Transition of Real Time Network from IPv4 to IPv6 – Simulated Test Bed and Analysis

Saadullah Kalwar, Sarang Shaikh, Nafeesa Zaki, Aftab Memon
MUET
Pakistan
{saad.kalwar, nafeesa.zaki, aftab.memon}@faculty.muet.edu.pk, sarang@listedium.com

***ABSTRACT*:** *It has been quite a while since the introduction of IPv6 and it is one of the crucial issues being discussed today in networking society. IPv6 provides many seamless features that make it far better protocol as compared to predecessor version IPv4. On the other hand IPv4 is being used in current deployed Internet architecture and transitioning process looks very challenging. In order to avoid the transition, or in actual sense to delay it, many techniques have been introduced such as CIDR and NAT but still the fact is that pool of IP addresses is depleting and ultimate solution is to move to IPv6. In this paper issues related to transition from IPv4 to IPv6 have been focused. A simulated test bed has been deployed at Mehran University of Engineering & Technology to observe and tackle the issues and challenges that would be faced in transition from IPv4 to IPv6. The aim of this study is mainly to look into the transition mechanism that can be provided seamlessly to end users where they will be able to use all the services already being used over IPv4.*

Keywords: Ipv6, Transition Strategy, NAT, Dual Stack, Translation

Received: 24 February 2014, Revised 2 April 2014, Accepted 9 April 2014

1. Introduction

In 1970s when Internet started evolving from ARPANET, intentions about Internet were not something what we see today. It was introduced to connect few agencies of US from where it evolved to a network of networks connecting complete globe. Thus the original IP is naturally light and simple [1]. As the use of Internet protocol increased, it started becoming over whelmed because of lower features of security etc. In order to cater the demands, a lot of extensions were introduced such as Classless Inter Domain Routing (CIDR), Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT). Due to this, simple IPv4 protocol working with a lot of extensions became very complicated to use over public networks. Even worse, Internet users kept increasing in geometric progression, which created address shortage because IPv4 supports only 32 bit address that means 4.3 billion addresses but addresses based on classes would only be less than a billion. To cater these problems, CIDR and NAT mechanisms were introduced which increased total number of IP nodes from 2 ^ 32 addresses of class full addressing and somehow delayed the transition [2].

The rest of paper is organized as: Section 2 discusses the constraints that have been responsible for delay of transition and need for the transition. Then a comparison between NAT and IPv6 is provided to show difference between both the choices. In section 3 overview of transition mechanisms is given. In section 4 simulated test bed is presented. In Section 5 we will discuss why we have chosen dual stack for our network. In the last part we will discuss about various issues such as compatibility and addressing scheme.

2. Overview and Motivation

There are many constraints that have been delaying the transition process but this delay is not a long term solution. Ultimate solution is the transition to IPv6. Keeping this in mind, network of Mehran University of Engineering & Technology (MUET), Jamshoro is taken in this research and proposed complete transition layout in this paper.

Most discussed topic in networking society today is either to move to IPv6 or to stay with IPv4? If both of them are compared, the advantages being offered by IPv6 can clearly be seen over the previous versions then the question arises what holds the transition? First answer to this question is the interoperability between both the protocols. As they are not interoperable, it requires new network infrastructure, which is normally not preferred. Therefore, it is normally preferred to keep running existing protocol as long as possible. If we keep running IPv4, what keeps us using it, is network address translation (NAT). NAT makes our network a private network using private IP addresses which are not routable, connected to the router responsible for translation of private IP into the public IP address [3]. So in this way using a single public IP, set of stations can be connected to Internet, and the private IP addresses being used by them would also be used by other private networks, an example network as shown in Figure 1.

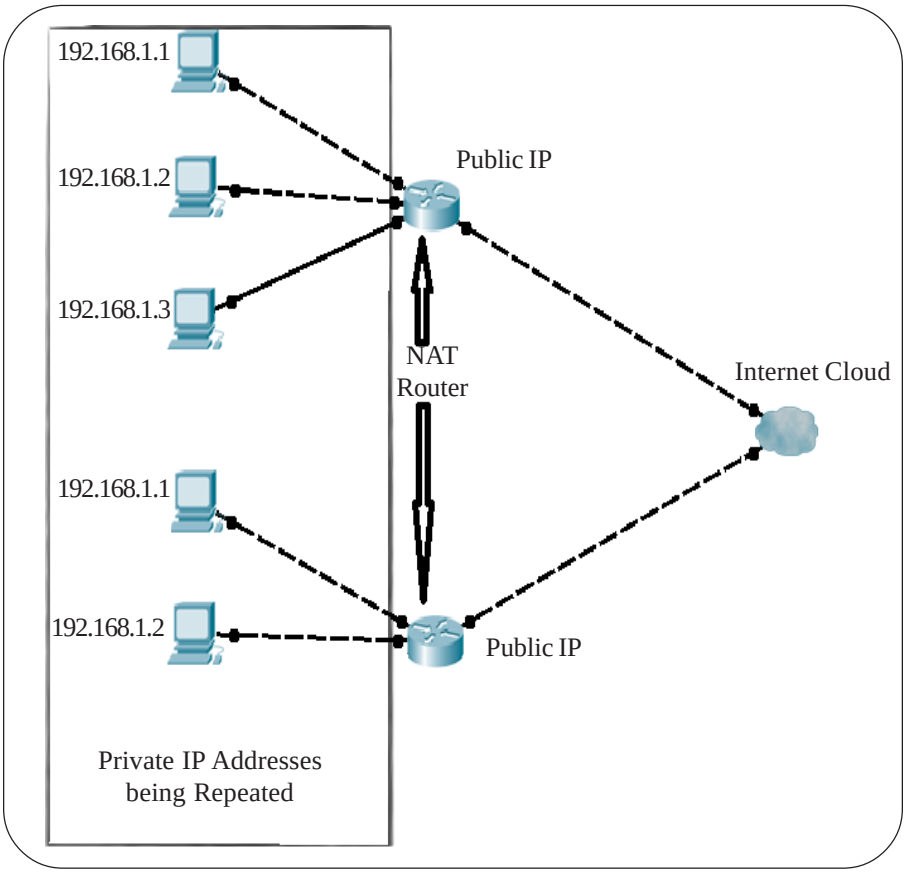

Figure 1. Working of NAT

Due to the mechanism shown in Figure 1, there is an increase in the total number of IP addresses, hence, no need to provide unique IP to each and every host over the Internet. Part of network shown inside box (Figure 1) uses private IP addresses. This introduced one more discussion that either to go for IPv6 or keep using NAT. The comparison between IPv6 and NAT is given in Table 1.

From Table 1, it can be observed that NAT is not a solution to the address shortage problem, it's just way to keep this problem on hold and keep using Internet, actual solution is IPv6. IPv6 eliminates the need of NAT by providing huge number of addresses so that every node on the Internet may have unique IP address and there be no any need of NAT [4]. It is also the necessity of time because in coming cellular generation, every mobile phone would be a unique IP node and looking at the

NAT	IPv6
NAT doesn't provide actual end to end connectivity to hosts	IPv6 global address provides end to end connectivity
NAT is not a long term solution	IPv6 is the actual solution due to unlimited address space
NAT provides isolation benefit of security	Less secure due to direct connectivity

Table 1. Comparison between IPv6 & NAT

population of countries such as China and India, we need more addresses. This will require IPv6 to be implemented as it gives us total number of addresses lot more than total population on the globe. So it may be sufficient for coming generations too.

3. Introduction to Transition Strategies

Transition strategies have also evolved along with the evolution of IPv6. Transition strategies can be categorized in translation mechanisms, tunneling and dual stack mechanism [5]. We will discuss these techniques one by one briefly.

3.1 Translation

Translation is meant for communication between IPv4 and IPv6 network. Basic mechanism behind the strategy is header translation due to which it is known as translation mechanism. It can be considered similar to NAT. NAT translates between private and public IP addresses, here IPv4 and IPv6 headers are translated to each other [6]. For example a packet originating from IPv4 network, the translator would convert its header into Ipv6 header before it is sent to IPv6 network and same process is done in inverse manner too, that can be understood from Figure 2.

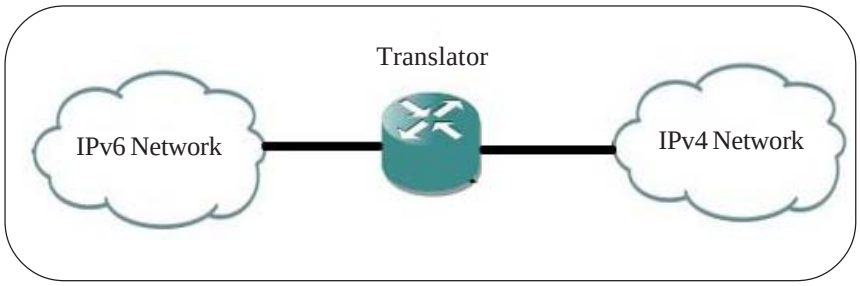

Figure 2. Translation as Transition Mechanism

In this technique, separate translator is required between both the networks, programming translators is difficult task and sometimes high capacity translators may be required. It faces similar security issues as in NAT because there is no end to end connectivity. On the other hand, it can be useful in some scenarios such as if we need to connect independent IPv6 and IPv4 nodes this one is suitable [7].

3.2 Tunneling

Tunneling is very different as compared to translation. It is used to connect two IPv6 nodes using IPv4 network. So based on today's scenarios where IPv4 is still dominant, if two IPv6 networks would communicate with each other, probably the feasible scheme would be tunneling for them. It encapsulates packets of one protocol on another. Packets originating from IPv6 node would be encapsulated within IPv4 packets so that they can be propagated along IPv4 network [8]. As shown in Figure 3:

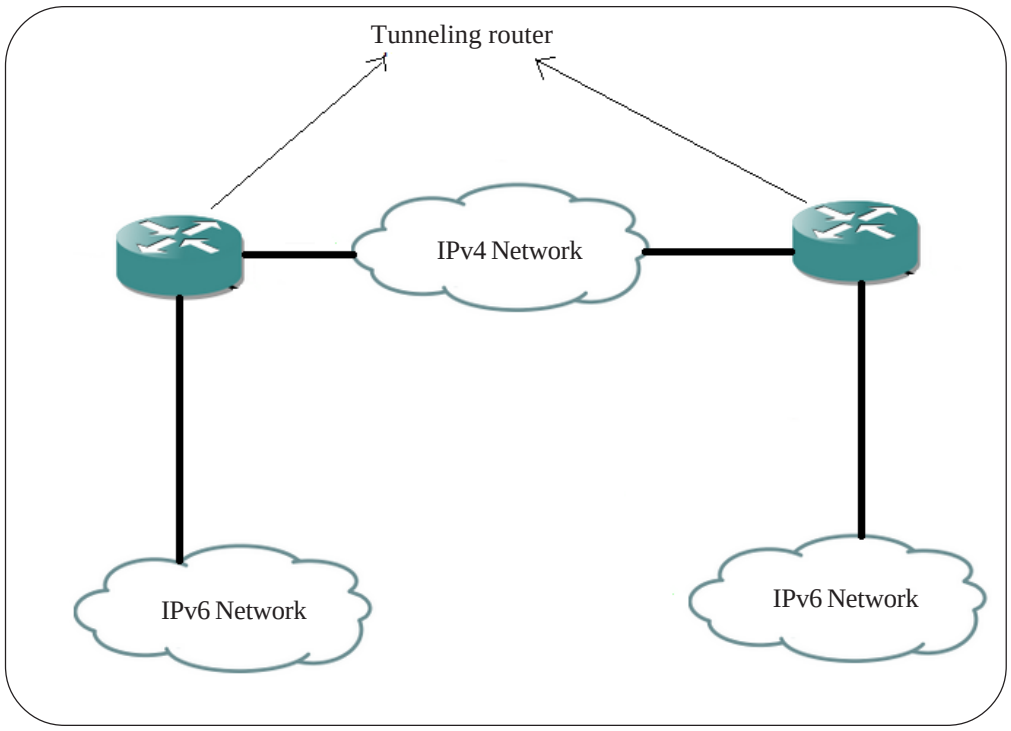

Figure 3. Tunneling as Transition Mechanism

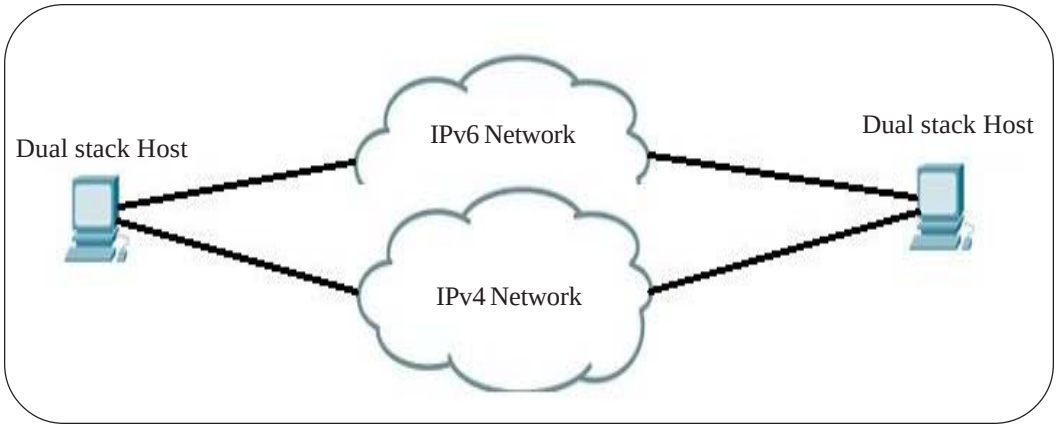

Figure 4. Dual Stack as Transition Mechanism

3.3 Dual Stack

It is the most widely translation mechanism used throughout the world [9]. That is because of its ease of implementation and support for both the protocols. In order to migrate to Ipv6, IPv4 cannot be removed because current infrastructure is on Ipv4 and it needs to be replaced gradually as IPv6 will grow. During this phase, both protocols would be used; Dual Stack Transition Mechanism (DSTM) offers us this service [10]. Using DSTM, we can assign both IPv4 and IPv6 addresses to every node on the network so we would be able to use both the services at same time, as shown in Figure 4.

4. Simulation Test Bed

For analysis, a simulated test bed was created based on the network of MUET, Jamshoro Pakistan. The network is based on Cisco standard layered hierarchy consisting of core, distribution and access layer. It is difficult to take into consideration the complete network of MUET, Jamshoro, Pakistan, therefore, standard Cisco hierarchal network is considered for simulation. Discussion about devices and their support for IPv6 is given in the Section VI.

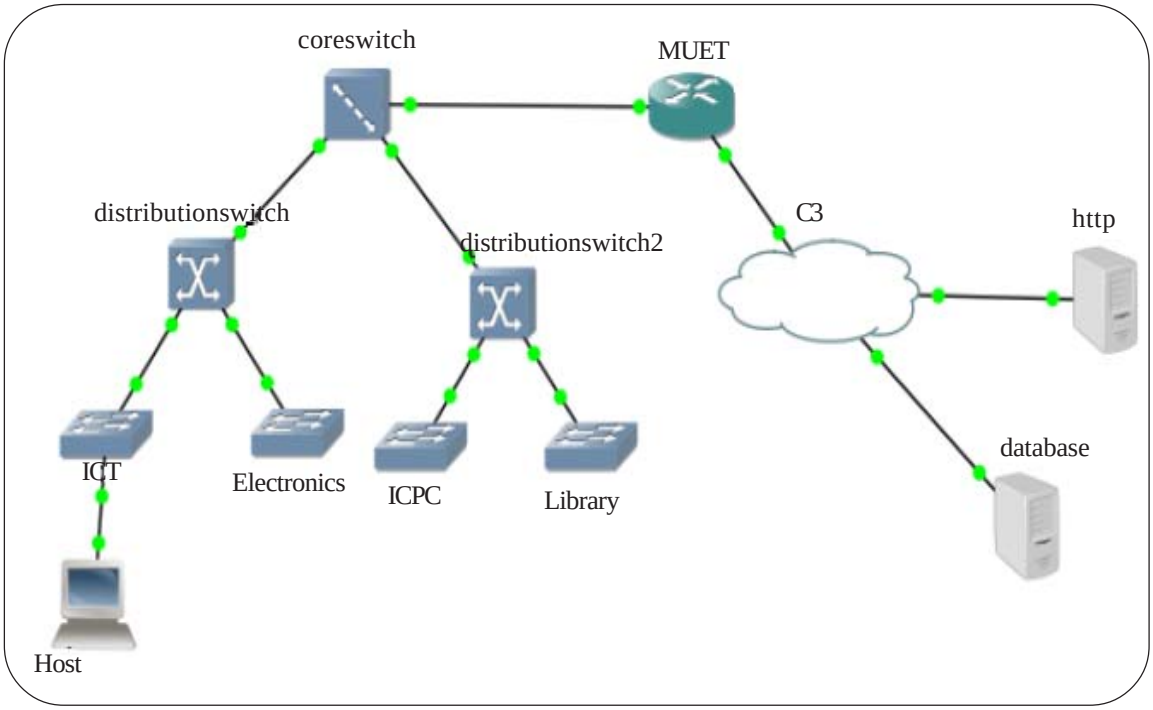

Figure 5. Test Bed Setup

Router	Interface	IPv4 Address	IPv4 Address
MUET	e0/0	192.168.0.2/30	2001.DB8::3/64
MUET	e0/1	172.16.23.3/24	2001:db8:5::1/64
Dist:	f0/0	192.168.0.6/30	2001:db8:1::4/64
Dist:	f1/0	12.0.0.1/24	2001:db8:3::3/64
Dist:	f1/1	192.168.2.1/24	2001:db8::4::3/64
Dist:2	-	192.168.0.10/24	2001:db8:2::4/64
Core	f0/0	192.168.0.1/30	2001:db8:4/64
Core	e0/0	192.168.0.5/30	2001:db8:1::3/64
Core	f1/0	192.168.09/30	2001:db8:2::3/64
Host	f2/0	12.0.0.2/24	2001:db8:3:0:a978:69b3:8d6f:2f44
C3	-	DHCP	2001:db8:5::1/64

Table 2. Dual Stack IP addresses

For simulation we have used GNS3, GNS is Graphical network simulator that allows emulation of complex networks. It allows us to use cisco IOS in virtual environment [11]. Simulation test bed is shown in Figure 5:

Figure 5 is the dual stacked network i-e every node has been assigned IPv4 address as well as IPv6 address. Tests show that both protocols would be working over the network without interfering each other. IOS image used for simulation is "*c3640-jk9o3s-mz.124-16.bin*" with IOS version 12.4. Addressing scheme is shown in Table 2.

To see how both protocols coexist, Wire Shark is used. Wire Shark is packet sniffing software which is used as network protocol analyzer. In order to show that the packets of both protocols moving over the same link, packets have been captured over a MUET dist switch as shown in Figure 5. Results are shown in Figure 6.

93	100.932000	cc:00:10:74:00:00	cc:00:10:74:00:00	LOOP	Reply
94	101.806000	192.168.0.6	224.0.0.10	EIGRP	Hello
95	102.180000	cc:02:10:74:00:10	cc:02:10:74:00:10	LOOP	Reply
96	105.128000	192.168.0.5	224.0.0.10	EIGRP	Hello
97	106.798000	192.168.0.6	224.0.0.10	EIGRP	Hello
98	109.933000	192.168.0.5	224.0.0.10	EIGRP	Hello
99	110.214000	fe80::ce00:10ff:fe74:0	ff02::5	OSPF	Hello Packet
100	110.542000	fe80::ce02:10ff:fe74:10	ff02::5	OSPF	Hello Packet
101	110.932000	cc:00:10:74:00:00	cc:00:10:74:00:00	LOOP	Reply
102	111.166000	192.168.0.6	224.0.0.10	EIGRP	Hello
103	112.180000	cc:02:10:74:00:10	cc:02:10:74:00:10	LOOP	Reply
104	114.301000	192.168.0.5	224.0.0.10	EIGRP	Hello
105	115.643000	192.168.0.6	224.0.0.10	EIGRP	Hello
106	119.137000	192.168.0.5	224.0.0.10	EIGRP	Hello
107	120.089000	192.168.0.6	224.0.0.10	EIGRP	Hello
108	120.229000	fe80::ce00:10ff:fe74:0	ff02::5	OSPF	Hello Packet

Figure 6. Wire Shark Hello Packets

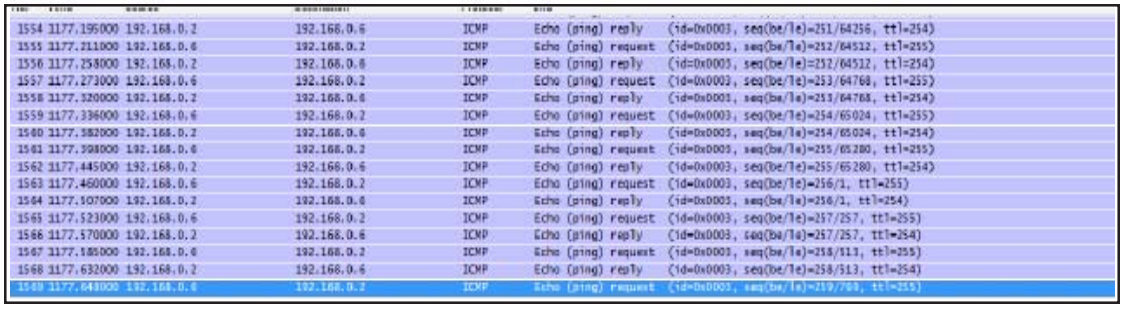

Figure 7. Ping over IPv4

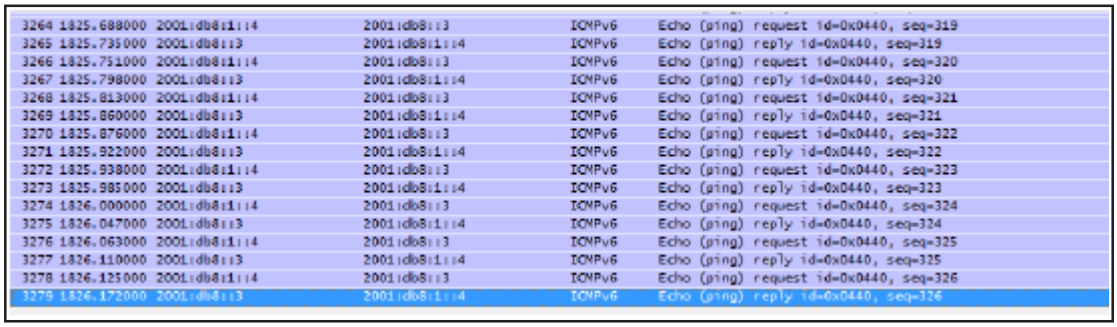

Figure 8. Ping over IPv6

Hello packets of EIGRP and OSPF can be seen in Figure 6. EIGRP is running over IPv4, its multicast address is 224.0.0.10 which can be seen, similar address for OSPF in IPv6 is ff02::5 which can also be seen.

To check connectivity, ping MUET from dist switch.

Figure 7 shows ping requests and replies over IPv4, we now check connectivity from same routers over IPv6:

Figure 8 shows connectivity over IPv6. The protocol used for ping in IPv6 is ICMPv6 similar to ICMP in IPv4.

The connectivity between both (Ipv4/IPv6) the protocols has been discussed in the above Sections, which shows that for smooth transition, it is necessary that end user should not be affected which is only be possible when user gets all the services over new protocol (IPV6) which were available over IPv4. In order to test that, some basic services were run over the network.

To show how users will use applications, IPv6 Internet is required which is not yet available in Pakistan, hence, we made our own servers which are shown in test bed (Figure 5) by connecting to cloud C3. These servers were made on separate machines and

Figure 8. HTTP Server being accessed over IPv6

linked up to GNS3 through physical interface. Hence, works like our own Internet cloud.

To simulate the end user, VMware virtual machine has been used as host which is connected to ICT switch in the test bed. Virtual machine has been linked with GNS3 with the help of loopback adapter. Windows XP operating system is used for virtual machine. Windows XP (and all newer operating systems of Microsoft) has built in support of IPv6. But IPv6 is disabled in Windows XP by default. We can simply enable it by entering "*ipv6 enable*" in command prompt.

When http server is accessed from the virtual machine, following results (Figure 8) are achieved:

Figure 8 shows end to end connectivity as well as it shows how we can provide transition without effecting the end user's applications.

5. Why dual stack as the transition mechanism?

As explained in Section IV, DSTM meets all our requirements of co-existing with IPv4 and IPv6, whereas other transition mechanisms do not allow us to use both the services. Most of the equipment and software today already support dual stack mechanism. Most of the major websites throughout the world are already dual stacked. Keeping all this in mind, DSTM has been chosen as the transition mechanism for the test bed, this will allow both protocols to run simultaneously and provide seamless transition from IPv4 to IPv6 gradually.

6. Compatibility

In 2000, Cisco announced an IPv6 roadmap for its IOS operating system. In 2001, Cisco IOS Software Release 12.2T incorporated IPv6 in its first commercial release. Subsequently, Cisco Software Release 12.0S enabled the support of IPv6 in core service provider infrastructures. Currently Cisco IOS releases enable IPv6 in a wide range of Cisco products.

In our simulation, we have used Cisco 3645 router that has IOS 12.4 that is compatible with IPv6. The edge router of MUET is Cisco 3845 that has IOS Cisco 12.4. Cisco cat 4006 is the switch being used at core layer, it has IOS version 12.2. Similarly at distribution layer, the network of MUET has Cisco 3550 and 3750 switches, those also have IOS version 12.2. Switches at access layer are Cisco 2950, those have IOS version 12.1.

At the user end, everything will remain unchanged. In case of PC having Windows XP, IPv6 can be enabled easily using simple commands [12].

7. Addressing Scheme

Current subnet structure of MUET is 172.16.x.0/24, where x is VLAN number. Great address space of IPv6 again provides

advantage here. More number of VLANs can be created and more hosts can be conFigured for each VLAN. Creating VLANs in IPv6 is similar to that of IPv4. We can use link local addresses. A possible structure of VLANs can be: FF00:0:0:x::/64, where x is the VLAN number. So with this addressing scheme, we can assign similar subnet numbers to all VLANs and we'll still be having a lot of free subnets available for future use. For example core router has IPv4 address 172.16.60.0, so its IPv6 address will be FF00:0:0:60::

VLANs will be created in the same manner. Here we take example of ICT. The VLAN number of ICT is 23 so the IP addresses assigned belong to 172.16.23.0. IPv6 addresses for the hosts of ICT will be in network FF00:0:0:23::. A host having IPv4 address 172.16.23.10 will have IPv6 address FF00:0:0:23::10 [13].

8. Conclusion

Transition to IPv6 is a planned process; major players all over the world have already started the process. We also need to do so before it's the high time. Based on the research work, it is concluded that the decision of transition strategy depends on the type of network. All the strategies have been discussed. Most of the hardware and software is also supporting the IPv6 so it is the high time to move towards IPv6, before the actual need arises.

9. Acknowledgements

We would like to acknowledge Prof. Dr. Aftab A Memon along with staff of ICPC, Mehran University Jamshoro, Pakistan for his valuable guidance throughout this research work. Without their kind support this work would not have been possible.

We would also like to acknowledge the support and services of IEEE RDPP for creating awareness about research and development around the region

References

[1] Postel, J. (1981). Internet Protocol, STD 5, RFC 791, September.

[2] Fuller, V. (1993). Classless Inter-Domain Routing (CIDR), RFC 1519, September.

[3] Cisco Systems. How NAT works, http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml.

[4] Next Generation Internet: IPv4 Address Exhaustion, Mitigation Strategies and Implications for the U.S. An IEEE-USA White Paper.

[5] IoanRaicu, SheraliZeadally. (2003). Evaluating IPv4 to IPv6 Transition Mechanisms, IEEE International Conference on Telecommunications, ICT'2003, V. 2.

[6] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., Li, X. (2010). IPv6 Addressing of IPv4/IPv6 Translators, RFC 6052, October.

[7] CISCO. (2012). bNAT64 Technology: Connecting IPv6 and IPv4 Networks, White paper, April.

[8] Conta, A., Deering, S. (1998). Generic Packet Tunneling in IPv6, Cisco Systems December.

[9] Xianhuiche Dylan Lewis. (2010). IPv6: Current Deployment and Migration status, *International Journal of Research and Reviews in Computer Science* (IJRRCS), June.

[10] Martin Dunmore. (2005). An IPv6 Deployment Guide, 6net, The 6NAT Consortium, September.

[11] Mike Fuszner. Graphical Network Simulator, http://www.gns3.net/

[12] Cisco router guide, summer .

[13] Chown, T. (2006). Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks, RFC 4554, June.