Performance Analysis of Three Transition Mechanisms between IPv6 Network and IPv4 Network: Dual Stack, Tunneling and Translation

Md. Asif Hossain[a]*, Durjoy Podder[b], Sarwar Jahan[c], Mustafa Hussain[d]

[a,b,c,d]*Department of Electronics & Communications Engineering, East West University, Dhaka-1212, Bangladesh.*

[a]*Email: asif@ewubd.edu*
[b]*Email: durjoypodderewu065@gmail.com*
[c]*Email: sjahan@ewubd.edu*
[d]*Email: mhussain@ewubd.edu*

Abstract

Due to the increasing demand of the Internet, we are facing a great problem of the depletion of our existing IPv4 (Internet Protocol version 4) network. To solve the situation, we have to use IP version 6 in coming years. But the IPv4 network will not be opt out, but also coexist with IPv6 network. For the transition from IPv4 to IPv6 and vice versa, there are three prominent transition mechanisms are used. They are Dual Stack, Tunneling and Translation. In this paper, the performances of these three mechanisms have been analyzed. IPv6 header format, its security and the routing also have been focused. For the simulation Packet Tracer simulation software has been used**.**

Keywords: IPv4; IPv6; Dual Stack; Tunneling; Translation.

1. Introduction

Every end device and node needs an IP (internet protocol) address to communicate between the hosts. Address number of currently used IP version 4 is too limited to handle the new demand of IP addresses [1].

----

* Corresponding author.

There are some techniques developed to handle this address space problem, they are Network Address Translation (NAT), Variable Length Subnet Mask (VLSM), Classless Inter domain Routing (CIDR), Port address translation (PAT) and so on. But these all technology are not able to save the IP address shortage's problem. Due to the limitation of IPv4 addresses, another technology raised: Internet Protocol Version 6 (IPv6). The IPv6 was designed for sufficient address space for the present and the future demand for the increased growth of internet. IPv6 increases IP address scheme size from IPv4-32 bits to 128 bits [2]. IPv6 address is cooperated with IPv4 address; this means IPv6 networks is able to merge with IPv4 networks for the future networks. But, anyhow IPv4 does not support new upcoming network criteria. The present IPv4 network is huge and complex, so IPv4 could not be replaced by IPv6 suddenly. Migration from one technology to another technology is absolutely difficult, because of IPv4 and IPv6 are not same assemblage for communication. The three prominent transition mechanisms are widely known as Dual Stack, Tunneling and Network address translation [3].

Though several works have been done on the comparison between these mechanisms [4-8], but still many problems not resolved yet, calling for huge challenges on IPv6 transitions research. In this paper, the typical analysis has been done after developing the separate networks for each transition.

The rest of the paper has been arranged as follows: in chapter 2, details of IPv6, its format, types and other features have been discussed. Three transition mechanisms have been discussed in chapter 3. In chapter 4, the three transitions have been deployed by using packet tracer. Results have been analyzed in chapter 5 and the paper has been concluded in chapter 6.

2. Overview of IP version 6

In this section, details about IPv6, its representation, format, features and the comparison between IPv4 have been discussed.

2.1 IPV6 Address

IPv6 Internet Protocol is developed as the upcoming future network layer protocol, to overcome the shortages of IPv4 address space .The IPv6 is the sixth version of the IP address. The IPv6 protocol address is 128-bit long .To represent the 128 bit address, IPV6 uses total 8 field of consisting 4 hexadecimal values separated by colons which is represented like(:).So it creates possible $2^{128} = 3.4 \times 10^{38}$ addresses[2]. This is a very large number of addresses, then IPV4. These new IPv6 address will meet the Internet demand and it assure to fulfill the needs.

Basically, there are 3 types of addressing of IP version 6, they are:

1. Unicast address

It identifies the signal at the network interface where the IP delivers packets sent to a unicast address to the specific host to the internet.

2. Anycast address

In this addressing system, the IP address is assigned to a group interfaces and it can be different nodes. It also used as the identification of the hosts on the internet. If a multicast addresses, sent a packet to an anycast address it reach only one of the interface in the nearest host. On the contrary, anycast addresses are not being able to identify when the addresses are in the same format as unicast address and only differ that by the sense of multiple point for this reason it can be said that the unicast address working function is like that anycast address.

1:1 Unicast addresses   1:n Multicast addresses   1: closest Anycast addresses
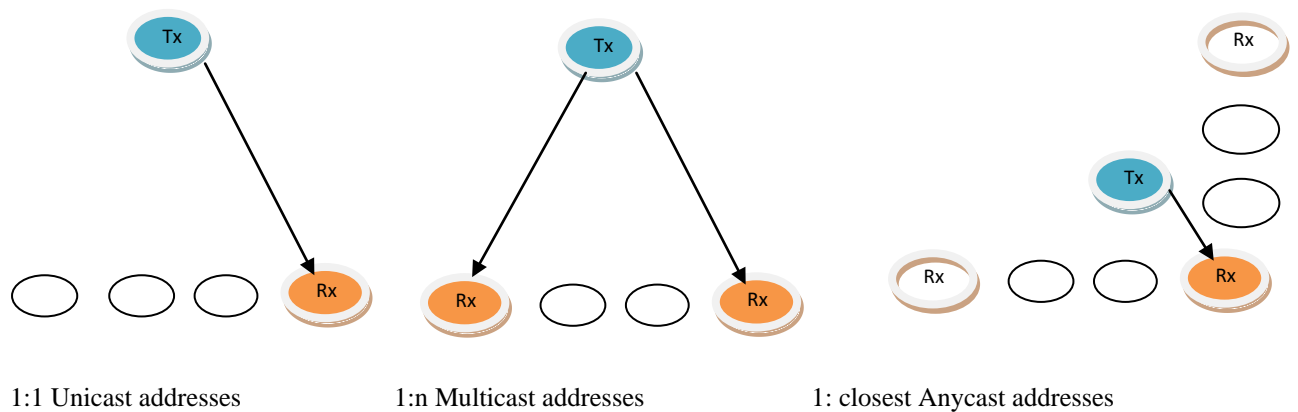
Figure1: Types of IPv6 Addresses

3. Multicast address

A multicast address identifies the multiple interfaces on the internet. A packet sent into the all interfaces in the set which can join the corresponding multicast group by using multicast address. It is known that IPV6 does not have broadcast address, but here broadcast is subsumed by multicast addressing using a multicast group "ff02::1".For reducing the hampers of interface the IPV6 protocol uses the link-local multicast group**.**
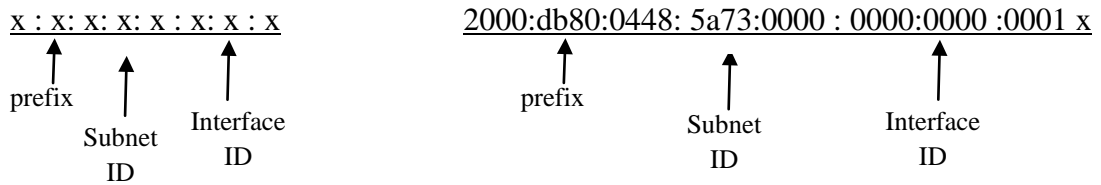
2.2 Benefits of IPv6

Some benefits of IPv6 protocol are given bellow:

- Very large address space (2^{128}).
- It allows extensibility
- Simpler header format compared to IPv4.
- It supports enhanced mobility and increased security than IPv4.
- IPV6 addresses support the auto-configuration mode that gives more flexibility manageability of the larger network.

2.3 IPv6 Address Format

IPV6 address use basically 128 bit for IP addressing and this 128 bits are separated by eight groups, each group have sixteen bit and they are separated by colons ":". For Example,

"2000:db80:0448:5a73:0000:0000:0000:0001" here it can notice that every letter is used in small letter, which is suggested by IETF. The block of zeros can be simplified using double colons "::". Thus the given address is like 2000:db80:448:5a73::1. Network address ranges are written in Classless Inter Domain Routing (CIDR) notations. A network is denoted by the first address in the block, a backslash (/) and a decimal value equal to the size in bits of the prefix.

x : x: x: x: x : x: x : x

prefix

Subnet ID

Interface ID

2000:db80:0448: 5a73:0000 : 0000:0000 :0001 x

prefix

Subnet ID

Interface ID

Figure 2: IPV6 addressing format

3. Transition Mechanisms between IPV4 and IPV6

There are three mechanisms are currently used for IPv4 to IPv6 transition. They are: dual stack, tunneling and network address translation.

3.1 Dual Stack

Dual stack is a common and core system of transition techniques between IPV4 and IPV6 network. As stated earlier Dual Stack technique is allowed to apply between an IPv4 and IPv6 address, it has to be defined on the same network interface, it means that we can use a router but we have to use a separate interface for both ipv6 addressing. In the dual stack implementation all the network devices like workstations, servers, routers, and so on**.** In order to implement dual stack all the devices need to support both the IP versions and extra processing power and simultaneously handle both the protocols**.** In Figure3, a typical dual stack scenario has been shown.

IPv4/ IPv6 Application

TCP   UDP

IPv4   IPv6

Ethernet   FDDI   PPP   etc
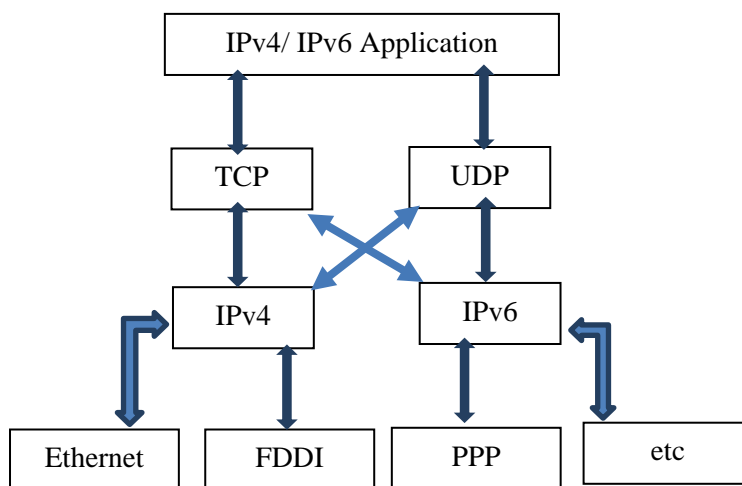
Figure 3: Dual Stack Transition

This technology does not change the packet header and it also does not make encapsulation between IPv4 and

IPv6. According to [6], the Internet contains nodes and the nodes whose are able to support both protocols in parallel within the same infrastructure can provide the transmission of data for IPv4 and IPv6 network. This system is not suitable for large networks like the Internet because it is complex and costly to cover all the nodes in such huge networks. However, it is suitable for the small network.

3.2 Tunneling

In tunneling, the header of the packet is changed when it moves from one type protocol to another. So an IPv6 packet can migrate to IPv4 packet to interconnect IPv6 network hosts via IPv4 backbone using IPv6 tunnels. This mechanism is applicable when one IPv6 site has to be connected with another IPv6 site through an IPv4 infrastructure by creating a tunnel interface between two IPv6 networks. Tunneling strategies provide a cost effective solution for connecting IPv6 networks. Only the gateway routers need to be upgraded to support both IPv4 and IPv6 protocols. It allows communication establishment between IPv6 networks over an IPv4 network only or still not ready to deploy IPv6. There are several types of tunneling are available such as manual tunneling, GRE (Generic Routing Encapsulation) tunneling, ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), Tunnel broker and 6to4 tunneling. In this paper, 6to4 tunneling is used [9].
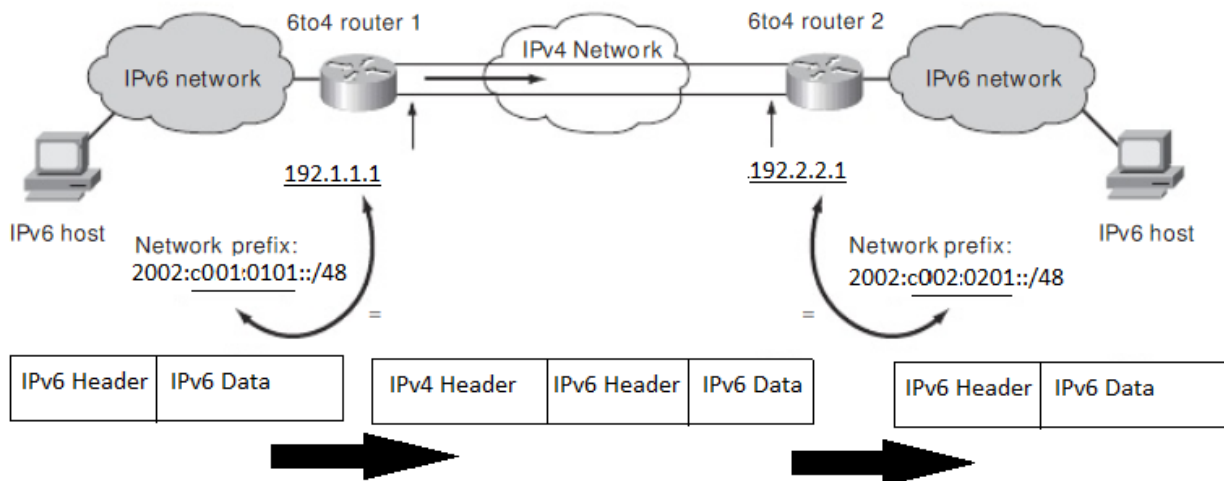
Figure 4 : 6to4 Tunneling

From the Figure4, it is shown that two IPv6 hosts from two different networks are connecting each other through IPv4 network infrastructure. The IPv6 packets are encapsulated inside IPv4 packets for the transmission within IPv4 network. The global IPv4 address that is assigned to a host, a 48-bit 6to4 IPv6 prefix can be constructed by that host by appending the IPv4 address to 2002::/16. For example, the global IPv4 address 192.1.1.1 has the corresponding 6to4 prefix 2002:c001:0101::/48 (known as 6to4 address) This gives a prefix length of 48 bits, which leaves space for a 16-bit subnet field and a 64 bit host addresses within that subnets [10].

3.3 Translation

This mechanism of transition changes the header format from IPv4 to IPv6 format and vice versa. This scheme translates the packet from both the addresses. By using this translation, IPv6only hosts can communicate with IPv4only hosts. Translation methods are of two types, such as stateless and stateful. The stateless translation, the packets are not interrelated to each other while the stateful translation is interrelated to each other.
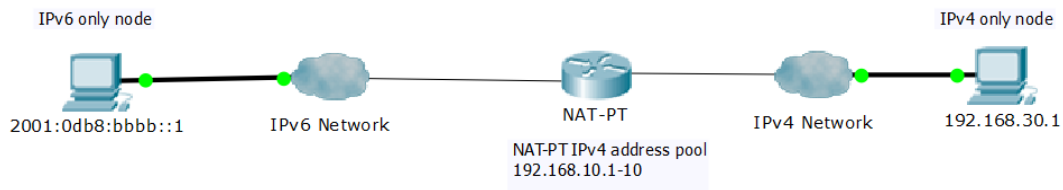

Figure 5: NAT-PT Transition

In this paper, NAT-PT (Network Address Translation--Protocol Translation) mechanism has been used.

4. Implementation of the Transition

4.1 Dual Stack

The following topology has been developed in Packet Tracer 6.2 to implement the dual stack transition.
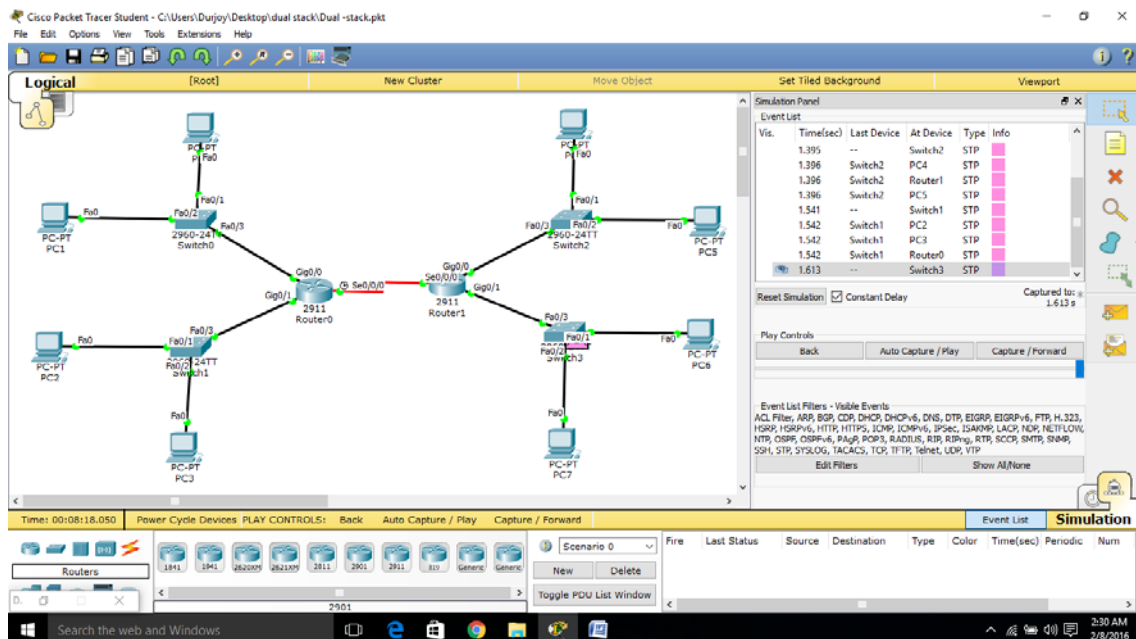

Figure 6: Dual-stack system

For the above topology, the following key configuration codes have been used:

Router(config)#router rip

Router(config-router)#no auto-summary

Router(config)#ipv6 unicast-routing

Router(config)#ipv6 router rip cisco

Router(config)#interface gigabitEthernet 0/1

Router(config-if)#ipv6 rip cisco enable

Router(config-if)#exit

In Figure6, a server having both IPv4 and IPv6 address configured, in that it can now communicate with all the hosts on both the IPv4 and the IPv6 networks with the help of a Dual Stack Router.

4.2 Tunneling

For developing the scenario for tunneling transition, the following topology (Figure7) and the configurations have used:
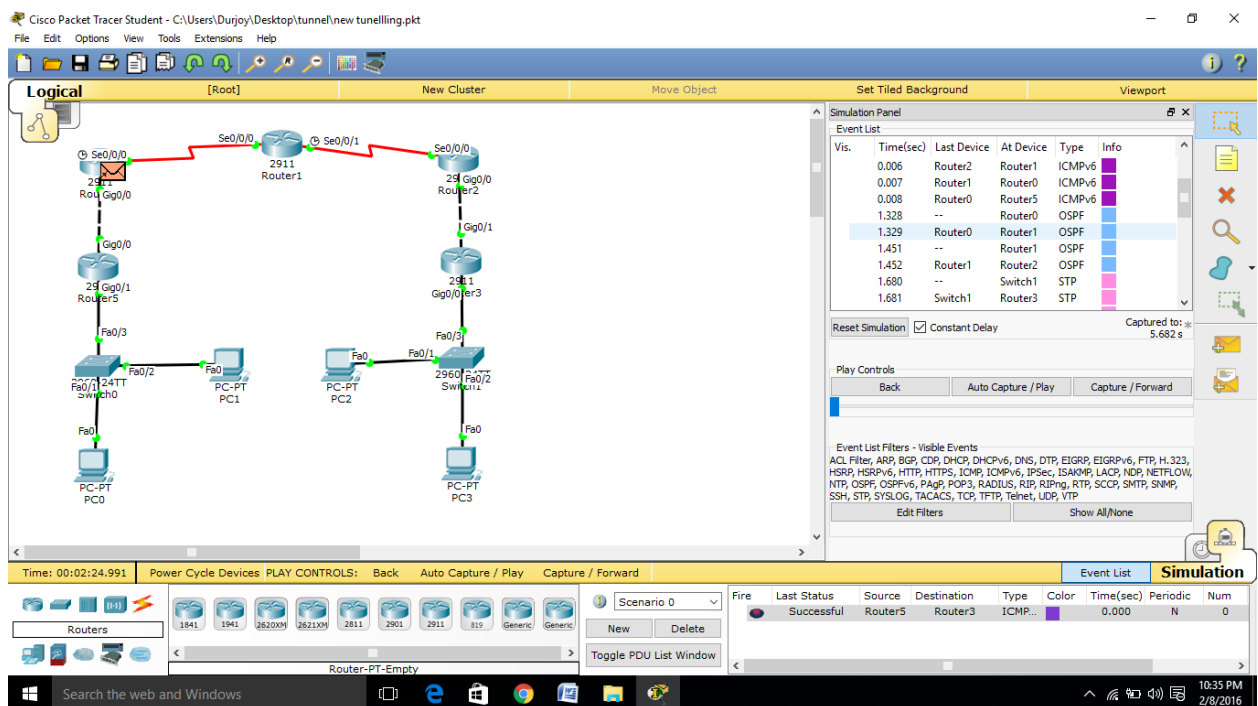

Figure 7: Tunneling system

Some main configuration codes:

Router(config-router)#network 192.23.1.0 0.0.0.255 area 0

Router(config-if)#ip address 192.23.1.2 255.255.255.0

Router(config-if)#ipv6 address 2000:1:1:1:1:1:1:1111/112

Router(config)#ipv6 unicast-routing

Router(config)#interface tunnel 10

Router(config-if)#ipv6 rip 6bone enable

Router(config-if)#tunnel source serial 0/0/0

Router(config-if)#tunnel destination 192.34.1.4

Router(config-if)#tunnel mode ipv6ip

Router(config-if)#duplex auto

Router(config-if)#speed auto

4.3 NAT Protocol Translation

We have configured the topology for the NAT Translation like Figure8:

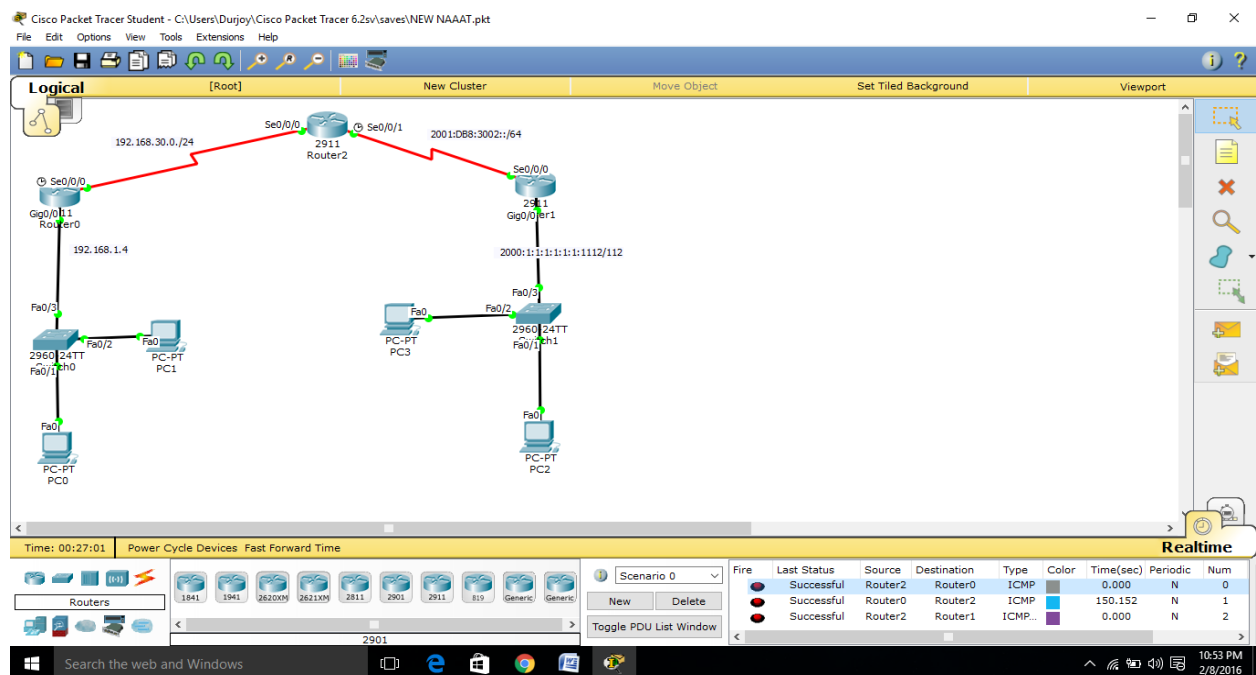**Figure 8:** NAT translation system

The only transition codes have been shown:

Router(config)#ipv6 unicast-routing

Router(config)#interface Loopback0

Router(config-if)# no ip address

Router(config)#interface serial 0/0/0

Router#configure terminal

Router(config)#interface gigabitEthernet 0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#duplex auto

Router(config-if)#speed auto

Router(config-if)#ipv6 address 2000:DB8:30002::9/64

Router(config-if)#ipv6 address 2001:DB8:3002::9/64

Router(config-if)#ipv6 route ::/0 2001:DB8:3002::10

Router(config)#ipv6 nat v4v6 source 192.168.30.9 2000::960B:202

Router(config)#ipv6 nat v6v4 source 3001:11:0:1::1 150.11.3.1

Router(config)#ipv6 nat prefix 2000::/96

5. Results

In this paper, the latency analysis, the throughput analysis and the packet loss analysis have been done. After deploying the above topologies of the transition mechanisms, some complex Protocol Data Unit (PDU) have been transferred from one host to another host. In this analysis, ICMP packets have been transferred with various sizes and duration. After observing the packet transmissions, the following results have been found:

From the Figure9, it has been found that the NAT-PT transition gives the highest latency, while Dual stack provides the moderate and the Tunneling mechanism provides the lowest latency.

After collecting data of throughput vs packet size from the simulation, it is found that Tunneling gives the highest throughput rate than the other transition mechanism and the NAT-PT method provides the lowest
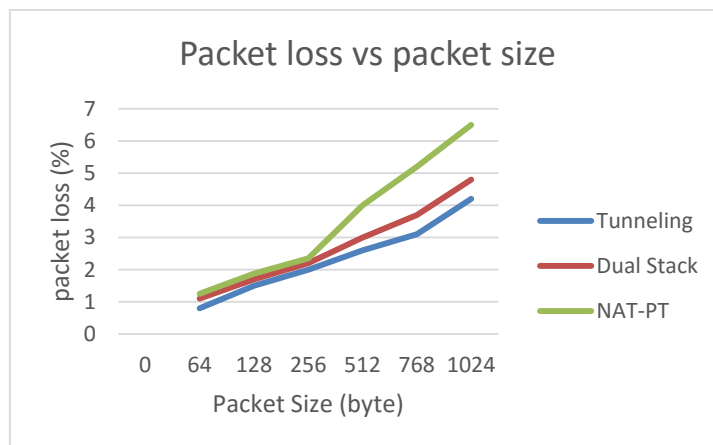
because of its extra time consuming for the header translation. It is to mentioned that, throughput, R= packet size (L)/ time consumed for transmission.
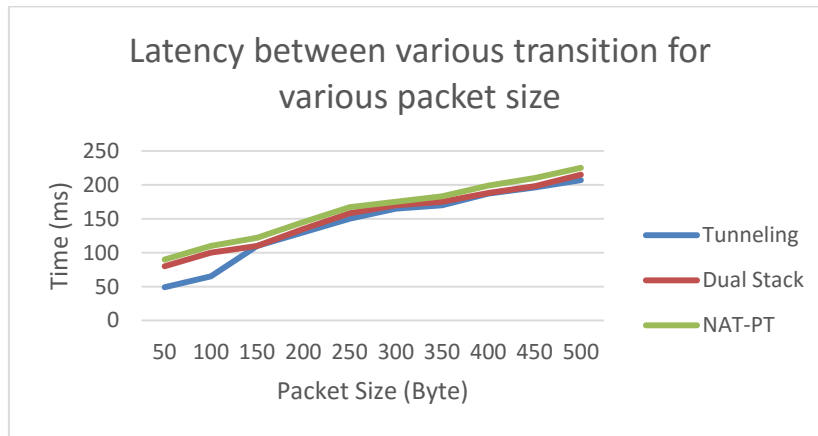
Figure 9: Latency Analysis of the transition mechanisms
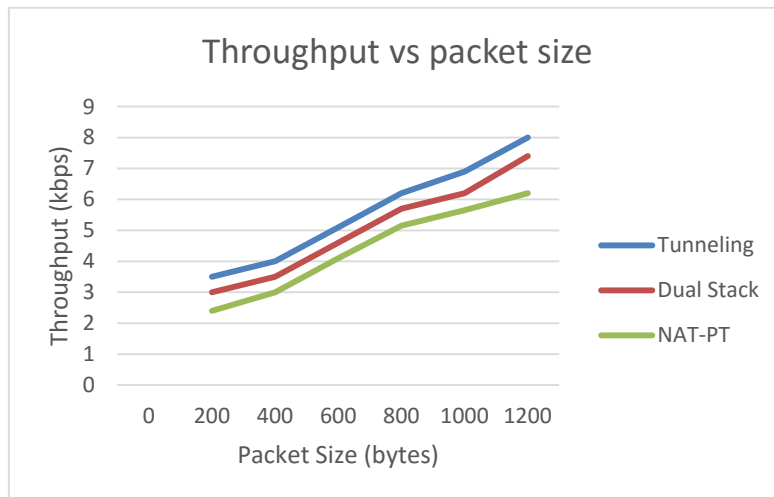
Figure 10: Throughput Analysis

Figure 11: Packet Loss Analysis

From Figure11, it is found that NAT-PT transition mechanism experiences highest percentages of packet loss due to its time consuming limitation. On the other hand tunneling has the lowest packet lost experience.

From the above overall scenarios, the following results have been found:

Table 1: Comparative analysis of three transition mechanisms.

Features	Tunneling	Dual Stack	NAT-PT
Latency	Low	Medium	High
Throughput	Highest	Moderate	Lowest
Packet Loss	Low	Higher compare to tunneling	High

5. Conclusion

In this paper, the three mechanisms of the IPv6 to IPv4 transition have been discussed, deployed and analyzed. It has been found that three mechanisms have distinct advantages and features with some disadvantages. The appropriate transition mechanism will be chosen for the network based on various parameters like the size of the network, the availability of the latest devices, the cost, the security concern and so on. Some of them have been focused on this paper with the simulation results. If latency, throughput and packet loss are considered then tunneling method is the best choice while the NAT-PT is the worst. But the tunneling method has some security issues that will be solved by IPsec (IP security). So our recommendation is to use tunneling mode with IPSec for the transition purpose. Due to the limitation of Packet Tracer, our comparisons were also limited to few application layer services. Our experiments were also limited to the Cisco devices only. So, in future, the paper will be expanded in NS3 simulator and also in real devices. The analysis will also be extended by including the security concern in details.

References

[1] G. Huston, "IPv4 Address Report." http://www.potaroo.net/tools/ipv4/index.html. 2010.

[2]Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2005.

[3] J. Bi, J. Wu, and X. Leng, "IPv4/IPv6 Transition Technologies and Univer6 Architecture", IJCSNS, Vol. 7, No. 1, pp. 232-242, January 2007.

[4] Raicu, I.; Zeadally, S., "Evaluating IPv4 to IPv6 transition mechanisms," in Telecommunications, ICT 2003. 10th International Conference on, vol.2, no., pp.1091-1098 vol.2, 23 Feb.-1 March 2003.

[5] Kuobin Dai, "IPv4 to IPv6 Transition Research Based on the Campus Network," in Intelligence

Information Processing and Trusted Computing (IPTC), 2011 2nd International Symposium on , vol., no., pp.199-202, 22-23 Oct. 2011.

[6] Wu, P., Cui, Y., Wu, J., Liu, J. and Metz, C., "Transition from IPv4 to IPv6: A state-of-the-art survey", IEEE Communications Surveys & Tutorials, 15(3), pp.1407—1424, 2013.

[7] Yu Zhai; Congxiao Bao; Xing Li, "Transition from IPv4 to IPv6: A Translation Approach," in Networking, Architecture and Storage (NAS), 2011 6th IEEE International Conference on, vol., no., pp.30-39, 28-30 July 2011.

[8] Ibáñez Parra, J., "Comparison of IPv4 and IPv6 Networks Including Concepts for Deployment and Interworking", INFOTECH Seminar Advanced Communication Services (ACS), pp.1-13, 2014.

[9] Amr, P.; Abdelbaki, N., "Convergence study of IPv6 tunneling techniques," in Communications (COMM), 2014 10th International Conference on , vol., no., pp.1-6, 29-31 May 2014.

[10] Coonjah, Irfaan; Catherine, Pierre Clarel; Soyjaudah, K.M.S., "6to4 tunneling framework using OpenSSH," in Computing, Communication and Security (ICCCS), 2015 International Conference on , vol., no., pp.1-4, 4-5 Dec. 2015.

[11] Wenming Shi; Chuanhe Huang; Qinggang Wang; Yan Chen; Yiming Huang; Yong Cheng, "A Novel IPv4/IPv6 Translation Mechanism Based on NAT-PT," in Advanced Communication Technology, The 9th International Conference on , vol.2, no., pp.1037-1041, 12-14 Feb. 2007.

[12] Ali Albkerat and Biju Issac, "Analysis of IPv6 Transition Technologies", International Journal of Computer Networks & Communications (IJCNC) Vol.6, No.5, September 2014.