offers high scalability and can support a large number of remote users. This mechanism presents a limitation for the support of users who use private IPv4 addresses (NAT mechanism). Also, it is aimed more at short-term periods of native IPv6 connectivity rather than providing long term access.

The second category supports the following three (3) mechanisms:

Automatic Tunneling Mechanism: This mechanism utilizes the IPv4 compatible IPv6 addresses (Gilligan and Nordmark, 2000). For the application of this mechanism it is required only the installation of a software module to the hosts. This module is a pseudo-interface, which is responsible for the encapsulation of IPv6 packets into IPv4 packets and their forwarding over the IPv4 interface. This mechanism requires globally routable IPv4 addresses and excludes private addresses.

Usually, this mechanism is used in combination with a configured tunnel, in order to make able the IPv6 host to communicate with the total of IPv6 hosts (native IPv6 hosts and hosts using the 6to4 mechanism) and not only with hosts using automatic tunneling. As the automatic tunneling mechanism allows to remote hosts to have access to the IPv6 network and operates with a simple and flexible way, this mechanism can be combined with other mechanisms in order to achieve an end-to-end communication.

6to4 Transition Mechanism: The 6to4 mechanism enables IPv6 sites to connect to other IPv6 sites over the IPv4 network (Carpenter and Moore, 2001), (Tsirtsis, 2000). It does not employ any tunneling mechanism neither the host needs to have an IPv4 compatible IPv6 address. The only requirement is the IPv6 router to have a routable IPv4 address. This mechanism uses the IPv4 infrastructure for the interconnection of remote IPv6 hosts. It faces the IPv4 network as a unicast point-to-point link layer and implements the IPv6 network using encapsulation techniques. 6to4 mechanism has been assigned the IPv6 prefix 2002/16.
The main aim of this mechanism is to allow isolated IPv6 sites/hosts, which are attached to an IPv4 network with no IPv6 support to communicate with other IPv6 domains. Another advantage is that the 6to4 mechanism may be used in networks that have private IPv4 addresses and only one routable address, while it is not affected by the presence of firewalls and NAT boxes. The 6to4 mechanism supports the progressive migration from IPv4 to 6to4 and later to native IPv6.

6over4 Mechanism: The 6over4 mechanism allows isolated IPv6 hosts to act like fully functional IPv6 hosts even without direct contact with an IPv6 router (Carpenter and Jung, 1999). This mechanism utilizes the IPv4 multicast domain, that is considered as the link layer over which the IPv6 stack is built. In this case, the IPv4 domain has to support multicast operations. Also, if connections with external IPv6 sites have to be supported, then it is required a router that applies the same mechanism to the link connected to the multicast domain. The 6over4 mechanism does not use IPv4 compatible IPv6 addresses or configured tunnels. Also it is provides independence on the technology of the used links and the topology of the IPv6 network. Usually the 6over4 mechanism is called as a "virtual Ethernet".

2.3. Translation Mechanisms

The translation mechanisms aim to allow the communication between hosts that support different protocols. They may be applied in networks where only one protocol is used, while it is desirable the support of services of the other protocol, for example support of IPv4 services in IPv6 hosts. The most well known translation mechanisms are described briefly in the following.

Header Conversion: According to this mechanism the IPv4 headers are translated to IPv6 headers and vice-versa. It is similar to the NAT protocol (IPv4-to-IPv4 Header Conversion). Although this mechanism is fast enough, it appears some limitations to its application, for example it does not support translation in the application layer.

NAT-PT (Network Address Translation –Protocol Translation): The NAT-PT mechanism allows to native IPv6 hosts and applications to communicate with IPv4 hosts and applications respectively. The host that makes the translation lies on the borders between the IPv4 and IPv6 networks. Each host acting as an address translator keeps a pool of addresses that are assigned dynamically to IPv6 hosts and a session is generated between two hosts supporting different protocols. The NAT-PT mechanism supports both address and header translation. The implementation of the NAT-PT mechanism is simple and does not require any extra configuration to the hosts. However, this mechanism does not support the implementation of end-to-end security strategies and requires the usage of a large IPv4 space.

Mechanism type	Implication on application	IPv4 address requirements	Hosts/Site mechanism	Comments
Dual stack	None	Permanent or Pool of addresses allocated by a DHCP server.	Site/Host	Very simple to set up, available to every node supporting IPv6 stack.
DSTM	None	Pool of addresses required for AIIH server.	Site/Host	Allows hosts to run end-to-end IPv4 application within an IPv6 only network. Allows IPv4/IPv6 of IPv6-only host application to communicate with either IPv4 or IPv6 end point without need of specific ALG.
6to4	Applications need to be ported to interface with the IPv6 stack.	IPv4 address of border routers.	Site/Host	Allows to automatically joining IPv6 network separated by an IPv4 only network. Each IPv6 network needs to have a 6to4 border router.
Tunnel Broker	Applications need to be ported to interface with the IPv6 stack.	One for the dual stack host. At least one for the tunnel broker implementation.	Site/Host	Allows an isolated IPv4 host within an IPv4 only network, to reach an IPv6 wide network.
6over4	Applications need to be ported to interface with the IPv6 stack.	One per host	Host	Allows to automatically joining IPv6 network separated by an IPv4 only network. The IPv4 network needs to support multicast. Each IPv6 network needs to have a 6over4-border router.
NAT-PT	Applications including IP addresses in the packet payload need the availability of a dedicated ALG into the NAT-PT router.	Pool of IPv4 addresses needed.	Site	Needs specific ALG for DNS, FTP, IPSEC, … Mechanism located in a single point.
SOCKS64		The Socks Server must have an IPv4 address	Site	Allows IPv4 applications to communicate with IPv6-only hosts and vice-versa.

Table 1: Overview of Transition Mechanisms

Address Mapping: This technique refers to one-to-one correspondence between IPv6 destination addresses and IPv4 source addresses and vice-versa.
Socks: Socks is a gateway mechanism implemented by a "Socks Server", that acts as a relay mechanism in TCP or UDP sessions between two hosts supporting different protocols (one IPv4 host and the other IPv6 host) (Toutain and Afifi, 2000). Socks is considered is a unidirectional mechanism and may be used for the connection of an IPv4 network to an IPv6 network and vice-versa. Its main disadvantage is that the connections have to be initialized by the hosts lying behind the Sock Server. Table 1 summarizes the transition mechanisms (EuresCom Project P1009 results, 2001).

3. Transition Scenarios applied on the Greek Research & Technology Network (GRNET)

GRNET is the Greek Research & Technology Network, providing Internet services to the Greek Academic and Research community. It interconnects Universities and Research Centers in Greece, as well as other R&D Departments of industrial organizations through an advanced high-speed network. Like many other NRNs, GRNET maintains a pilot IPv6 network in order to enable its users to familiarize with the new protocol. The IPv6 network was built over the IPv4 infrastructure so that the core IPv6 links are not actually native IPv6 links but IPv6 over IPv4 tunnels that interconnect the IPv6 routers of the participating organizations and the core IPv6 router of GRNET. The topology implemented is a star one. The figure 1 shows the topology of the IPv6 network of GRNET.

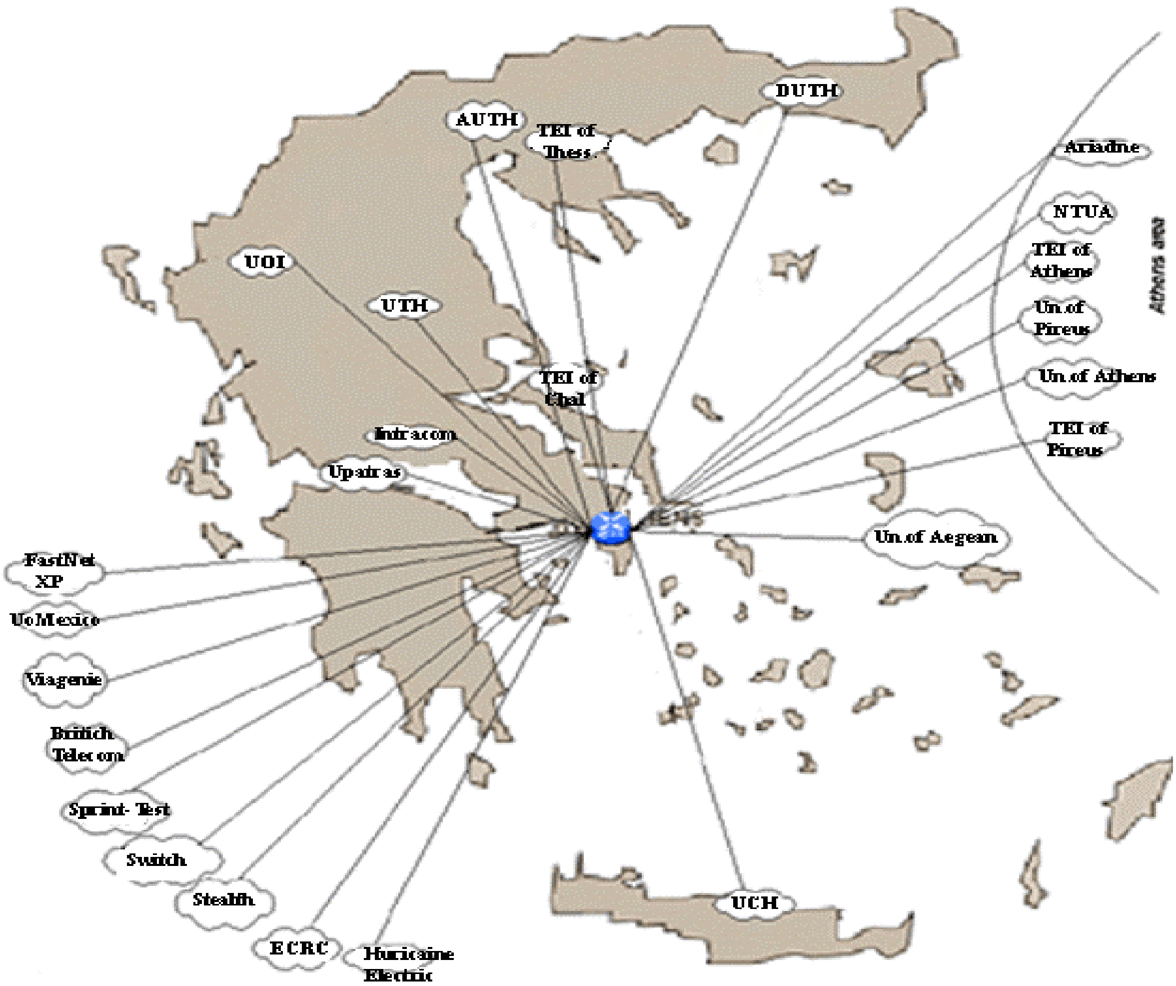

Figure 1: IPv6 Network Topology of GRNET

3.1. Address assignment

GRNET is the administrative authority of a SLA, the 3FFE:2D00::/24 that has been assigned to it by the RIPE for the needs that will come up during the deployment of the IPv6 protocol at the east Mediterranean area. Following the guidelines of RFC 2450 an address plan was designed so as to distribute the allocated address space to the possible clients (Universities, Technology and Research Institutes etc) (Hinden, 1998). The decision was to allocate 3 bits for sharing between the Mediterranean countries, the next 5 bits for the big ISPs in each country, leaving the total of 96 bits to be consumed by the customers. This leads to 8 countries, 32 big ISPs in each country and each ISP can support up to ~65000 clients. Since the last 64 bits comprise the host part, each client disposes 16 bits for the internal sub netting.

3.2. Motivation

The IPv6 backbone of GRNET comprises of an IPv6 router that is connected through IPv6 over IPv4 tunnels to each client and with 6bone too. Initially in each Academic Institute there was a small IPv6 LAN that was connected to the local IPv6 router. This small IPv6 LAN was the test best where the new protocol had been tested on and a knowledge base obtained by technicians so they could support the expanding procedure to the end user. The last one was the challenge that had to been taken: How the IPv6 network could reach to the end user? The main goal was to use the IPv6 backbone in a manner similar to the use of the IPv4 backbone, meaning that all IPv6 traffic from every Institute should cross the local IPv6 router. The reasons that enforced this policy were mainly administrative in terms of traffic measurement and accounting. So we focused on transition techniques that could provide this characteristic.
Although it is common accepted that the IPv6 will be the internetworking protocol of the next years and the users have to get familiar with it, there were certain reasons that kept us from enabling the protocol to the entire network and make it a full dual stack network and thus providing end to end communication with both protocols.
In the following we describe the techniques that were proposed to the Network Operation Centers of the Academic Institutes in order to provide IPv6 services to the end users.

3.3. The Tunnel Broker solution for GRNET

In order to provide IPv6 services to the end users without investing many resources or making changes to the network, one of the apparent solutions is the deployment of the tunnel broker.
Our approach is described in figure 2. We setup a server that implements the user interface and also has the permissions to change the routers configuration in order to setup the tunnels. The tunnel broker software checks the IPv4 address of every user, determines in which Institute he belongs to and setups a tunnel between the user and his local IPv6 router. If the Institute does not maintain an IPv6 router then the tunnel is established between the user and the backbone IPv6 router.

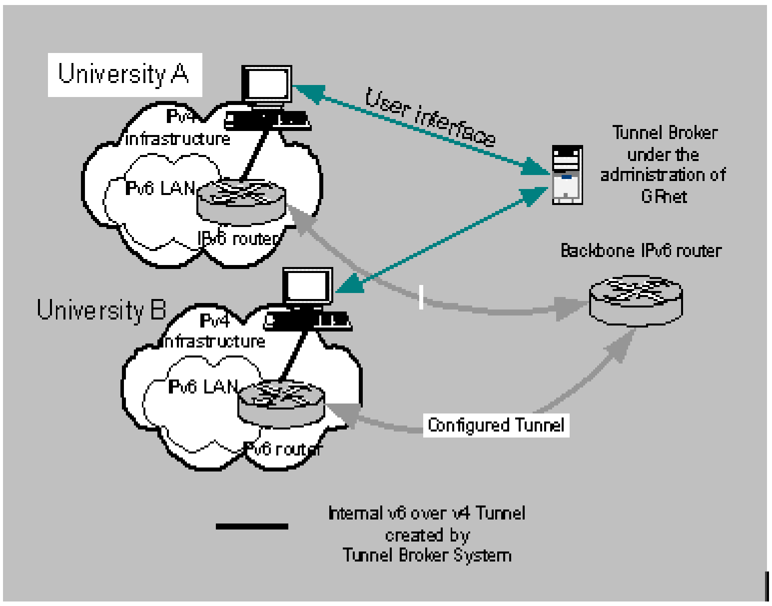

Figure 2: Tunnel Broker operation in GRNET

3.4. The configured tunnels solution for GRNET

The second solution in order to provide IPv6 connectivity to the end user was to deploy configured tunnels between specific routers and the local IPv6 router. Each University used the IPv6 space that had been assigned to it by GRNET. The topology that is implemented inside the campus networks is a mesh one meaning that there is a tunnel between each pair of routers participating to the IPv6 network. Each router with an IPv6 interface activated on it has been configured with a static route for all native IPv6 addresses pointing to the local IPv6 router, which is connected to the 6bone through the tunneling interface of the backbone IPv6 router.

4. Future work

Using the mechanisms described above GRNET could provide IPv6 connectivity to any end user at the participating institutes. However, the variation of network architectures, technologies and demands that exist in each academic institute enforces us to deploy a mixture of the described techniques. The main target is to select the appropriate technique for each institute in order to provide better IPv6 service and smoother transition procedure for the end user and the network administrators. Our future work includes the deployment of combination of 6to4, automatic tunneling and configured tunneling techniques inside campus networks and the use of translating techniques (e.g. NAT-PT) wherever IPv6-only clouds are created.

5. Conclusion

The transition to the next version of the IP protocol inside the GRNET is a long-term procedure that is considered to consume a lot of resources. The whole toolset of transition tools that have been defined and tested will provide the “middle step” in order to make the whole procedure smooth for the end users and the administrators. Currently, we are studying on more techniques in order to cover all the possible cases of implementation.

6. References

Carpenter, B. and Jung, C. (1999), *"Transmission of IPv6 over IPv4 Domains without Explicit Tunnels"*, RFC 2529.

Carpenter, B. and Moore, K. (2001), *"Connection of IPv6 Domains via IPv4 Clouds"*, RFC3056.

Crawford, M. and Huitema, C. (2000), *"DNS Extensions to Support IPv6 Address Aggregation and Renumbering"*, RFC 2874.

Deering, S. and Hinden, R, (1998), *"Internet Protocol Version 6 (IPv6) Specification"*, RFC 2460.

Durand, A. and Buclin, B. (1999), *"6Bone Backbone Routing Guidelines"*, RFC2546.

Durant, A. Fasano, P. Gardini, I. and Lento, D. (2001) *"IPv6 Tunnel Broker"*, RFC 3053.

EuresCom Project P1009 results (2001), *"Armstrong IPv6 deployment -A small step for IP but a giant leap for mankind"*.

EuresCom Project P1009 results, (2001), *"Transition Mechanisms Overview"*.

Gilligan, R. and Nordmark, E. (2000), *"Transition Mechanisms for IPv6 Hosts and Routers"*, RFC 2893.

Hinden, R. (1998), *"Proposed TLA and NLA Assignment Rules"* RFC 2450.

Kitamura, H. (2001), *"A SOCKS-based IPv6/IPv4 Gateway Mechanism"*, RFC 3089.

Toutain, L. and Afifi, H. (2000) *"Dynamic Tunnelling: A new method for the IPv4-IPv6 Transition"* draft-ietf-ngtrans-dti-00.txt.

Tsirtsis, G, and Srisuresh, P. (2000), *"Network Address Translation - Protocol Translation (NAT-PT)"*, RFC 2766.

Tsirtsis, G. (2000), *"Dual stack deployment using DSTM and 6to4"* draft-ietf-ngtrans-6to4-dstm-00.txt.