Routing Virtualization Intended for a Real Time Simulation over a Testbed designed for IPv4/IPv6 Transition Techniques

SHERYL RADLEY, SHALINI PUNITHAVATHANI D, MARI KUMAR B.

Department of Computer Science and Engineering
Government College of Engineering, Tirunelveli, Anna University
Rettiyar Patti, Nagercoil NH, Tirunelveli, 627007
Tamil Nadu, India
sherylradley@gmail.com

Abstract: - The swift growth of the Internet has led IPv6 to loom on the horizon. IPv4-IPv6 transition rolls out several challenges to the world of Internet as the Internet is migrating from IPv4 to IPv6. IETF proposes transition techniques which includes Dual stack, Translation and Tunneling. A transition allows IPv4/IPv6 coexistence and interoperability, in order to maintain end to end model that the Internet is built on. The three individual mechanisms do not provide a thorough solution. To address this need we have developed a Testbed using a Real Time Simulator Packet tracer 6.0.1 for Routing Virtualization (RV) using a single physical Router and have compared the different transition techniques proving high scalability and reachability. The throughput is witnessed in the test analysis. The different parameters are also compared and studied for different transition mechanism under access, distribution and core network.

Key-Words: - : IPv4, IPv6, Dual stack, Tunneling and Translation, Routing Virtualization

1 Introduction

With the rapid development of wired/wireless communication networks in recent decades, necessity for sufficient Internet Protocol (IP) addresses to meet the demand of many devices which communicates with/without an infrastructure are considered. The data in the internet is transmitted in the form of packets over the networks. Ipv4, the first version of the internet protocol that provides unique global computer addressing to make sure two entities can uniquely identify one another. Due to growth in the number of users day to day, IPv4 is losing its pace. The next generation IP (IPng), IPv6 has been selected from several proposed alternatives as a suitable successor of the existing protocol, since it provides sufficient IP addresses to enable all kinds of devices to connect to the internet [10]. Unfortunately, IPv4 and IPv6 are incompatible protocols. IP provides the critical functionality that enables stable, reliable communication and survivability of information between computers across various network types, access network, distribution network and core network. With rapid growth of the Internet has led to the anticipated depletion of address in the current version of the Internet Protocol, IPv4. Hence IPv6 is designed to rectify the short comings. For instance, number of addresses, fragmentation, security and supports auto configuration [22].

The IETF Next Generation Transition Working Group (NGtrans) has proposed many transition mechanisms to enable the seamless integration of IPv6 facilities into current Networks. The transition mechanisms are proposed to create a smooth transition [2] [25]. Deployment of Internet Protocol Version 6 (IPv6) in the Internet has been relatively slow since its introduction over a decade ago. There are a variety of business and practical reasons for the low prevalence of IPv6 networks. The reason behind this is the backbone of the network cannot be changed overnight [26]. Number of techniques has been proposed over these years to support the continuous growth of the global Internet required for overall architecture development to accommodate the new technologies that support the over growing number of users, applications, appliances and services such as NAT-PT, Bump in stack (BIS), Stateless Internet Protocol Internet Control Messaging Protocol (SIIT), static tunneling, Tunnel Broker, ISATAP, 6to4, 6in4, 6over4, Teredo, NAT64, 6rd (IPv6 Rapid Development) has been developed to support the interoperability between IPv4 and IPv6 [3]. IPv4-IPv6 transition and coexistence is only possible with techniques like dual stack, translation and tunneling [17]. All the transition mechanism are considered as a set of methods to facilitate a smooth transition to new version IP, unfortunately not all of them are amenable to the users option. The network as a whole can be divided as an access network, distribution network and core network [27].

Access network, Distribution network and Core network comprises of users, Internet Service Provider [5] and Internet respectively. Much attention has been paid to access network when compared to the other two networks [7]. Clearly, most of past researches focus on the end user's need. We anticipate mainly on the scenario in access network as end user. Cisco router plays a vital role in transition [20][21]. There are many routers available such as CISCO, Huawei, D-Link, HP, Juniper, Brocade, Avaya, Telco Systems, ZyXEL. The Scenario Chosen over the Testbed is core network. In Real time CISCO predominantly used in the core segment when compared to the other available routers. Only CISCO can arrange for the platform for campus, division, data centre, and wide-area networks that are exceedingly available while incorporating security at all levels of the network, aiding to ensure the optimized distribution of application and communications, and providing inherent manageability. The market segment of CISCO is Prime associated to others. Also, At the ISP terminal the equipment's used in CISCO, since technologically it's superior in core networks.

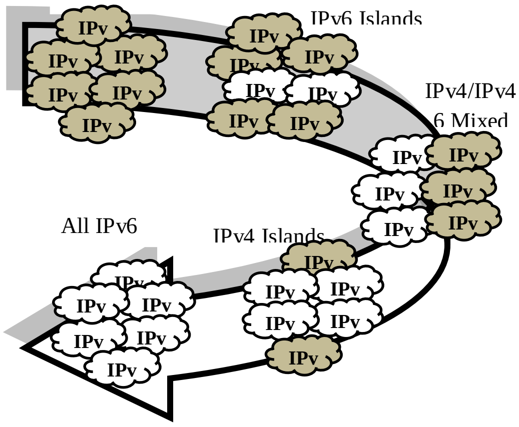


Fig. 1. IPv4-IPv6 Transition Scenarios

In this paper, we proposed Routing Virtualization using a single physical Cisco Router in a real time simulation over a test bed. We have compared the transition techniques at core, access and distribution network. In this paper, our goal is to allow a flexible transition between IPv4 and IPv6 in all kinds of networks having a common Cisco router so to avoid reconfiguration of routers for each transition to take place. The router is actually configured with Dual Stack and virtually configured with Translation and Tunneling techniques [8]. To achieve this goal, we first propose a novel transition scenario which consists of the following networks such as: i) All IPv4, ii) IPv6 Islands, iii) IPv4/IPv6 mixed, iv) IPv4 Islands and v) All IPv6 as shown in Figure 1 [12]. In real time co-existence of IPv4 & IPv6 for every network there cannot be a separate setup for IPv6 clients and IPv4 clients. The cost factor, design implementation complexity and maintenance also increase considerably. For instance, we cannot afford to deploy separate router, server and link for each of the IPv4 and IPv6 users for any particular application. In Routing Virtualization there is no particular need for separates set-up for each of the IP network. We virtually run on over the other which leads to the reduction in cost and complexity.

2 Transition mechanisms

2.1 Dual Stack

Dual stack allows both protocols IPv4 and IPv6 to run alongside one another and have no dependency on each other to function, 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. It supports and ensures any type of communication regardless of the IP version. A dual stack migration strategy makes a transition from core to the edge. This includes enabling two TCP/IP protocol stacks on the WAN core routers. Applications choose between IPv4 and IPv6 based on the response of DNS request. The application selects the correct address based on type of IP traffic as Dual Stack allows hosts to simultaneously reach existing IPv4 content and IPv6 content. The dual stack doubles the communication requirements, which in turns causes performances degradation in spite of it providing flexible adaptation strategy [9]. Dual stack techniques are appreciable for an access network and not appropriate for a core network and distributed network. Dual stack networking is one of several solutions for migrating from IPv4 to IPv6, but it is also one of the most expensive techniques [16]. It doubles the communication requirements, which in turn causes performance degradation. Dual stack is the foundational and preferred IPv4to IPv6 transition mechanism [18].

2.2 NAT64

Network Address Translation (NAT) operates on the router to connect two networks together. It makes the router function as an agent between the private or (“Inside”) and the public, internet or (“Outside”). Translation mechanisms are either stateless or stateful. NAT64 translates IPv6 packets into IPv4 packets and vice versa. It has essentially two components, the address translation mechanism and protocol translation mechanism [4]. NAT64 allows a small number of public IP address to be shared by a large number of host using private network. Also provides security benefits by making hosts more difficult to address directly by foreign machines on the public Internet [28]. NAT64 creates the mappings by using as IPv6 prefix (denoted as prefix 64::/n) as the IPv6 address pool [14]. Each Ipv4 address is mapped into a different address by concatenating the prefix 64::/n with the IPv4 address being mapped and, if ‘n’ is less than 96, padding the result to 128 bits with a suffix of zero bits [11] [13].

NAT has serious drawbacks in terms of the quality of internet connectivity and requires careful attention in its implementation. The translation methods have been devised to alleviate the issues encountered. NAT is highly complex along with performance reduction and lack of public addresses. Address, Port substitution, TCP/UDP checksum recomputing, application layer translation and IP/ICMP protocol translation are all required to accomplish proper translation [24]. Both stateful and stateless translation mechanisms are highly unscalable [19].

2.3 6to4/4to6 Tunneling

The 6to4/4to6 Tunneling is the technique that permits IPv6 packets to be transmitted over an IPv4 network and vice versa [1]. Tunneling can take place between two routers, two hosts, router and a host. The 6to4 mechanism operates by having the IPv4 address of the router’s IPv4 interface be a portion of the prefix of the IPv6 addresses assigned to the IPv6 host in the respective IPv6 domain. When a tunnel is configured manually, it is quite possible that a tunnel do not always take an optimal path between sites, where one Ipv6 hop may span many Ipv4 hops. Whereas automatic tunnel such as 6to4 tunnel routes the Ipv6 traffic over Ipv4 tunnels by the most efficient Ipv4 path between two 6to4 gateways. Automatic tunneling originates in the 6to4/4to6 edge router and IPv6/IPv4 is the subnet technology. 6to4 is especially relevant during the initial phases of deployment to full, native IPv6 connectivity, since IPv6 is not required on nodes between the host and the destination. However, it is intended only as a transition mechanism and is not meant to be used permanently. 6to4 may be used by an individual host, or by a local IPv6 network. When used by a host, it must have a global IPv4 address connected, and the host is responsible for encapsulation of outgoing IPv6 packets and decapsulation of incoming 6to4 packets. If the host is configured to forward packets for other clients, often a local network, it is then a router [6]. Due to encryption and decryption, the CPU utilization is high. Fragmentation issue also arises. Time to live also increases due to processing delay. Apart from the 6to4/4to6 tunnel, we have Generic Routing Encapsulation Tunnel, Automatic Tunnel, Manually Configured Tunnel, Tunnel Broker, Intra-Site Automatic Tunnel Addressing Protocol Tunnels, IPv6 over IPv4 Tunnel, IPv6 in IPv4 Tunnel and IPv6 Rapid Development Tunnel [23].

3 Routing Virtualization for IPv4-IPv6 Coexistence

A number of transition mechanisms such as Dual stack, Translation and Tunneling Mechanisms have been developed to support the interoperability between IPv4 and IPv6 during the time of migration from the existing IP version (IPv4) to the new IP version (IPv6). But not all transition can place in one common router [15]. These individual mechanisms do not provide a complete transitioning solution. Both infrastructural and economic factors play a vital part in forming a complete solution. Routing Virtualization (RV) provides a feasible solution to meet the above requirements and to achieve IPv4-IPv6 coexistence without deploying additional hardware. The technology is appropriate to support three transition techniques within one router. In this application environment, IPv4 and IPv6 are identical for data forwarding. As for addressing and routing, as well as operations, administration, and maintenance (OAM), they must be treated differently and independently.

Much of this work involve a return to simplicity and ease of use with as little disruption the existing networks as possible. Routing Virtualization can provide the proper level of usage of a single Cisco router for all the transition techniques. As a result, end-to-end connectivity along with scalability can be built, as long as two communication ends join the homogeneous virtual networks which are globally interconnected. In general, the routing virtualization for IPv4-IPv6 coexistence will depend heavily on the capability of the virtual routing for the two transition techniques. As a result, the global interconnectivities of both the virtual routing and actual routing are only achieved by a single router so as to avoid repeated router reconfiguration and additional router deployment. This method will significantly improve network cost efficiency, scalability and routing overheads. As users gradually transits to IPv6, they will need ways to interact with the existing IPv4 networks. NAT (Network Address Translation) boxes could translate from one protocol to another. In addition, tunneling servers could be permitted to encapsulate IPv6 packets within IPv4 packets for transmission across IPv4 networks. Mobile users could also connect directly to an IPv6 server.

4 Testbed Setup Descriptions

The transition between the IPv4 Internet today and IPv6 Internet will be a long process during both protocols coexists and also it is unreasonable to expect that many millions of IPv4 nodes will be converted overnight. Testbed is a platform on which an assortment of experimental tools and products that may be deployed and are allowed to interact in real-time. Successful tools and products are identified and are developed in an interface in order to have a successful testing. The testbed created for Routing Virtualization proves high scalability and reachability.

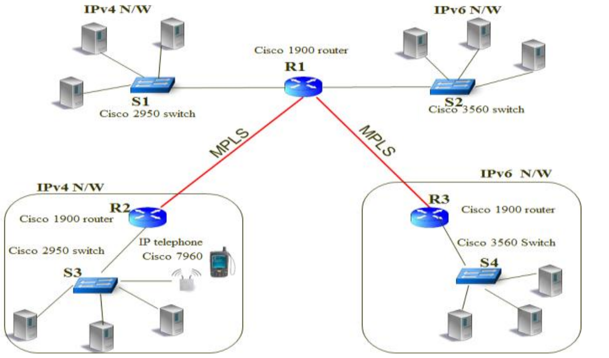


Fig. 2. Scenario designed and implemented

The configuration of the testbed consists of four networks, two IPv4 networks and two IPv6 networks. There are about 12 nodes connected with two Cisco 2950 switches (S1 and S2) and two Cisco 3560 switches (S3 and S4). Switch S1 and S2 are connected with Router R1. S3 switch is connected with router R2. IP telephone Cisco 7960 is connected with switch S3. The Router IOS supports different version types such as data, security, video, advanced security services, basic, voice etc. The Cisco 1900 routers are used in our testbed which it supports the basic Router IOS. R2 and R3 are connected with R1 via MPLS. R3, Cisco 1900 router is actually configured as Dual stack and virtually configured as NAT and 6to4/4to6 tunneling. Routers are needed to be configured again and again for any of the transition. In routing virtualization, router interfaces need not be changed for each transition. Addition of network does not cause change in base configuration of core network.

Setting up a native IPv6 router involves: Step 1: Installing the router operating system, Step 2: Configuration and Step 3: Running the Script

The communication takes place between all the networks via the R1 router. Depending upon the transmission, the transition takes place. The generic network setup for the experiments is shown in Figure 3. The figure shows the real time simulation that has been done using packet tracer 6.0.1 which is a real time simulator.

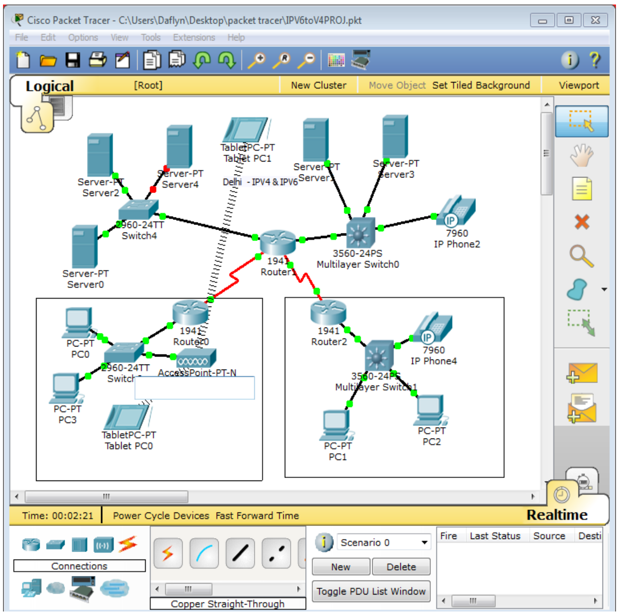
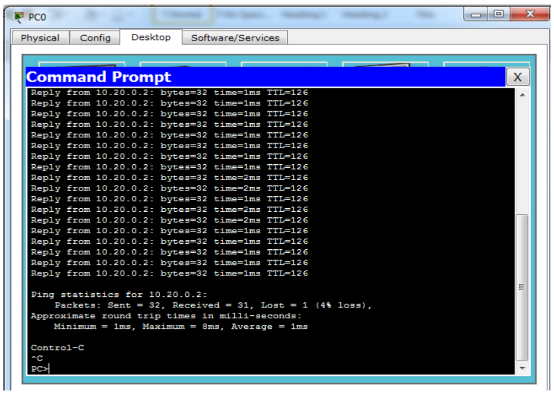


Fig. 3. Routing Virtualization architecture using Real Time Simulation with Packet Tracer 6.0.1

The pinging of one node from one network to another is shown in figure 4. All the data packets sent from one endpoint to other endpoint via a common router which allows all three transition techniques. For the proposed network that works with routing virtualization allows addition of network without any downtime. The experiments were conducted by passing different types of traffic through the four networks via a common router which is actually configured as a Dual stack but virtually as NAT64 and 4to6/6to4 Tunneling technique.



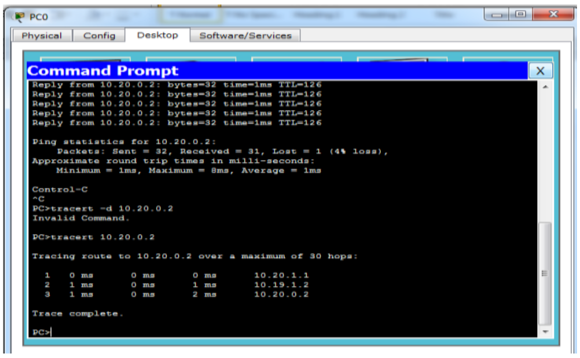
```
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=2ms TTL=126
Reply from 10.20.0.2: bytes=32 time=2ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=2ms TTL=126
Reply from 10.20.0.2: bytes=32 time=2ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126

Ping statistics for 10.20.0.2:
    Packets: Sent = 32, Received = 31, Lost = 1 (4% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 8ms, Average = 1ms

Control-C
^C
PC>
```

Fig. 4. Command Prompt: Ping Statistics

Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the targets and wait for an ICMP response. In the process it measures the time from transition to reception (round trip time) and records any packet loss. The response can be a successful response, slower response or a failed response. Figure 4 and Figure 5 Shows the end to end pinging response and trace route command prompt in which the TTL, bytes, trace route and reply from the destination node is obtained. The ping statistics for each node is also obtained which includes the total number of packets sent, received and packets lost. The throughput is calculated having all these parameters.



```
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126
Reply from 10.20.0.2: bytes=32 time=1ms TTL=126

Ping statistics for 10.20.0.2:
    Packets: Sent = 32, Received = 31, Lost = 1 (4% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 8ms, Average = 1ms

Control-C
^C
PC>tracert -d 10.20.0.2
Invalid Command.

PC>tracert 10.20.0.2

Tracing route to 10.20.0.2 over a maximum of 30 hops:

  1   0 ms     0 ms     0 ms     10.20.1.1
  2   1 ms     0 ms     1 ms     10.19.1.2
  3   1 ms     0 ms     2 ms     10.20.0.2

Trace complete.

PC>
```

Fig. 5. Command Prompt: Tracing Route

5 Performance Comparisons

The real time simulation for Routing Virtualization over a testbed illustrates that Routing Virtualization identifies it to be highly scalable and reachable. Having a common Cisco router for all three transitions avoids reconfiguration of routers for each transition that needs to take place. The router is actually configured with Dual Stack and virtually configured with Translation and Tunneling techniques. Table 1 below highlights the comparison of network and router performance parameters between the various transition techniques. Latency is high for NAT64 and low for 6to4/4to6 tunneling technique. For a load balance, External appliances is required for Dual stack technique, Hardware is required for NAT64 and can be configured for 6to4/4to6 tunneling technique. 6to4/4to6 tunneling provides high security whereas dual stack provides a medium security. Security forensic is most preferred for dual stack, medium for NAT64 and low for 6to4/4to6 tunneling technique. The performances are measured by the evaluating the data obtained in the testbed. Both the Core router RAM utilization and Core Router CPU utilization are low for the Dual stack technique and high for the 6to4/4to6 tunneling technique. Both endpoint RAM utilization and endpoint CPU utilization have been found to be very low for Dual stack technique and very high for the NAT technique. Non Volatile RAM requirement is very high for 6to4/4to6 tunneling technique. Throughput of End Router in 6to4/4to6 tunneling is very low related to dual stack also low related to NAT64. Core Router's RAM utilization, CPU utilization and temperature are low for dual stack technique when compared to the other two techniques. Performance issues like Throughput, End-to End Delay and Jitter are discussed.

Table 1. Comparison between Transition Techniques: Network and Router Performance parameters

	Performance Parameters	**Dual Stack Technique**	**NAT64 Technique**	**6to4/4to6 Tunneling Technique**
Network Performance	IPv4 and IPv6	Both needed	Either or can be converted	Either or can be tunnelled
	Latency	Medium	High	Low
	Load balance	External appliance required	Hardware required	Can be configured
	Over head	High	Very high	Low
	Security	Medium	High	Very high

	Security forensic	Most preferred	Medium	Low
Router Performance Parameter	Core Router RAM Utilization	Low	Medium	High
	Core Router CPU utilization	Low	Medium	High
	Core Router temperature	Low	Increases	Increases
	Endpoint Router RAM utilization	Very Low	Very high	High
	Endpoint Router CPU utilization	Very Low	Very high	High
	Endpoint Router Temperature	Very Low	Very high	High
	NV-RAM requirement	Low	High	Very High
	Throughput of End router	Not Applicable	Low	Very low related to DS also low related to NAT64
	Throughput of core router	High	High related to tunneling	Low

6 Real Time Simulation Analyses

6.1 Throughput Analysis

Throughput is the number of packets successfully delivered per unit time. Throughput is controlled by available bandwidth, as well as the available signal-to-noise ratio and hardware limitations (CPU, RAM). We measured the throughput performance metric in order to find out the rate of received and processed data at the intermediate device (i.e. Router) during the simulation time period. The throughput is calculated from the formula:

$$T_i = [{}^{P_i}/_{L_i}] \qquad (1)$$

For [i=1, 2, 3…n]

Where, T_i is denoted as the Throughput, P_i is the Packet per Network; L_i is the Latency per Network, i is the Data packets and N is the Total number of the packets in the network. The variations in the total number of packets in the network are proportional to the throughput. The throughput for different packets per network was calculated using the formula below

$$T_i = [{}^{P_1}/_{L_1} + {}^{P_2}/_{L_2} + {}^{P_3}/_{L_3} + \cdots + {}^{P_N}/_{L_N}] \qquad (2)$$

The threshold Limit taken in the testbed is taken about: 90% of Link utilization, 75% of CPU utilization and 75% of RAM utilization.

We have set up the CPU and RAM utilization threshold as 75% since there is every chance that the Router as a whole goes down. In order to ensure the continuity of service we have set the limits lower.

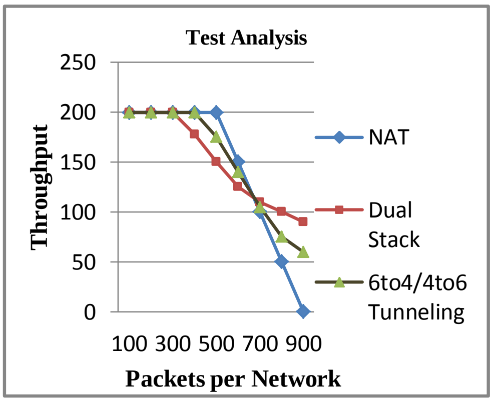


Fig. 6. Test Analysis

Figure 6 shows the test analysis graph. The throughput is constant until the CPU utilization is 75% after which it gradually decreases. Also at the same time throughput is constant until the RAM utilization is 75% after which it gradually decreases. When the data load keeps on increasing, upto a particular limit based on the capacity of the link, throughput is normal. Beyond the threshold limit the performance (throughput) starts decreasing. Similarly when the number of networks keeps on increasing, up to a specific limit the Router CPU takes care normally. Beyond the threshold limit the performance (throughput) starts decreasing, since the processing load on the CPU increases. Also when the number of networks keeps on increasing, up to a particular limit the Router CPU works steadily normally also as the complexity of the configuration increases the RAM utilization increases. Beyond the threshold limit the performance (throughput) starts decreasing, since the load on the CPU increases.

6.2 Round Trip Time Analysis

In addition to the throughput, we have observed the Round Trip Time (RTT); it is the response time to identify the quality-of service experienced by the nodes sin IPv6 and IPv4 networks. All nodes on different networks have been involved by means of sending and receiving the ICMP or ICMPv6 packets to each other.

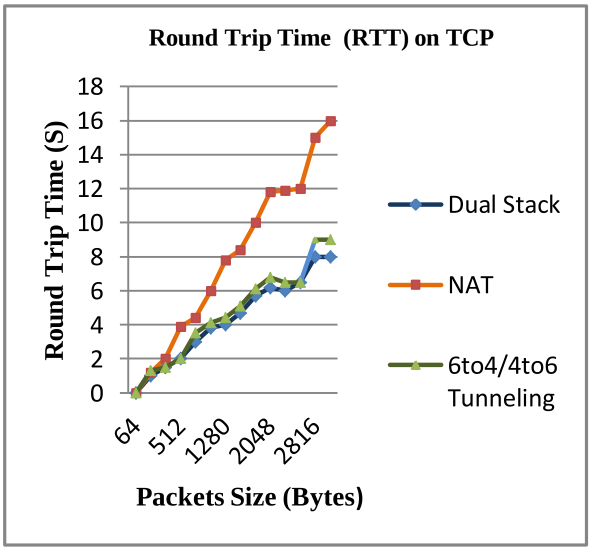


Fig. 7. Round Trip Time (RTT) on TCP

The RTT depends on many factors like load at the particular moment of time, Router processor availability and number of virtual routers that are established at that particular point of time. As the complexity of congestion and load increases, the RTT decreases proportionally. With the RTT we can also have a clear idea about the end-to-end cloud loop communication. The RTT is also known as a Ping time and according to [21], next RTT can be defined by the following calculation.

$$RTT_{next} = (a * RTT_{old}) + ((1 - a) * RTT_{new}) \quad (3)$$

Where, a is the smoothing factor (value between 0 and 1).

Figure 7 shows the Round Trip Time (RTT) on TCP graph. The RTT is first determined with no load after checking the end to end connectivity. RTT is checked for all the three transition techniques: Dual stack, Translation and Tunneling. The RTT is low in case of Dual Stack. The RTT is higher in Tunneling when compared to that of the Dual Stack. Since, the tunnel runs end to end and originates at the source instead of processing in the router at the gateway. In translation the gateway router plays the vital role by allowing the packets to move out of gateway router. Hence the load in the router is doubles the processing load in the other transitions techniques. Hence the RTT is the highest for the translation technique.

6.3 Jitter Analysis

We illustrate the jitter experienced by the network for the various transition mechanisms. The general trend in the plots is that as the number of nodes in the network increases, so does the delay. This phenomenon occurs because of the increasing number of messages exchanged in the network, with increasing number of nodes, for any fixed value k=10%N. *K* is the number of trusted neighbours of an existing IPv4 and IPv6 network and *N* is the total number of nodes operational in the network.

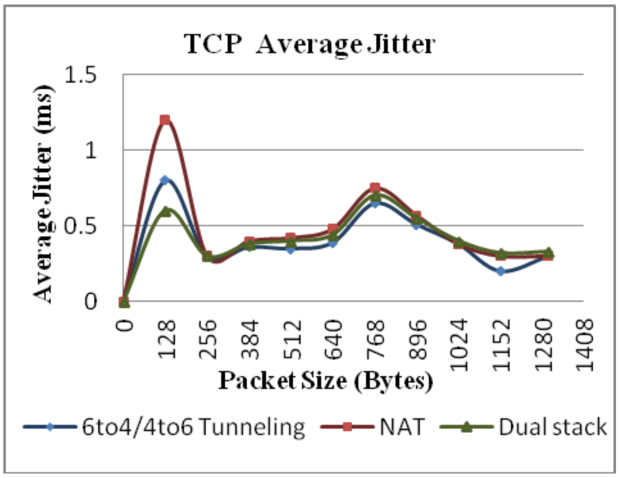


Fig. 8. TCP average Jitter

As the trust values in the messages exchanged in the network increases, the jitter experienced by the messages is less. As a result, the performance of the scheme is seen to improve with increasing values of the trust factor. NAT mechanism has the highest recorded jitter of all the transition mechanisms.

6.4 Latency Analysis

Samples such as 64kb, 128 kb, 256kb, 384kb data are taken and transmitted over the testbed. While testing the data sample 64kb, the time delay was 110kb for Dual stack, 127kb for 6to4/4to6 tunneling and 175kb for NAT. On transmission of data of higher packet size the latency increased for all the three transition mechanisms as shown in figure 9. Though the delay was increased by smaller fractions in Dual stack, in Tunneling the time delay increased linearly after 256kbps and it was almost equal to the time delay of the NAT Network. The performance of NAT Network decreased above loads of 512 kbps. There was a major delay in the packet being delivered to the end points. The graph clearly depicts that the performance of tunneling and NAT decreases drastically on transmission of packets of higher data rates. During Routing Virtualization the tunneling end points outperforms the NAT in the latency.

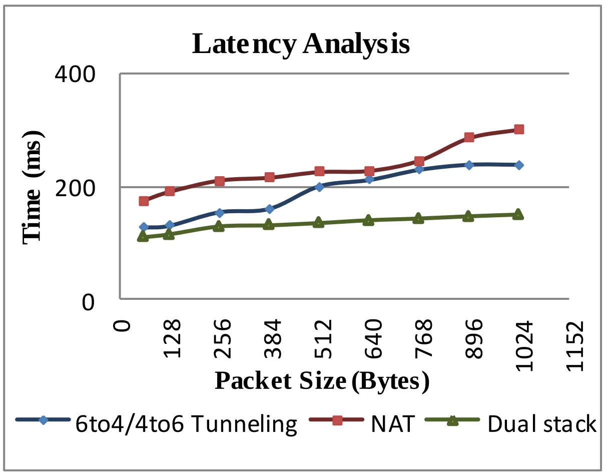


Fig. 9. Latency Analysis

6.5 Loss Rate Analysis

In the loss rate analysis, the packet size was increased to measure the corresponding change in the loss rate. Some packets are successfully sent from the client to the server via several network nodes or routers, and some packets are lost unexpectedly reasons. In Figure 10, loss rates analysis for datagram packet size of Nx64 are taken as the samples and transmitted over the testbed.

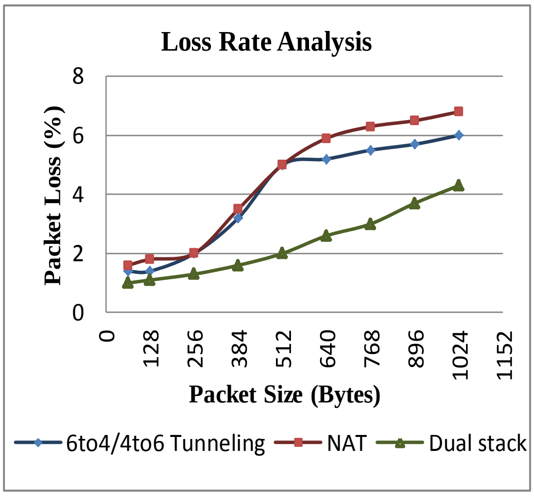


Fig. 10. Loss Rate Analysis

The packet loss is measured in terms of % of packets that are lost. Upto data ratios of 256kbps there was no significant loss in loss of packets. But when the load increased the packet loss (%) increased considerably. when the packet size is 64 bytes, the loss rates of the Dual Stack, 6to4/4to6 Tunnel and NAT are 1.0%, 1.4% and 1.6%, respectively. When the size of the packet is increased to 1024 bytes, these loss rates become 4.4%, 6% and 6.8%. Hence, increasing the packet size increases the loss rate.

7 Conclusions and Future Work

This paper describes Testbed for Routing Virtualization over a Real time Simulator for IPv4-IPv6 coexistence for various IPv4-IPv6 transition techniques such as Dual stack, NAT and 6to4/4to6 Tunneling. We have achieved a transmission of packets between two different networks by having a common Cisco router so as to avoid reconfiguration of routers for each transition to take place. The router was actually configured with Dual Stack and virtually configured with Translation and Tunneling techniques. Test analysis was also obtained.

In any network, beyond a particular level of addition of networks, the processing speed depends on routers specification of a core network. The blemishes of routing virtualization can be overcome by upgrading the existing router by addition of new routers. The existing and new router must be configured in high availability mode. Between both routers, Hot Standby Router Protocol (HSRP) must be made to run between the routers, after which old router can be removed. HSRP is a Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway. This can be considered as a future work.

References:

[1] Yong Cui, Jiang Dong, Peng Wu, Chris Metz,Yiu L. Lee and Alain Durand , "Tunnel-based IPv6 Transition," *IEEE Internet Computing*, 2013 IEEE.

[2] D.Shalini Punithavathani and K. Sankarnarayanan, "IPv4/IPv6 Transition Mechanism", *European Journal of Scientific Research*, ISSN 1450-216X Vol.34 No. 1 (2009), pp. 110-124.

[3] Arturo Azcorra, "Integrated Routing and Addressing for Improved IPv4 and IPv6 Coexistence", *IEEE Communication Letters*, Vol. 14, No. 5, May 2010.

[4] P. Srisuresh and K. Egevang: "Traditional IP network address translator (Traditional NAT)", *RFC3022*, IETF Jan 2001.

[5] Li Zimu, Peng Wei and Liu Yujun, "An innovative IPv4-IPv6 Transition Way for Internet Service Provider", *2012 IEEE*

symposium on Robotics and Application (ISRA).

[6] Ra'ed AlJa'afreh, John Mellor and IRfan Awan, "A Comparison between the Tunneling process and mapping schemes for IPv4/IPv6 Transition", 2009 *International Conference on Advanced Information Networking and application workshop*.

[7] Jayanthi, J. Gnana, and S. Albert Rabara. "IPv6 addressing architecture in IPv4 network." In *Communication Software and Networks, 2010. ICCSN'10. Second International Conference on*, pp. 461-465. IEEE, 2010.

[8] Mohd.Khairil Sailan, Rosilah Hassan and Ahamed Patel, "A Comparative Review of IPv4 and IPv6 for research Test Bed", 2009 *International Conference on Electrical Engineering and Informatics*, 5-7 August 2009, Selangor, Malaysia.

[9] Yingjiao Wu and Xiaoqing Zhou, "Research on the IPv6 Performance Analysis Based on Dual-Stack and Tunnel Transition." The 6th *International Conference on Computer Science & Education*, August 3-5, 2011.SuperStar Virgo, Singapore.

[10] Ruri Hiromi and Hideaki Yoshifuji," Problem on IPv4-IPv6 Transition", *Proceedings of International Symposium on Application and the Internet Workshops*, 2005.

[11] Yu Zhai, Congxiao Bao, Xing Li, "Transition from IPv4 to *IPv6: A translation Approach" 2011 sixth IEEE International Conference on Networking, Architecture, and storage*.

[12] Cisco,"IPv6 Assessment and migrations Services," *Whitepaper*, 2005.

[13] G.Tsirtsis and P. Srisuresh, Network Address Translation- Protocol Translation (NAT-PT), *IETF RFC 2766*, Feb.2000: www.ietf.org/rfc/rfc2766.txt

[14] E.Nordmark and R.Giligan, Basic transition mechanism for IPv6 Hosts and routers, *IETF RFC 4213*, October 2005: www.ietf.org/rfc/rfc4213.txt

[15] Jivika Govil , Jivesh Govil , Navkeerat Kaur , Harkeerat Kaur , "An Examination of IPv4 and IPv6 Networks: Constraints and various transition mechanism" *Southeastcon,2008.IEEE*, 3-6 April 2008, Page(s): 178 - 185

[16] G.Tsirtsis, P. Srisuresh," Network Address Translation –Protocol Translation (NAT-PT)", *IETF RFC2766*, Feb.2000. [online] Available:http://tools.ietf.org/html/rfc2766.

[17] IETF IPv6 Transition Working Group, http//www.6bone.net/ngtrans.

[18] A.Durand et al., "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaution," *IETF RFC6333*, August 2011.

[19] C.Aoun, E.Davies, "Reasons to Move the Network Address Translator-Protocol Translator (NAT-PT) to Historic Status," *IETF RFC4966*, July 2007.

[20] C.Popoviciu, E. Levy-Abegnoli, and P. Grossetete, Deploying IPv6 Network. Cisco Press, 2006.

[21] Cisco System, The ABCs of IP Version 6, Technical Report. Cisco IOS Learning Services, Cisco System. Available athttp:/www.cisco.com/wrap/public/732/abc/docs/abcIPv6.pdf, 2002.

[22] Arkko, Jari, and Fred Baker. "Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment." (2011).

[23] Cui, Yong, Jiang Dong, Peng Wu, Jianping Wu, Chris Metz, Yiu L. Lee, and Alain Durand. "Tunnel-based IPv6 transition." *Internet Computing, IEEE* 17, no. 2 (2013): 62-68.

[24] Bagnulo, Marcelo, Alberto García-Martínez, and Iljitsch Van Beijnum. "The NAT64/DNS64 tool suite for IPv6 transition." *Communications Magazine, IEEE* 50.7 (2012): 177-183.

[25] Lou, YaFang, YongBing Xu, and ZhiJun Yuan. "Research and Implementation of smooth transition strategies---IPv6 tunnel technology." In *Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering*. Atlantis Press, 2013.

[26] Wang, Kui Fu, Yan Ge Chen, and Jing Tao Xu. "Research of IPv6 transition technology and its department on campus network." *Advanced Materials Research* 457 (2012): 79-84.

[27] Colitti, Lorenzo, Steinar H. Gunderson, Erik Kline, and Tiziana Refice. "Evaluating IPv6 adoption in the Internet." In *Passive and Active Measurement*, pp. 141-150. Springer Berlin Heidelberg, 2010.

[28] Yu, Se-young, and B. Carpenter. "Measuring IPv4-IPv6 translation techniques." *Computer Science Technical Reports* (2012).