CONCEPTION ON TRANSITION METHODS: DEPLOYING NETWORKS FROM IPV4 TO IPV6

[1] MS. CHAITA JANI, [2] PROF.MEGHA MEHTA

[1]M.E.[C.E] Student, Department Of Computer Engineering, Noble Group Of Institutions, Junagadh ,Gujarat
[2] Asst.Professor And Head, Department Of E & C Engineering, Noble Group Of Institutions, Junagadh ,Gujarat

Jani.chaita@gmail,com, meghamehtaec85@gmail.com

ABSTRACT: *The IPv6 protocol was created with the main purpose of solving the problem of the depletion of IP addresses that IPv4 is currently facing. This thesis gives an introduction to the differences between IPv4 and IPv6 and when one should use one protocol rather than the other. It describes the services that we will use in order to evaluate what kinds of problems IPv4 may experience and if these problems can be solved by using IPv6. We also show how to set up a network with both protocols for each service that we examine. We will subsequently evaluate the performance of these two protocols for each of these services. We found that there were no significant differences in the performance of any of the applications that we tested with both IPv4 and IPv6. Here the transition methods are Dual stack, tunnelling, translation.*

Keywords—Dual Stack, Tunneling, IPv4 , IPv6, Translation, Tunnel Broker .

I: INTRODUCTION

The Internet has grown to be a significant part of everyday life everywhere in the world. Most people have more than one device that uses IP-addresses. In the IPv4 address-space that is now almost completely used, there are 4,294,967,296 possible addresses; from which private addresses account for 17,891,328 and the rest are public addresses. Therefore it seems that IPv4 will not be able to satisfy the need for addresses. The situation now (18.10.2010) with unallocated IPv4 addresses according to IANA is that there is only 5% (that is 214,748,364 addresses) of the total address space available. Sounds like a large number, but with the current rate of usage there will be only 1% of unused addresses left in 2011. The last 5%, from 10% to 5% was used in 9 months.

Besides, according to its nature in the structure of Internet, the TCP/IP has also played an important role in the global expansion of communications. As a result, the more users join the Internet, the better it would be to spread knowledge in every field around the world. However, this is also the problem as the IP address is not unlimited and the Internet community is witnessing the exhaust of IPv4 not year by year but day by day, which calls for a proper solution. The first group of Internet users that would be affected is internet service providers (ISPs), large enterprises, companies, etc. The reason is that they hold the most number of IPv4 for operation and management and before the IPv4 runs out, they will need an appropriate act to handle the exhaustion, and otherwise, the collapse of the worldwide Internet is foreseeable . In general, we can classify various transition techniques into three categories with respect to connectivity and necessary elements for the implementation

II: IPV6 COMPARED TO IPV4

Address space

The most obvious difference between IPv4 and IPv6 is the size of the addresses. In the IPv4 protocol addresses are 32 bits long. This leads to a theoretical limit of 232 = 4,294,967,296 addresses. In the IPv6 protocol the addresses is 128 bit long. This makes the total number of possible addresses to 2128 ~3.4 * 1038 addresses.

Address notation

There are some differences in the notation between IPv4 and IPv6 addresses. IPv4 is represented in a dot-decimal notation where every byte in the address is represented by a decimal number. These numbers are demarcated with dots. In IPv6 two bytes are represented as a four digit hexadecimal number separated with colons.

Source and destination

The source and destination IP address fields simply indicate the source and destination addresses of the packet. The fields are 128 bits for IPv6. One difference from IPv4 is that in IPv6 the address in the destination field might not be the final destination if a Routing header extension header is used.

Extension headers

Instead of carrying options inside the header, IPv6 exploits extension headers that are placed between the IPv6 header and the next protocol header. If there is more than one extension header, then RFC 2460 states that the following order should be used:

1. IPv6 header

2. Hop-by-Hop Options header
3. Destination Options header (if the options are to be processed by the first router and
succeeding)
4. Routing header
5. Fragment header
6. Authentication header
7. Encapsulating Security Payload header
8. Destination Options header (if the options are only to be processed by the final destination)
9. upper layer header

III: TRANSITION METHODS

The transition from IPv4 to IPv6 is not a one-day step and involves a lot of changes in network structures with the use of IP addresses. For the future success of IPv6, the next step in deploying IPv6 is to vote for the most suitable transition methods and their management. Although many kinds of transition mechanisms have been invented to help with the process, the implementation of IPv6 is never said to be easy and simple, even for experienced administrators. As a result, the most difficult problem to make decisions for is which method will be chosen for the implementation process to achieve a smooth and seamless transition. In general, we can classify various transition techniques into three categories with respect to connectivity and necessary elements for the implementation.

Since there is such a large difference between IPv4 and IPv6, they cannot communicate directly with each other. A system that is capable of handling IPv6 traffic can be made backward compatible, but an already deployed system that handles only IPv4 is not able to handle IPv6 datagram. This means that a major upgrade process would need to take place, involving hundreds of millions of machines, in order to make a complete transition to IPv6. This is way too expensive and time consuming and in any case will not happen overnight. The network world will most likely see a gradual transition to IPv6, where IPv6 will be integrated into the IPv4 world that exists today.

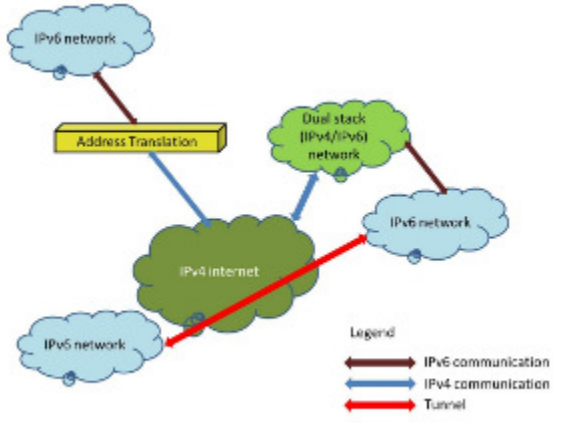

Fig.1. Different transition technologies

According to the above picture, there are different kinds of technologies which can be applied such as dual stack, tunneling mechanisms, and translation techniques. Over sixteen transition techniques have been used and tested for the communications between different networks to ensure IPv4 and IPv6 interoperability.

Therefore, to make decision on the best suited transition methods, it is really important to have an overview of the current IPv4 networks. In addition, enterprises must analyze needed functionalities, scalability, and securities in the corporation. Besides, "one size does not fit all" and a network can be applied different transition mechanisms together to support a complete distributed system. In general we catagorised Transition By three approaches dual stack, tunneling, translation.

IV: DUAL STACK

Dual-stack, or dual IP layer, requires that a node implement both IPv4 and IPv6. The node and therefore communicate with IPv4 nodes as well as IPv6 nodes. The node has full support for both protocols and has the ability to turn one of the stacks off, thus making it into an IPv4- or IPv6-only node. In order to be configured with addresses, the node uses static or DHCP configuration for IPv4 and static or auto configuration and/or DHCP for IPv6. A so called IPv6/IPv4 node will have at least one address for each version of IP.

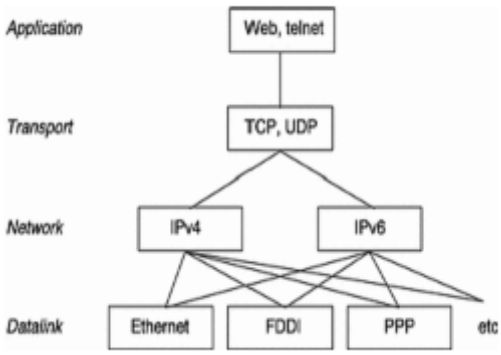

Fig 2 .structure of dual stack

As presented in Figure, the dual stack method is implemented in the network layer for both IPv4 and IPv6. Before transferring the packet to the next layer, the network layer will choose which one to use based on the information from the data link layer. Large enterprise networks that are decided to transit to IPv6 can apply the dual stack method as the basic strategy, which involves the device configuration to be able to utilize IPv4 and IPv6 at the same time on the core routers, perimeter routers, firewalls, server-farm routers, and desktop access routers.

The dual stack method is literally to use two IPv4 and IPv6 stacks for operating simultaneously, which enables devices to run on either protocol, according to available services, network availability, and

administrative policies. This can be achieved in both end systems and network devices. As a result, IPv4 enabled programs use IPv4 stack and this goes the same for IPv6. The IP header version field would play an important role in receiving and sending packets. In other words, this kind of IPv6 transition is the encapsulation of IPv6 within IPv4. The complete transition can be managed by DNS.

V: TUNNELLING

Tunneling IPv6 traffic over an IPv4 network is another possibility. This approach allows the IPv6 traffic to be encapsulated in an IPv4 packet and forwarded, creating an IPv6 tunnel over the IPv4 infrastructure. A scenario where that would be useful would be if you as an IPv6 network user want to reach another IPv6 network, but have to traverse an IPv4-only network. A tunnel can be created as a solution for transporting your IPv6 traffic, from your IPv6 node to the destination IPv6 node, over the IPv4-only network. A "virtual link" is created and, from the perspective of the two establishing IPv6 nodes, this appears as a point-to-point link. The different types of tunneling techniques can be categorized into two types: manually configured and automatic tunneling. A point-to-point link has to be manually configured, as the name suggests .For automatic tunneling, an IPv6 node can dynamically tunnel packets by using a 6to4 address.

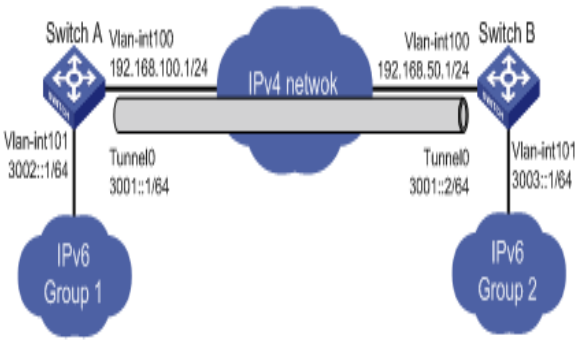

Fig 3. Tunneling transition method

This is used to transfer data between compatible networking nodes over incompatible networks. There are two ordinary scenarios to apply tunneling: the allowance of end systems to apply offlink transition devices in a distributed network and the act of enabling edge devices in networks to inter-connect over incompatible networks. Technically speaking, the tunneling technique utilizes a protocol whose function is to encapsulate the payload between two nodes or end systems. This encapsulation is carried out at the tunnel entrance and the payload will be de-capsulated at the tunnel exit. This process is known as the definition of tunnel. Therefore, the main issue in deploying tunnel is to configure tunnel endpoints, determine positions for applying encapsulation.There are different types of tunnelling available automatic and manual tunnelling.

6to4 Automatic Tunneling

One problem is that ISPs do not deploy IPv6 unless there is a great demand for it from their customers; however, the customers do not demand it since their applications work well on the current infrastructure (IPv4 with NATs)[55]. The current infrastructure is what the developers of applications adapt to since ISPs have not deployed IPv6. Fortunately, 6to4 is a technique that meets (most of) the IPv6 user's requirements, while meeting the ISP's requirements in terms of costs and administration.

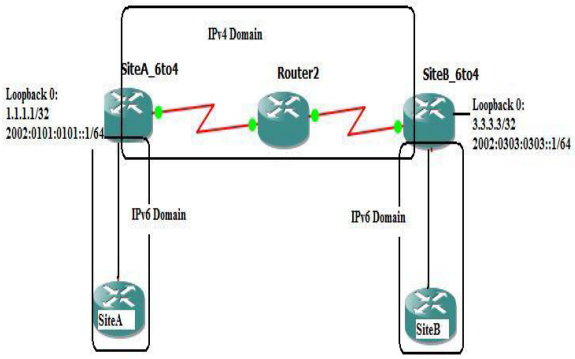

Fig. 4. 6to4 Automatic Tunneling model

Automatic means that tunnel configuration is carried out with no additional management. As shown in fig, this method is considered as the most popular choice in the field of automatic tunneling technique. When in operation, this mechanism will have IPv6 traffic tunneled upon IPv4 networks within isolated 6to4 networks. A special prefix containing the IPv4 address of its 6to4 gateway is supposed to be present in each 6to4 network, which enables tunnel endpoint addresses are acquired easily and requires no IPv6 administrative work. Then connection from 6to4 network to the rest of the IPv6 network is established via a dual stack local gateway and a dual stack relay router. Therefore, every IPv6 packet is directed to the gateway. These kinds of tunnels would transfer the traffic to appropriate gateway with suitable IPv4 address. 6to4 is an automatic type of tunneling that does not require configuration of explicit tunnels. Between the so called 6to4 gateways (6to4 routers) the communication treats the intermediate IPv4 network as a point-to-point link.

IPv6 Tunnel Broker

To set up and administer a tunnel can be difficult. An IPv6 tunnel broker provides a tunnel service to its customers with the intention of helping them to connect to an existing IPv6 network[60]. As described in the tunneling section, the tunnel routes IPv6 traffic over IPv4. This is another approach to IPv6 with the support of dedicated servers, known as Tunnel Brokers as illustrated in Figure, to answer automatically tunnel requests from users, which is believed to increase IPv6 growth with connected hosts and to support access to IPv6 networks.

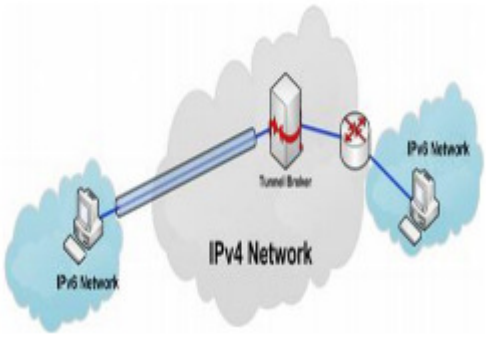

Fig. 5. Tunnel broker

Generally, the tunneling mechanism allows us to connect isolated IPv6 nodes and networks whether or not the ISP has been upgraded to IPv6. Moreover, it also takes advantage of emerging IPv6 services while remaining connected to the IPv4 world.

VI: TRANSLATION

The meaning of translation is to convert directly protocols from IPv4 to IPv6 or vice versa, which might result in transforming those two protocol headers and payload. This mechanism can be established at layers in protocol stack, consisting of network, transport, and application layers.

The translation method has many mechanisms, which can be either stateless or stateful. While stateless means that the translator can perform every conversion separately with no reference to previous packets, stateful is the vice versa, which maintains some form of state in regard to previous packets. The translation process can be conducted in either end systems or network devices.

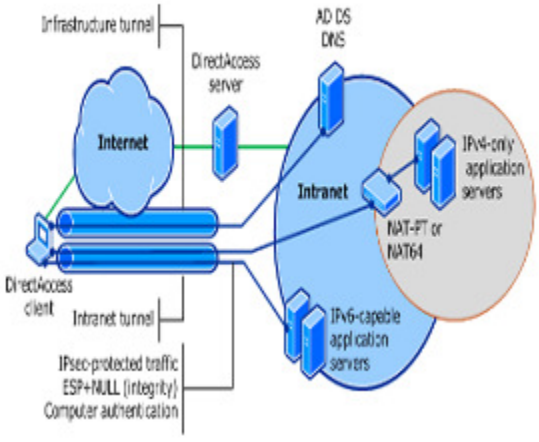

FIG. 6. Translation method model

The fundamental part of translation mechanism in transition process is the conversion of IP and ICMP packets. All translation methods, which are used to establish communication between IPv6-only and IPv4-only hosts, for instance, NAT-PT or BIS, apply an algorithm known as Stateless IP/ICMP Translator (SIIT). The function of this algorithm is to translate packet-by-packet the headers in the IP packet between IPv4 and IPv6, and also addresses in the headers among IPv4, IPv4-translated or IPv4-mapped IPv6 addresses. However, this does not mean IPv6 hosts can get an IPv4 address or route packets, but this assumes that each IPv6 host can have a temporary assigned IPv4 address

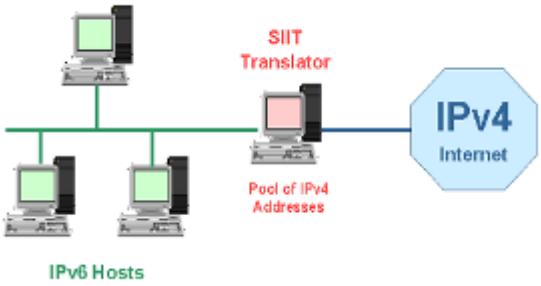

FIG. 7. SIIT Model

The above figure indicates an algorithm that designates a two-way translation between IPv4 and IPv6 packet headers or between ICMPv4 and ICMPv6 messages. The interpretation has been arranged so that UDP and TCP header checksums are not influenced during the process. More importantly, SIIT is currently used as the backbone for NAT-PT and BIS.

Network Address Translation-Protocol Translation (NAT-PT)

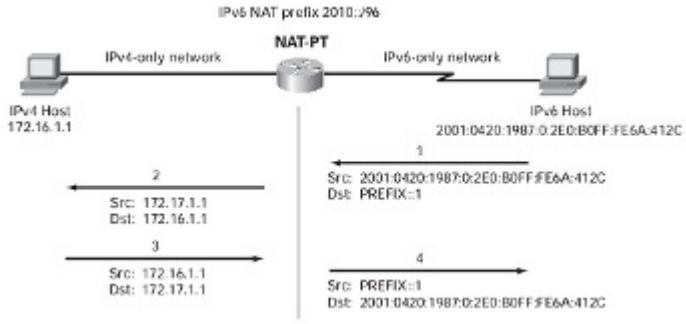

FIG.8. Deployment of IPv6 using NAT-PT

From the figure above, the router is used as a translation communicator between an IPv4-only network and an IPv6-only network. NAT-PT is considered as a stateful translator functioning in the network layer with the SIIT algorithm. The main role of a NAT-PT device, such as routers or servers, is to support numerous IPv6 nodes by assigning a temporary IPv4 address for each, which permits native IPv6 hosts and applications to communicate with native IPv4 hosts and applications. In general, it acts as a communication proxy with IPv4 peers. However, this mechanism still possesses limitations similar to IPv4 NAT such as point of failure, decreased performance of an application level gateway (ALG), reduction in the overall value and

utility of the network. NAT-PT also prevents the ability to implement security at the IP layer.

VII: CONCLUSION

From the above analysis it is very clear IPv6 has many advantages over IPv4, such as a larger address space, streamlined header, extension headers, and no need for NATs. Almost all of the most used software for implementing services in a network support IPv6 with their default configuration. Although it is a bit more complicated to implement automatic configuration of IP addresses, DNS server addresses, and default gateways for clients -- as you need software to transmit router advertisements as well as a DHCP server. One big issue is the transition from IPv4 to IPv6. The support from hardware and software vendors is there, but the demand from customers generally controls the rate at which something changes. While everything works well over IPv4 there will be little demand for IPv6. At least in the beginning phase when (and where) there still are addresses left. Given the "IPv6 world launch" occurred on 6 June 2012, we will hopefully see a larger and larger scale of implementation of IPv6 in order to accommodate the need for addresses. IPv6 will soon be the only viable option for growing networks .The transition should be as transparent for the end users as possible. We noticed for instance that an IPv6 compatible router (not part of the lab setup) had suddenly set up a 6to4 tunnel automatically. This might have occurred in association with the IPv6 launch, but we are not certain of this.

In this paper the all the methods have been analysed and we have gone through advantage and disadvantage of each transition method. There is no best method among these, each can be beneficial depends on situation of network. So, when we think of deploying networks the scenarios of ipv4 and ipv6 networks must be known and then we can select appropriate transition method for deployment.

REFRENCES

[1 "ARPAnet - The First Internet." [Online]. Available:http://inventors.about.com/library/weekly/aa091598.htm.

[2 "IANA — Number Resources." [Online]. Available: http://www.iana.org/numbers/.

[3] Bi, Jun, Jianping Wu, and Xiaoxiang Leng. "IPv4/IPv6 Transition Technologies and Univer6 Architecture." *IJCSNS International Journal of Computer Science and Network Security*, 2007: VOL.7 No.1.

[4] Hirorai, R., and H. Yoshifuji. "Problems on IPv4 - IPv6 network transition." IntecNetCore, Inc., February 13, 2006..

[5] Huang, Shiang-Ming, Wu Quincy, and Yi-Bing Lin. "Tunneling IPv6 through NAT with Teredo mechanism." Taiwan: National Chiao Tung University, April 25, 2005.