Asian Journal of Information Technology 13 (9): 485-493, 2014
ISSN: 1682-3915
© Medwell Journals, 2014

Real Time Simulation of Routing Virtualization over a Test bed designed for the Various IPv4-IPv6 Transition Techniques

Sheryl Radley and Shalini Punithavathani
Department of CSE, Government College of Engineering, Tirunelveli, India

Abstract: The rapid 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-IPv6. IETF proposes transition techniques which includes dual stack, translation and tunneling. A transition permits 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 researchers have developed a test bed 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 observed 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

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 (Hiromi and Yoshifuji, 2005). 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.

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 (Punithavathani and Sankaranarayanan, 2009). 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. 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 (Azcorra *et al*., 2010). IPv4-IPv6 transition and coexistence is only possible with techniques like dual stack, translation and tunneling. 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.

Access network, distribution network and core network comprises of users, internet service provider

Corresponding Author: Sheryl Radley, Department of CSE, Government College of Engineering, Tirunelveli, India

(Li *et al*., 2012) and internet, respectively. Much attention has been paid to access networkwhen compared to the other two networks (Jayanthi and Rabara, 2010). Clearly, most of past researches focuson the end user's need. researchers anticipate mainly on the scenario in access networkas end user. Cisco router plays a vital role in transition (Popoviciu *et al*., 2006; CISCO, 2002).

In this study, researchers proposed routing virtualization using a single physical Cisco router in a real time simulation over a test bed. Researchers have compared the transition techniques at core, access and distribution network. In this study, the goal is toallow 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 (Sailan *et al*., 2009). To achieve this goal, researchers first propose a novel transition scenario which consists of the following networks such as: all IPv4, IPv6 islands, IPv4/IPv6 mixed, IPv4 Islands and all Ipv6 as shown in Fig. 1 (CISCO, 2005). In real time co-existence of IPv4 and 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 increaseconsiderably. For instance, researchers 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. Researchers virtually run on over the other which leads to the reduction in cost and complexity.

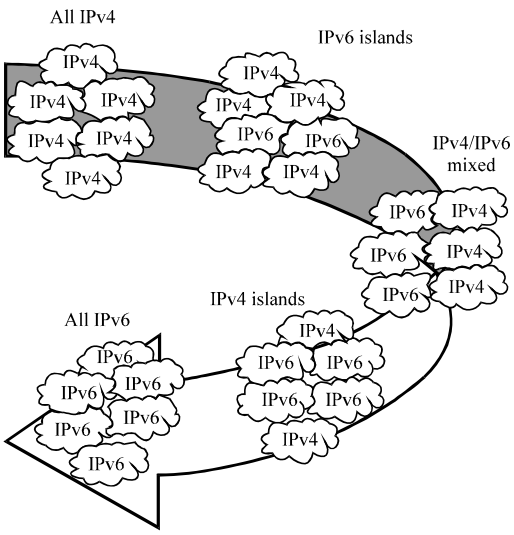

Fig. 1: IPv4-IPv6 transition scenarios

TRANSITION MECHANISMS

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 (Wu and Zhou, 2011) in spite of it providing flexible adaptation strategy. 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-IPv6 but it is also one of the most expensive techniques (Tsirtsis and Srisuresh, 2000). It doubles the communication requirements which in turn causes performance degradation. Dual stack is the foundational and preferred IPv4-IPv6 transition mechanism (Lee *et al*., 2011).

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 (Srisuresh and Egevang, 2001). 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. NAT64 creates the mappings by using as IPv6 prefix (denoted as prefix 64::/n) as the IPv6 address pool (Nordmark and Gilligan, 2005). 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 <96, padding the result to 128 bits with a suffix of 0 bits (Zhai *et al*., 2011; Tsirtsis and Srisuresh, 2000).

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. Both stateful and stateless translation mechanisms are highly unscalable (Aoun and Davies, 2007).

6 to 4/4 to 6 tunneling: A system that allows IPv6 packets to be transmitted over an IPv4 network and vice versa (Cui *et al*., 2013). Tunneling can take place between two routers, two hosts, router and a host. The 6 to 4 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 6 to 4 tunnel routes the IPv6 traffic over IPv4 tunnels by the most efficient IPv4 path between two 6 to 4 gateways. Automatic tunneling originates in the 6 to 4/4 to 6 edge router and IPv6/IPv4 is the subnet technology. The 6 to 4 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. The 6 to 4 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 6 to 4 packets. If the host is configured to forward packets for other clients, often a local network, it is then a router (AlJa'afreh *et al*., 2009). 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 6 to 4/4 to 6 tunnel, researchers have generic routing encapsulation tunnel, automatic tunnel, manually configured tunnel, tunnel broker, intra-site automatic tunnel addressing protocol tunnels, IIPv6 over IPv4 tunnel, IPv6 in IPv4 tunnel and IPv6 rapid development tunnel.

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 (Govil *et al*., 2008). 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 research 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.

TEST BED SETUP DESCRIPTION

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. Test bed 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 ansuccessful testing. The test bed created for routing virtualization proves high scalability and reachability. The configuration of the test bed 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. The S3 switch is connected with router R2. IP telephone Cisco 7960 is connected with switch S3 (Fig. 2).

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 the test bed 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 6 to 4/4 to 6 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
- Step 3: running the script

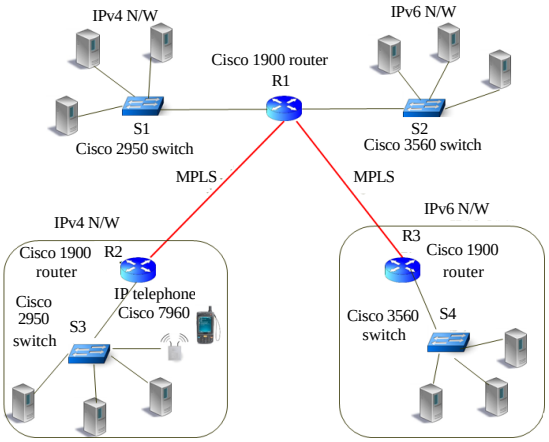

Fig. 2: Scenario designed and implemented

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 Fig. 3. Figure 3 shows the real time simulation that has been done using packet tracer 6.0.1 which is a real time simulator. The pinging of one node from one network to another is shown in Fig. 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 4 to 6/6 to 4 tunneling technique.

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

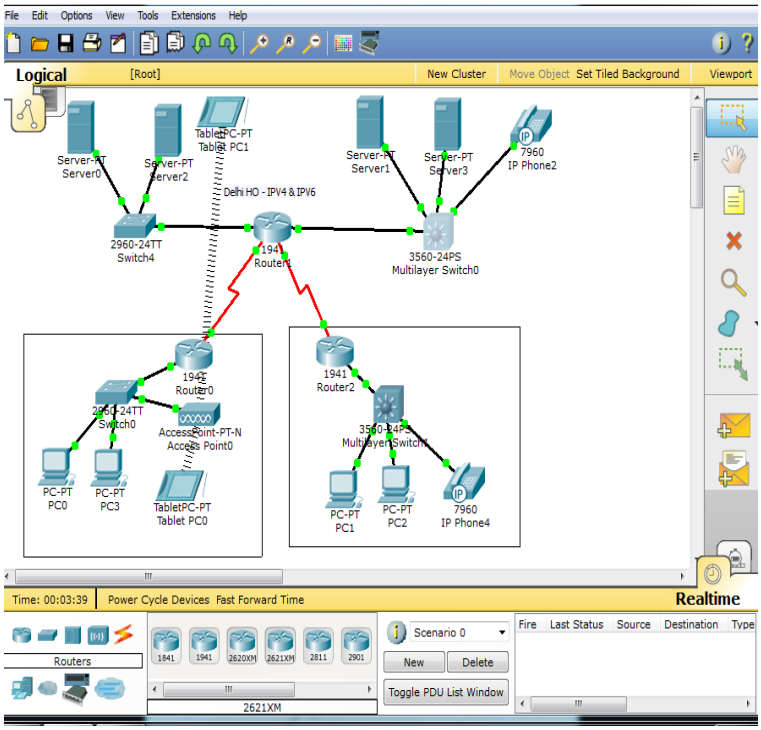

Fig. 3: Routing virtualization architecture using Real Time Simulation with Packet Tracer 6.0.1

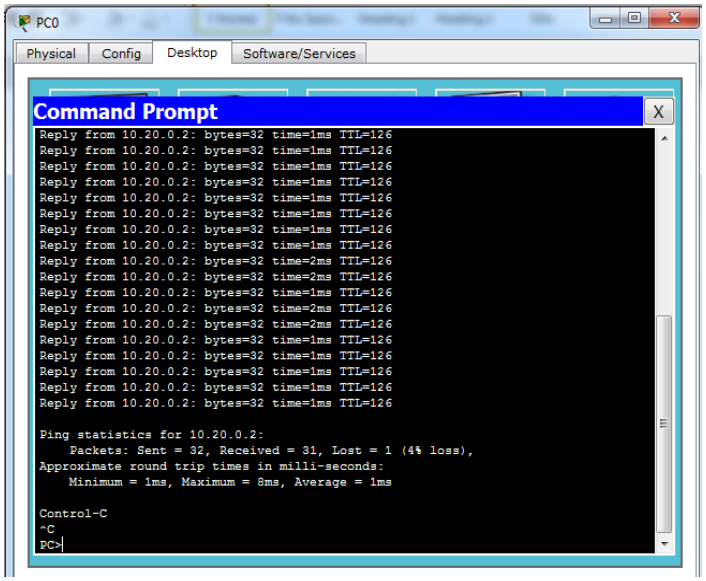

Fig. 4: Command prompt: Ping statistics

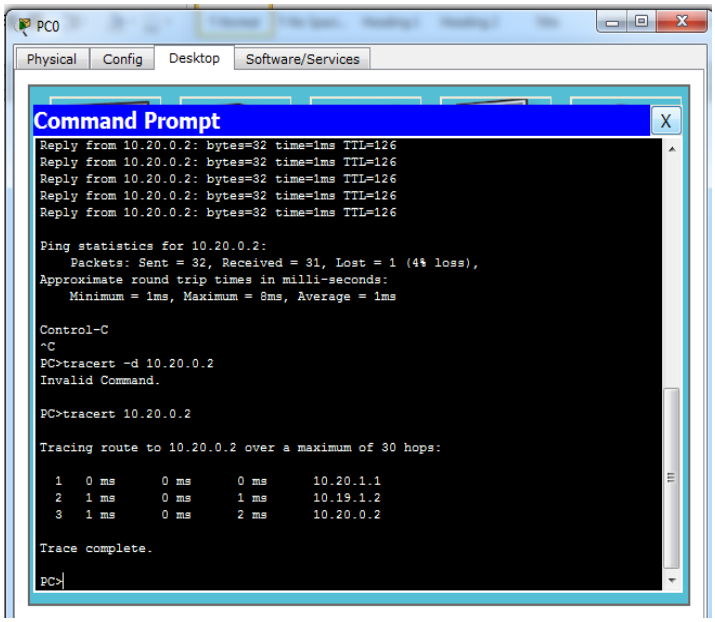

Fig. 5: Command Prompt: Tracing route

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 5 show 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.

PERFORMANCE COMPARISON

The real time simulation for routing virtualization over a test bed 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 highlights the comparison

Table 1: Comparison between transition techniques: network and router performance parameters

Performance parameters	Dual stack technique	NAT64 technique	6 to 4/4 to 6 tunnelingtechnique
Network performance parameters			
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	Highrelated to tunneling	Low

of network and router performance parameters between the various transition techniques. Latency is high for NAT64 and low for 6 to 4/4 to 6 tunneling technique. For a load balance, external appliances is required for dual stack technique, hardware is required for NAT64 and can be configured for 6 to 4/4 to 6 tunneling technique. The 6 to 4/4 to 6 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 6 to 4/4 to 6 tunneling technique. The performances are measured by the evaluating the data obtained in the test bed. Both the core router RAM utilization and core router CPU utilization are low for the dual stack technique and high for the 6 to 4/4 to 6 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 6 to 4/4 to 6 tunneling technique. Throughput of end router in 6 to 4/4-6 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.

REAL TIME SIMULATION ANALYSIS

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). Researchers 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 equation:

$$T_i = \left[\frac{P_i}{L_i}\right], \quad \text{for } i = 1, 2, 3, ..., n \tag{1}$$

Where:

T_i = The throughput
P_i = The packet per network
L_i = The latency per network
I = The data packets and
N = 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 Eq. 2:

$$T_i = \left[\frac{P_1}{L_1} + \frac{P_2}{L_2} + \frac{P_3}{L_3} + ... + \frac{P_N}{L_N}\right] \tag{2}$$

The threshold limit taken in the test bed is taken about:

- 90% of link utilization
- 75% of CPU utilization
- 75% of RAM utilization

Researchers 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, researchers have set the limits lower.

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

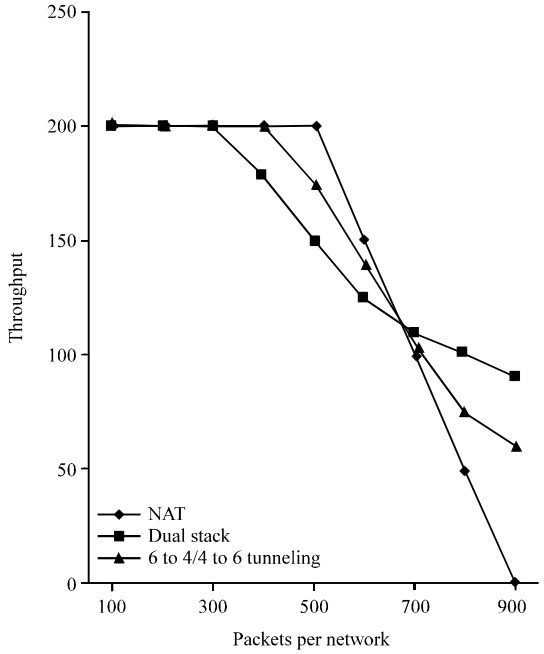

Fig. 6: Test analysis

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, upto 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.

Round trip time analysis: In addition to the throughput, researchers 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.

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 researchers 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 (CISCO, 2002), next RTT can be defined by the following calculation:

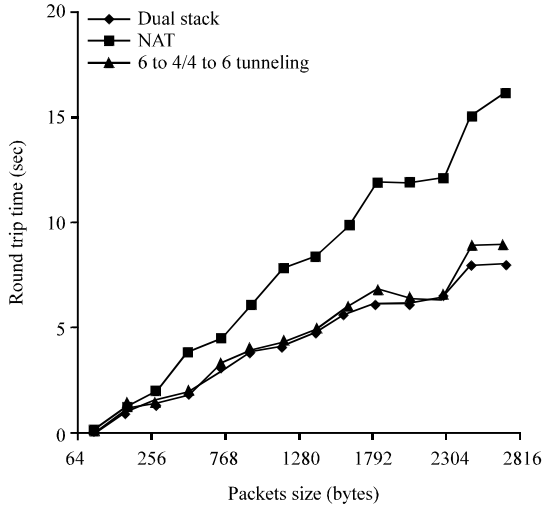

Fig. 7: Round Trip Time (RTT) on TCP

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

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.

Jitter analysis: Researchers 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).

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

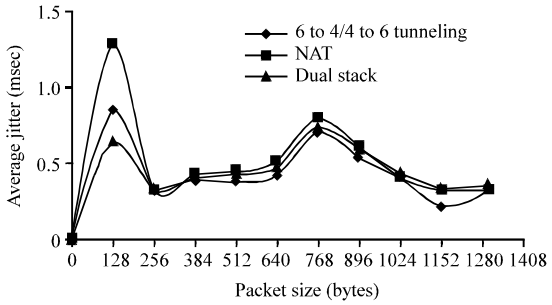

Fig. 8: TCP average jitter

to improve with increasing values of the trust factor. NAT mechanism has the highest recorded jitter of all the transition mechanisms.

CONCLUSION

This study describes test bed for routing virtualization over a real time simulator for IPv4-IPv6 coexistence for various IPv4-IPv6 transition techniques such as dual stack, NAT and 6 to 4/4 to 6 tunneling. Researchers 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 research.

REFERENCES

AlJa'afreh, R.E., J. Mellor and I. Awan, 2009. A comparison between the tunneling process and mapping schemes for IPv4/IPv6 transition. Proceedings of the International Conference on Advanced Information Networking and Applications Workshops, May 26-29, 2009, Bradford, UK., pp: 601-606.

Aoun, C. and E. Davies, 2007. Reasons to move the Network Address Translator-Protocol Translator (NAT-PT) to historic status. Network Working Group, RFC 4966, July 2007. http://www.hjp.at/doc/rfc/rfc4966.html.

Azcorra, A., M. Kryczka and A. Garcia-Martinez, 2010. Integrated routing and addressing for improved Ipv4 and Ipv6 coexistence. IEEE Commun. Lett., 14: 477-479.

CISCO, 2002. The ABCs of IP version 6: Technical report. CISCO IOS Learning Services, CISCO.

CISCO, 2005. IPv6 assessment and migrations services. http://www.cisco.com/web/strategy/docs/gov/IPv6_Services_DS.pdf.

Cui, Y., J. Dong, P. Wu, J. Wu, C. Metz, Y.L. Lee and A. Durand, 2013. Tunnel-based IPv6 transition. IEEE Internet Comput., 17: 62-68.

Govil, J., J. Govil, N. Kaur and H. Kaur, 2008. An examination of IPv4 and IPv6 networks: Constraints and various transition mechanisms. Proceedings of the IEEE Conference on Southeastcon, April 3-6, 2008, Huntsville, AL., USA., pp: 178-185.

Hiromi, R. and H. Yoshifuji, 2005. Problem on IPv4-IPv6 transition. Proceedings of International Symposium on Application and the Internet Workshops, January 31-February 4, 2005, Trento, Italy.

Jayanthi, J.G. and S.A. Rabara, 2010. IPv6 addressing architecture in IPv4 network. Proceedings of the 2nd International Conference on Communication Software and Networks, February 26-28, 2010, Singapore, pp: 461-465.

Lee, Y., A. Durand, J. Woodyatt and R. Droms, 2011. Dual-stack lite broadband deployments following Ipv4 exhaustion. Internet Engineering Task Force (IETF). Request for Comments: 6333, August 2011.

Li, Z., W. Peng and Y. Liu, 2012. An innovative Ipv4-ipv6 transition way for Internet service provider. Proceedings of the IEEE Symposium on Robotics and Applications, June 3-5, 2012, Kuala Lumpur, Malaysia, pp: 672-675.

Nordmark, E. and R. Gilligan, 2005. Basic transition mechanisms for IPv6 hosts and routers. RFC 4213, October 2005. http://tools.ietf.org/html/rfc4213.

Popoviciu, C., E. Levy-Avegnoli and P. Grossetete, 2006. Deploying IPv6 Networks. Cisco Press, Indianapolis, IN., USA.

Punithavathani, D.S. and K. Sankaranarayanan, 2009. Ipv4/IPv6 transition mechanisms. Eur. J. Sci. Res., 34: 110-124.

Sailan, M.K., R. Hassan and A. Patel, 2009. A comparative review of IPv4 and IPv6 for research test bed. Proceedings of the International Conference on Electrical Engineering and Informatics, Volume 2, August 5-7, 2009, Selangor, Malaysia, pp: 427-433.

Srisuresh, P. and K. Egevang, 2001. RFC 3022-Traditional IP network address translator (Traditional NAT). http://portal.acm.org/citation.cfm?id=RFC3022.

Tsirtsis, G. and P. Srisuresh, 2000. Network address translation-protocol translation (NAT-PT). RFC 2766, Internet Engineering Task Force.

Wu, Y. and X. Zhou, 2011. Research on the IPv6 performance analysis based on dual-protocol stack and tunnel transition. Proceedings of the 6th International Conference on Computer Science and Education, August 3-5, 2011, Singapore, pp: 1091-1093.

Zhai, Y., C. Bao and X. Li, 2011. Transition from IPv4 to IPv6: A translation approach. Proceedings of the 6th IEEE International Conference on Networking, Architecture and Storage, July 28-30, 2011, Dalian, China, pp: 30-39.