# Implementation of IPv6 Over IPv4 Using Dual Stack Transition Mechanism (DSTM) on 6iNet

**Data** · December 2014

CITATIONS
0

READS
862

**3 authors**, including:

Hatim Mohamad tahir
Universiti Utara Malaysia
**32** PUBLICATIONS **134** CITATIONS
SEE PROFILE

Azman Taa
Universiti Utara Malaysia
**35** PUBLICATIONS **112** CITATIONS
SEE PROFILE

# Implementation of IPv6 Over IPv4 Using Dual Stack Transition Mechanism (DSTM) on 6iNet

Hatim Mohamad Tahir, Azman Taa, Norshakinah Bt Md.Nasir
*Dept of Comp Sc, Faculty of Information Tech, Univ Utara Malaysia, 06010 Sintok, Kedah. MALAYSIA*
*hatim@uum.edu.my*

**Abstract -** *Moving from Internet Protocol version Four (IPv4) to Internet Protocol version six (IPv6) is not straightforward because IPv4 and IPv6 are incompatible protocols. To enable the smooth integration between IPv4 and IPv6, several transition mechanisms have been proposed by IETF IPng Transition Working Group (NGTrans). One of them is Dual Stack Transition Mechanism (DSTM). This paper reviews the implementation of DSTM over our IPv6 test-bed (6iNet) in University Utara Malaysia (UUM). This paper also describes our experience of configuring 6iNet. 6iNet is the first IPv6 test-bed in UUM and has become a platform for IPv6 research in UUM.*

*Keywords*: IPv4, IPv6, Transition Mechanism, and DSTM.

## 1. Introduction

The remarkable growth of today's Internet that based on the Internet Protocol version four (IPv4) has highlighted several fundamental limitations with that protocol. Due to the Internet rapid growth and the limitations in its design, there will be a point when no more free addresses are available for connecting to new hosts in the next few years. At that time, Internet will face a serious problem. IPv4 was defined in the 1970s when the structure of the protocol was sufficient for the existing networking infrastructure at that time. IPv4 is the first version of the Internet Protocol (IP) to be widely deployed, and forms the basis for most of the current Internet. The continuous success and growth of the global Internet requires that the overall Internet architecture evolve to accommodate new technologies that support increasing numbers of users, applications and services. The current IPv4 address space is unable to satisfy the potential huge increase in the number of users or the geographical needs of the Internet expansion such as the Internet-enabled personal digital assistants (PDAs), home area networks (HANs), Internet-connected transportations (such as automobiles), integrated IP telephony services, IP wireless services, and distributed gaming [1].

By 1990s, commercial users have discovered the Internet and commercial use, previously prohibited or constrained on the Internet, was actively encouraged. Nowadays, Internet technology has become the most important mechanism in the world of data communication. Since the beginning of this decade, new host system are being added to the Internet at rates of up to 10% per month, and the Internet has been doubling in size in every 10-12 months for several years [2]. By January 1997, the number of hosts on the Internet was over 16 million, ranging from PC-class systems to supercomputers, on more than 100,000 networks worldwide. The Figure 1 shows the trend of IPv4 address space usage [3]. The number of hosts and users increased dramatically and continually in 1993 with the release of Graphical User Interface (GUI) browsers for Hypertext Markup Language (HTML), World Wide Web (WWW) and e-mail [4]. This situation has made the number of the free addresses of IPv4 gets lower. IPv4 also cannot provide one address for each person on the earth where the number of population is about 6 billion. So, a new version of IP is designed to become the successor to IPv4 and to solve the problem of the limited address space in IPv4.

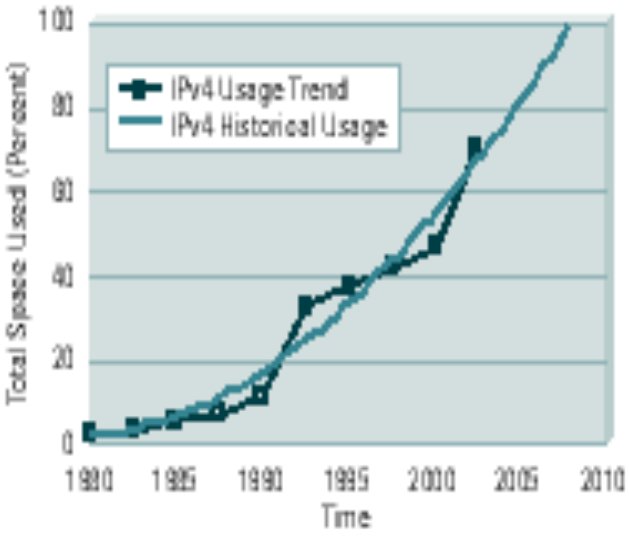


Figure 1:The Trend of IPv4 address space usage.

IPng is short for Internet Protocol next generation, a new version of IP reviewed in Internet Engineering Task Force (IEFT) standards committees to replace IPv4. The official name of IPng is Internet Protocol version six (IPv6). IPv6 is designed as an evolutionary upgrade to the IP and will be necessary, in fact, coexist with the older IPv4 for a long time and the interoperability between IPv4

and IPv6 nodes is an essential element. IPv6 is designed to allow the Internet to grow steadily, both in terms of the number of hosts connected and the total amount of data traffic transmitted. IPv6 offers quite a few enhancements and possibilities. IPv6 fulfills future demands on address space, and also addresses other features. The most important issue addressed by IPv6 is the need for increased IP addresses. IPv4, with its 32-bit address space is nearly exhausted, while the number of the Internet users continues to grow exponentially. IPv6 use 128-bit technology with $2^{128}$ theoretically addresses space provides an adequate number of globally unique addresses to support the anticipated growth and development of the Internet for the foreseeable future [5]. IPv6 supports a much greater number of addressable nodes. However, IPv6 is much more than provides more IP addresses. Others than the increased of the address space, IPv6 also offers a number of other improvements over IPv4 such as improved efficiency in routing and packet handling, support for autoconfiguration and plug and play, support for embedded IPSec, and enhanced support for mobile IP and mobile computing device.

IPv6 has been accurately designed, discussed thoroughly, and tested in the field by the IETF and by many other research institutions and organizations. A project call 6Bone was created so that users could acquire experience and test the IPv6 protocol stacks. 6Bone is an IPv6 testbed, is a spontaneous derivation of the IETF Internet Protocol next generation (IPng) working group to assist in the evolution and deployment of IPv6. The major goal of 6bone is to assist in the initial stages of IPv6 deployment. The 6bone can be used to test the interoperability of different emerging and develops a way to help in transition to IPv6. It also expected that 6bone operation practices would give the necessary feedback for building IPv6 networking experience.

This paper reviews the implementation of Dual Stack Transition Mechanism (DSTM), one of the transition mechanisms between IPv4 and IPv6 over our IPv6 testbed within a campus environment. This work has been conducted at the Faculty of Information Technology (FIT), University Utara Malaysia (UUM). This paper also describes our study and experience in the deployment of our IPv6 project. This project named as "Sintok IPv6 Network" or shortly, 6iNET (pronounced as "sinet"). 6iNET is the first IPv6 test-bed in UUM. The main objective of this project is to implements the first IPv6 test-bed in UUM. The designing and deployment of UUM IPv6 test-bed can be utilized to spearhead the implementation of operational IPv6 network in UUM in the future. By implementing the IPv6 test-bed, we attempt to identify and understand the problems exist in the test-bed such as the issue of the transition between IPv4 and IPv6 before any real implementation can take place. The output from this project can contribute in many aspects such as new IPv6 application testing, IPv6 performance analysis, mobile IPv6 and many more. It also gives us opportunity to test and understand the technology before any real implementation takes place.

## 2. Ipv6 test-bed configuration

Test-bed is a platform on which an assortment of experimental tools and products that may be deployed an allowed to interact in real-time. Successful tools and products may be identified and developed in an interface, evolutionary and interdependent process [6]. Test-bed also has been defined as an experimental proof of concept, technology, demonstration and pre-prototype.

An IPv6 test-bed is an example of a collaborative approach to implement future network protocols, IPv6, providing a practical interoperability test platform from which users will transition to native next-generation commercial network services. To implement the IPv6 test-bed, it will be necessary for us to understand the technical and functional aspects of IPv6. Implementing the IPv6 test-bed containing several of the existing independent implementations of IPv6 will enable us to work more closely with the vendor and other organizations developing IPv6 [7]. Many tasks have to be conducted to ensure that the test-bed is functionally and operationally correctly.

This subsection contains a description of our study and experience in the deployment of the first IPv6 test-bed in UUM called 6iNet. This test-bed has being set-up at FIT, UUM in order to assess, test and demonstrate the use of IPv6 network. This test-bed is a part of our research and will become the foundation for all of the IPv6 tasks that has been defined in this research such as the implementation of transition mechanism between IPv4 and IPv6. Throughout this work, we attempt to understand the technology and identify the problems exist in the test-bed before any real implementation can take place. The finding from the this research can contribute in many aspects such as we have been able to discover the basic of IPv6 technology, new IPv6 application testing, IPv6 performance analysis, mobile IPv6 and many more. This effort also allows us to develop an expertise in IPv6 technology and become technically competent with IPv6 technology in the academic environment.

### 2.1 6iNet infrastructure and configuration

The configuration of our test-bed consists of a Personal Computer (PC) based router that has been loaded with FreeBSD5.1 as an operating system, a pair of media converter (fiber to utp), several switches (P333, P550, and P880) and several hosts that were situated in Research Lab in FIT. These hosts were connected directly to the IPv6 router at Computer Center. This router is an experimental test-bed for IPv6 under UUM IPv6 Taskforce. It's an effort from collaboration between Malaysia Advanced

Network Integrated System (MANIS) and UUM. The hosts that we used were loaded with Windows XP and Linux Redhat 9 as an operating system. The location of 6iNet deployment is at the FIT, UUM. In UUM network, each faculty has their own LAN. 6iNet was built within the FIT's LAN. External connectivity to the UUM backbone is through FIT's 100Mbps Ethernet LAN. 6iNet uses software router. The router is located at the UUM Computer Center. The router uses two network interface card to receive and forward IPv4 and IPv6 datagram.

MANIS provide 2Mbps bandwidth access to 6iNet. From Computer Center to FIT LAN, we use Gigabit Ethernet technology using fiber optic, while in FIT LAN use twisted pair as media transmission with 100Mbps transmission rate. The 6iNet configuration and architecture depicted in Figure 2. For 6iNet we implement manually configured tunnel. We choose manually configured tunnel because it is more stable and secure connections for regular communication between two-edge routers, or between end-systems. From Computer Center, we established the tunnel to DNS server in MANIS. The tunnel from MANIS was established on March 2004 to UUM. When we establish the tunnel, MANIS provide the addresses to 6iNet. When host plug in the network, automatically it will get their own address. Tunnelling does not allow Network Address Translation (NAT); due to this issue, we have used 2 converters. The first converter is installed in Computer Center while another one is installed at the FIT.

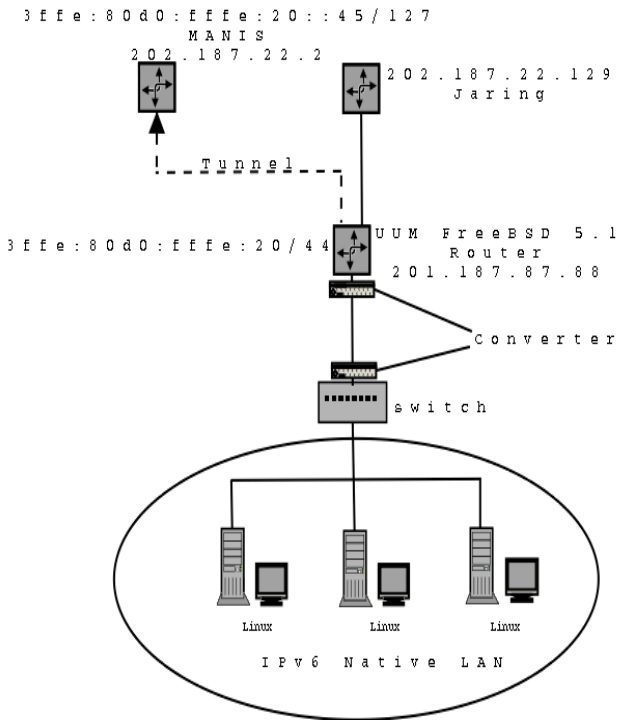


Figure 2. 6iNet Design

## 2.2 Setting up native IPv6 router

In order to provide IPv6 connectivity to the end user, we have deployed configured tunnels between PC router in UUM and the router in Jaring (MANIS). There are 3 steps to build tunnel for 6iNet project like follows:

- Step 1 - Installing the router operating system

The first step is to install FreeBSD 5.1 into the computer. Pentium II or Pentium III based system with 64 MB of memory is enough to set up the router. The most important part for the router is the needs of two network interface cards to receive and forward packets. The options for installation should keep to the minimum selection. No need to install GUI part.

- Step 2 - Configurations

There are three configuration files need to be configured and create. The first file is /etc/rc.conf. The second file is a script file. A “tunnel” script file is created in /etc directory. Lastly the third file is resolve.conf. The name server configuration file located at /etc directory.

- Step 3 - Running the script

After the script has been running successfully, the tunnel is completed.

Further information and details explanation about 6iNet such as the test-bed design, the technical aspect on configuring PC based router and deploying configured tunnels to setting up an IPv6 test-bed can be found at our website at www.uum.edu.my/6inet.

# 3. Transitioning From IPv4 to IPv6

The initial design of the Internet did not anticipate IP's huge deployment which had made it necessary to conceive a new IP, version 6, the successor to the long serving version 4, to correct some of its shortcomings. Therefore, it is an evolution rather than a revolution [8]. The transition process between today's IPv4 Internet and the future IPv6-based one will be a long process during which both protocol versions will coexist and operational side by side. Moving from IPv4 to IPv6 is not straightforward because IPv4 and IPv6 are two incompatible protocols. A guideline to simplify transition mechanisms between IPv4 and IPv6 has to be standardized. The IPv6 transition mechanisms are a set of protocol mechanisms implemented in hosts and routers, along with some operational guidelines for addressing and deployment, designed to make transition from Internet to IPv6 work with as little disruption as possible [9].

Even though IPv6 was designed more as an evolution and improvement from IPv4, nevertheless IPv4 and IPv6 are completely two separate protocols. IPv6 is not backwards compatible with IPv4, and IPv4 hosts and routers will not be able to deal directly with IPv6 traffic and vice

versa. Mechanisms to enable coexistence of IPv4 and IPv6 and transition between the two versions have to be standardized because there will be no single "flag day" on which the all-IPv4 network turns into an all-IPv6 network. It is impossible to switch the entire Internet over to IPv6 overnight.

The fundamental key to the successful market adoption of any new technology suite is depends on its easy of integration, smoothness, and compatibility with an existing technology without significant interfere of services. IPv6 provides many benefits over IPv4 technology. However, like mentioned above, all agree that any successful strategy for IPv6 deployment requires it to coexist with IPv4 for some extended period of time. It is because millions of IPv4 nodes already exist, upgrading every node to IPv6 at the same time is not feasible. As a result, transition from IPv4 to IPv6 happens gradually, allowing nodes to be upgraded independently and without disruption to other nodes. While a gradual upgrade occurs, compatibility between IPv6 and IPv4 nodes becomes a requirement. Otherwise, an IPv6 node would not be able to communicate with an IPv4 node.

Actually, the transition from IPv4 to IPv6 has already started even though most Internet and TCP/IP users have not yet seen new software neither on their local systems nor local networks [2]. The transition between today's IPv4 Internet and a future IPv6-based one will be a long process during which both protocol versions will coexist. Therefore, for a long period of time we are going to be dealing with a network in which the two protocols will be operating side by side. This is why a lot of attention was paid to the IPv4 to IPv6 transition mechanisms. A number of strategies have been proposed and developed for managing the complex transition process from IPv4 to IPv6. The following subsection describes several of these strategies or mechanisms.

## 3.1 Transition mechanisms.

IPv6 is designed as an evolutionary upgrade to the IPv4 and will, in fact, coexist with the older version for some time [10]. The integration and coexistence of IPv4 and IPv6 need to be well defined and planned. To make the transition to IPv6 easier, the Internet Engineering Task Force (IETF) has set up a work group called Next Generation Transition or shortly NGTrans, which their task is to specify mechanisms for supporting interoperability between IPv4 and IPv6. This has been the focus of the IETF NGTrans for several years. NGTrans has identified the transition mechanisms and issued several specifications that describe the transition mechanisms for IPv6 hosts and routers. These mechanisms are heavily used for the transition from the traditional IPv4-based Internet to an IPv6-based Internet. The transition mechanisms generally come in one of three following forms:

### 3.1.1 IPv6/IPv4 Dual Stack Approach

The first technique and the most straightforward way to introduce IPv6-capable nodes is a dual stack approach, where this technique requires hosts and routers to implement both IPv4 and IPv6 protocols. In this technique a network node installs both IPv4 and IPv6 stacks in parallel. This enables networks to support both IPv4 and IPv6 services and applications during the transition period in which IPv6 services emerge and IPv6 applications become available. When communicating with IPv6 nodes, they use IPv6 and when communicating with IPv4 nodes, they revert to IPv4. These nodes are called IPv4 compatible IPv6 addresses, these are addresses where the first 96 bits of the address are zeroes and the last 32 bits forms a valid IPv4 address [11]. Dual-stack is needed when an IPv6 network want to communicate with a native IPv4 hosts and applications. The hosts and applications in native IPv6 can communicate with the hosts and application that used the same protocol.

This technique allows IPv4 and IPv6 application to coexist in a dual IP layer routing backbone. All routers or a portion of them in the network need to be upgraded to be dual stack with IPv4 communication using the IPv4 protocol stack and IPv6 communication using the IPv6 stack. In dual stack approach, IPv6 datagram can be copied into the data field of the IPv4 datagram and appropriate address mapping can be done [12]. But when the IPv6 datagram mapped into IPv4 datagram, some fields in IPv6 have no counterpart in IPv4. The information in these fields will be lost. When it travel through network and arrive in IPv6 host, the datagram do not contain all the fields that were in the original IPv6 datagram sent from source. Dual-stack is needed when an IPv6 network want to communicate with a native IPv4 hosts and applications. The hosts and applications in native IPv6 just can communicate with the hosts and application that using the same protocol.

### 3.1.2. Tunnelling

An alternative to the dual-stack approach is known as tunneling, also discussed in RFC 2893 and can be used to overcome the drawback in dual-stack approach. IPv6 tunneling is a technique for establishing a "virtual link" between two IPv6 nodes for transmitting data packets as payloads of IPv6 packets. Different from dual-stack approach, tunneling encapsulates entire IPv6 datagram and puts in the data field of an IPv4 datagram. The IPv4 packet will travel inside the IPv4 network and upon arrival at the IPv6 network the destination node is located in the IPv4 header will be discarded and the encapsulated IPv6 packet will be forwarded to its destination [13].

Generally, there have been IPv6 manually configured tunnel and automatic configured tunnel. One of the characteristic of manual configured tunnel is it provide stable and secure connections for regular communi-

cation between two edge routers or between an end system and an edge router, or for connection to remote IPv6 networks such as the 6BONE. Manual configured tunnels are used between two points and require configuration of both the source and destination addresses of the tunnel. Each tunnel is independently managed. The more tunnel end-point we have, the more tunnel do we need, and the greater cost of management overhead [13]. NAT is not allowed along the path of the tunnel [Cisco System (2002)], while automatic tunnelling constructs tunnels with remote nodes on the fly. It can be set up and taken down as required. Both tunnels have their own advantages and disadvantages.

### 3.2. Translation Mechanism

The last technique in [15] uses a translation mechanism. Translation is necessary when an IPv6 only host has to communicate with an IPv4 host. At least, the IP header has to be translated but the translation will be more complex if the application processes IP addresses. In fact such translation inherits most of the problems of IPv4 Network Address Translators (NAT). ALGs (Application-Level Gateways) are required to translate embedded IP addresses, recomputed checksums example SIIT (Stateless IP/ICMP Translation) and NAT-PT (Network Address Translation Protocol Translation) are the associated translation techniques. A blend of translation and the dual stack model, known as DSTM (Dual Stack Transition Mechanism) have been defined to allow for the case where insufficient IPv4 addresses are available. Like tunneling techniques, translation can be implemented in border routers and hosts.

## 4. Dual Stack Transition Mechanism (DSTM)-An Overview

Dual Stack Transition Mechanism or shortly called DSTM is one of the IPv4 to IPv6 transition mechanisms that based on the use of IPv4-over-IPv6 tunnels. DSTM to carry IPv4 traffic within an IPv6 dominant and provides a method to allocate a temporary IPv4 address to Dual IP layer IPv6/IPv4 capable nodes [16]. DSTM is also the way to avoid the use of Network Address Translator (NAT) for early adopter IPv6 deployment to communicate with IPv4 legacy nodes and applications.

Actually, there is no specific solution to the IPv4 to IPv6 transition problem. Different mechanisms have been proposed but each one of the mechanisms only concerning with the one particular situation or scenario in the transition process. DSTM is intended for situation where IPv6-only networks in which hosts still need to exchange information with other IPv4 hosts or applications [17]. DSTM is a transition mechanism that uses existing protocols and does not specify a protocol. However, DSTM defines client, server, and border router behavior and the properties of the temporary addresses allocation mechanisms.

DSTM is targeted to help the interoperation of IPv6 newly deployed networks with existing IPv4 networks. The user may wants to begin IPv6 adoption with an IPv6 dominant network plan, or later in the transition of IPv6 when IPv6 dominant networks will be more prevalent. When DSTM is deployed in a network, an IPv4 address can be allocated to a Dual IP Layer IPv6/IPv4 capable node to connect with IPv4 only capable nodes. DSTM permits dual IPv6/IPv4 nodes to communicate with IPv4 only nodes and applications. Without modification to any IPv4 only node or application, or the IPv4 only application on the DSTM node. This allocation mechanism is coupled with the ability to perform IPv4-over-IPv6 tunneling of IPv4 packets inside the IPv6 dominant network [16].

Details explanation about DSTM can be found in Dual Stack Transition Mechanism Internet Draft [16]. DSTM offer five advantages and benefits over its uses as follows [17]:

- Dual-stack hosts on IPv6-only networks can reach IPv4-only nodes on the Global Internet.
- Legacy IPv4-only applications can be run over IPv6-only networks.
- Network is configured for IPv6 only.
- The need of global IPv4 addresses is reduced.
- Any type of protocol/application can be transparently forwarded.

### 4.1. Implementation of DSTM over 6iNet

In this work, we have conducted an implementation of DSTM over our IPv6 test-bed, 6iNet, in order to make our test-bed can reach IPv4-only nodes on the global Internet. At this moment, 6iNet can only run IPv6 Native LAN. Although we have deployed an IPv6 test-bed and works in the IPv6 networks environment, but we still need to works and communicates with the traditional IPv4-based Internet. So, we have decided to use DSTM as the transition mechanism over 6iNet because of it's main advantage, dual-stack hosts on IPv6-only networks can reach IPv4-only nodes on global Internet. It is because DSTM is intended for IPv6-only networks in which hosts still need to exchange information with other IPv4 hosts or applications [17]. DSTM is based on the used of IPv4 over IPv6 tunnels to carry IPv4 traffic within an IPv6 dominant and provides a method to allocate a temporary IPv4 address to Dual IP layer IPv6/IPv4 capable nodes. As mentioned before, for 6iNet we implement manually configured tunnel. We choose manually configured tunnel because it is more stable and secure for regular communi-

cation between two-edge routers, or between end-systems. Through the implementation of DSTM over 6iNET, our test-bed that based on IPv6-only networks will able to exchange information with other IPv4 hosts or applications. We also get the benefits from many other advantages that offer by DSTM such as easy to download and configure. These advantages can facilitate our works especially in the transition between IPv4 and IPv6. Figure 3 shows our design of the implementation of DTSM over 6iNet.

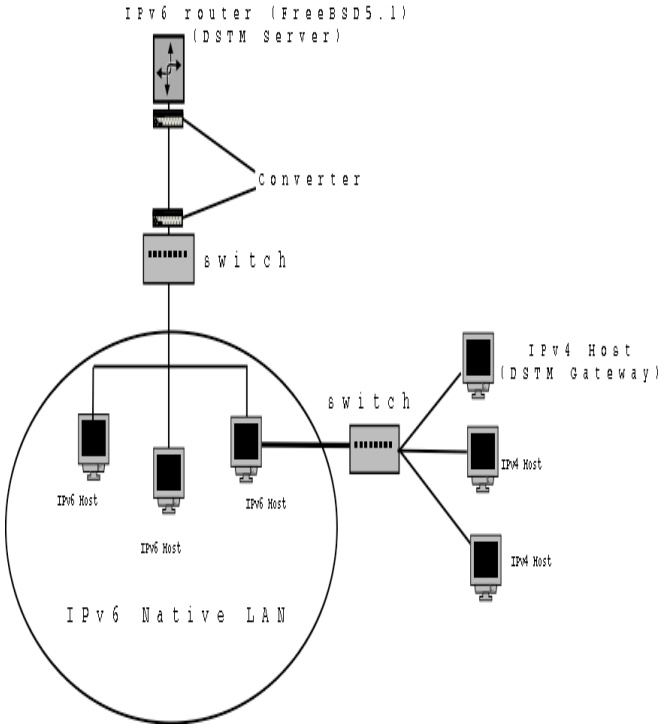


Figure 3. DSTM Implementation over 6iNet.

### 4.2. How DSTM works?

The DSTM architecture is consist of three (3) parts. They are the client (using FreeBSD and Linux as an operating system), the server and the DSTM gateway or called tunnel end-point router (TEP). The client is the machine that consist the code to put on an IPv6-only dual stack node to allow connections to the IPv4 world. The server machine also consist the code to relay between clients and the IPv4 world and it runs on a node connected to the both IPv4 and IPv6 providers. Lastly the gateway or TEP, is the machine that in charge of encapsulation and decapsulation of IPv4 over IPv6 packets. Only the gateway requires having direct IPv4 connectivity and a permanent IPv4 address. The server and gateway are often implemented on the same physical machine where the TEP is integrated in the server code. An external TEP also can be used, for example a 6Wind router with DSTM code [18]. If an external TEP will be used, the TEP will manage directly the tunnels with no interaction with the server, which only distribute leases.

Figure 4 shows a brief idea explains on how DTSM works and this explanation was refers to Dual Stack Transition Mechanisms Installation Guide by ENST Bretagne, Rennes [17]. As shown in that figure, we can identify 3 different types of equipments. First type is A where A is a Dual-stack host in an IPv6-only network that wishing to communicate using IPv4. B is a DSTM server who administrates the IPv4 address pool and lastly C where C is a DSTM gateway or TEP in charge of encapsulation and de-capsulation of IPv4 over IPv6 packets. Like mentioned above, only C (gateway or TEP) needs to have direct IPv4 connectivity and permanent IPv4 address.

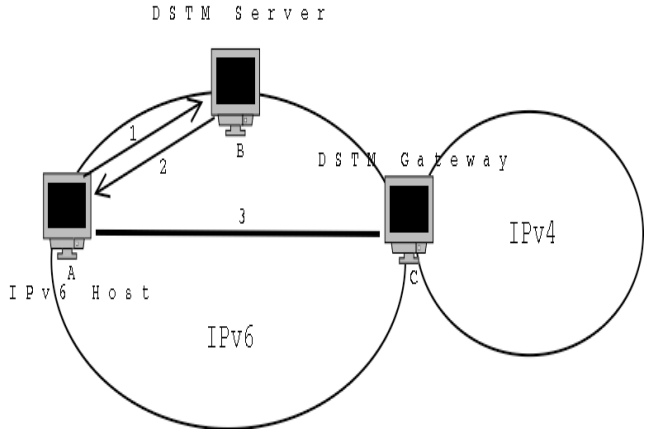


Figure 4: DSTM architecture

When A (IPv6-only host) in the IPv6 only domain needs to communicate in IPv4, the first step (labeling as 1 in the Figure 4) consists in asking the DSTM server, it's B, for a temporal IPv4 addresses. At that point, the B reserves one IPv4 address for A from the address pool and sends it on its replay. The replay message (labeling as 2 in Figure 4) also contains the validity time of the allocated address and the information concerning the DSTM gateway, the TEP. Following this message exchange (which can be done using DHCPv6, RPC or a proprietary format), station A configures its IPv4 stack with the allocated address. From that point on (labeling as 3 in Figure 4), all IPv4 packets coming from A, are tunneled (IPv4 over IPv6) to the C to perform the encapsulation and decapsulation of IPv4 packets. The C keeps a mapping table containing of the IPv4 and IPv6 address of Intranet hosts. In order to assure bi-directional communication IPv4 routing must assure that any packet intended for A passes through C.

## 5. Conclusion.

After a long period of testing, IPv6 is finally becoming accepted by the Internet world. It is obvious to say that two decades younger protocol is bringing enhancements into modern IP network through its new features and benefits. But, moving directly from IPv4 to IPv6 is not a practical way because IPv4 and IPv6 are two completely separate protocols, even though IPv6 was designed more as an evolution and improvement from IPv4. Transition mechanisms to enable the coexistence of IPv4 and IPv6 have to be standardized. The integration and coexistence of IPv4 and IPv6 need to be well defined and planned and this has been the focus of the IETF NGtrans for several years. NGtrans has identified the transition mechanisms and issued several specifications that describe the transition mechanisms for IPv6 hosts and routers. These mechanisms are heavily used for the transition from the traditional IPv4-based Internet to an IPv6-based Internet.

Nowadays, lots of works and researches have been done on IPv6 and its related issues, and there is still a long way to go. To experiments and understand the role which IPv6 will play in the future, it is necessary for us to develop hands on experience with the IPv6 technology. Through our effort in creating an IPv6 test-bed in UUM have allow us to develop this expertise and become technically competent with IPv6 technology in an academic environment. The effort to build this test-bed can increase our knowledge towards the IPv4 to IPv6 transition and migration. We have also been able to discover the basic of IPv6 technology and generate many researches such as the implementation of transition mechanisms, new IPv6 application testing, IPv6 performance analysis, mobile IPv6 and many more. It also gave us the opportunity to test and understand the IPv6 technology before any real implementation time comes. The finding of this research could be applied to other organizational setting which intends implement IPv6 in their network interconnection.

**Acknowledgements**

We like to extend our gratitude to Universiti Utara Malaysia for giving us the funding and opportunity to conduct this research.

## 6. References

[1] Cisco System, The ABCs of IP version 6, *Technical Report*. Cisco IOS Learning Services, Cisco System. Available at http://www.cisco.com/warp/public/732/abc/docs/abcIPv6.pdf, 2002.

[2] Kessler, G.C., IPv6: The next generation Internet protocol. *Handbook on Local Area Networks,* Auerbach, 1997.

[3] Cisco System, *IPv6 At a Glance*. Courtesy of Cisco Enterprise Marketing, Cisco System, Inc. 2004.

[4] Awad-Murshed, G.A. and Komosny, D., *Comparison of IPv4 and IPv6*, Brno University of Technology, Brno, Czech Republic, 2004.

[5] Ixiacom, Internet protocol version 6 (IPv6) conformance and performance testing, *White papers and guide*, Ixiacom, 2004.

[6] Tom, H., DLI UIUC glossary. *Technical Report*, University of Illinois, Urbana-Champaign. 1998.

[7] Glenn, R., Wack, J. and Fang, H., Project: IPv6 technology, *Technical Report.* National Institute of Standards and Technology (NIST), 1996.

[8] 6WIND, Why IPv6? *6WIND Homepage*. Available at http://www.6wind.com/frame.php, 2003.

[9] Gilligan, R., and Nordmark, E., Transition mechanisms for IPv6 hosts and routers, *Request for Comment 1933 (RFC1933),* Sun Microsystems, Inc. 1996.

[10] Interoperability, Interoperability between IPv6 and IPv4, *Internet Article*. Available at http://ntrg.cs.tcd.ie/undergrad/4ba2.02/IPv6/interop.html, 2004.

[11] Kurose, J.F. and Ross, K.W., Computer Network: A top-down approach featuring the Internet, Addison Wesley, United State of America, 2nd ed., 2002.

[12] Tian, J. and Li, Z., The next generation Internet protocol and its test. *IEEE Communication Magazine*, 210-215, 2001.

[13] Childress, B., Chathey. B. and Dixon, S., The adoption of IPv6, *Journal of Computing Sciences in Colleges.,* 153-158, 2003.

[14] Carmes, E., The transition to IPv6, *Internet Article*. The Internet Society, Virginia, USA. Available at www.isoc.org/briefings/006/isocbriefing06.pdf, 2002.

[15] Bound, J., Dual Stack Transition Mechanism. Internet Draft. Hewlett Packard. Available at http://www.IPv6.rennes.enst-bretagne.fr/dstm/draft-bound-dstm-exp-01.txt, 2004.

[16] ENST-Bretagne, Dual Stack Transition Mechanism (DSTM), DSTM Homepage, Ecole Nationale Superieure des Telecommunications de Bretagne, Rennes, France. Available at http://www.IPv6.rennes.enst-bretagne.fr/dstm/, 2003a.

[17] Raicu, I., An empirical analysis of Internet Protocol version 6 (IPv6), *Master Thesis*, Wayne State University, 2002.

[18] ENST-Bretagne, DSTM V2.0Beta for FreeBSD and Linux, Ecole Nationale Superieure des Telecommunications de Bretagne, France. 2003b.

.