Asian Journal of Information Technology 15 (7): 1193-1198, 2016
ISSN: 1682-3915

Computational Analysis of Traffic Flow on a Composite network with Multiple Transition Techniques

[1]D. Sivaganesan and [2]Sheryl Radley
[1]Department of CSE/IT, SVS College of Engineering, JP Nagar, Arasampalayam, Coimbatore, India
[2]Department of Computer Science Engineering, Government College of Engineering, Tirunelveli, Tamil Nadu, India

Abstract: IPv6 has interchanged IPv4, the transition rolls out several challenges to the world of internet. The IPv6 transition techniques turn out to be immature holding back the improvement of the next-generation Internet. Hence, IPv4-IPv6 coexistence is becoming increasingly imminent. There is indeed noscenario where all three transition techniques are used together. We proposed a scenario having three techniques overseen by a decision making device, Port Dependent Decision Device (P3D). The proposed device overcomes the difficulties by helping the input from any network to choose the transition technique with the help of the port number. The transition techniques like dual stack, NAT and tunneling is converged into a single router.

Key words: IPv4, IPv6, network services, dual stack, tunneling and translation

INTRODUCTION

The IPv4 address is facing a series of encounters which includes the shortage of address, routing scalability and so on. In order to overcome the difficulties faced by the IPv4, IPv6 was announced and established as the essential network protocol for the next generation internet. IPv6 overcomes the IPv4 by having a larger address space, feasibility of hierarchical addressing and routing, improved forwarding efficiency, mobility support. Since, both IPv4 and IPv6 are incompatible in design, their coexistence of two protocols in the same will pose umpteen numbers of challenges (Durand, 2001). There is no proper communication between IPv4 network and an IPv6 directly, therefore the network operators are essential to run two independent networks on the similar infrastructure by retaining dedicated addressing schema, network routing and data forwarding for each IP protocol (McFarland *et al*., 2011). Despite the network complexity end-to-end connectivity must be preserved; a user must be able to access internet service regardless of which IP protocol is used underneath (Phu *et al*., 2012). From the network perspective, following the end-to-end arguments, the network ought to be simple and complex functions should be left to end users. Three transiton techniques are generally focus upon; dual stack (Durand *et al*., 2011), translation and tunneling (Punithavathani and Sankaranarayanan, 2009; Govil *et al*., 2008). Tunneing transition techniques includes umpteen number of techniques. The study focuses on the various network services that exist. Some of them are File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Telecommunication Network/Terminal Emulation Link Network (TELNET), Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SHH), Real-time Transport Protocol (RTP), Video On Demand (VOD), Simple Network Management Protocol (SNMP), Simple Mail Transfer Protocol (SMTP), SSH File Transfer Protocol (SFTP) and Voice over Internet Protocol (VoIP).

Network services: Network services play a vital role. The service along witheir port number is shown in Table 1. The network file service is used to allow groups of people to share documents via the network. It also helps in providing transparent access to remote resources on the network such as the files. The trivial file transfer is an easy version of FTP that lacks the authentication services FTP offers and depends on UDP rather than TCP for data transport. TELNET is a network protocol that has been used on the internet or LAN in order to provide bidirectional interactive text oriented communication facility using a virtual terminal connection. The implementation of TELNET has no authentication that would the ensure

Table 1: Service with their port number

Dual stack	Port no	NAT64	Port no	Teredo tunneling	Port no
TELNET	23	HTTP	80	FTP	21
HTTPS	443	SMTP	25	TFTP	69
SSH	22	RTP	5004	SNMP	161
SFTP	22	VOD	554	VoIP	5060

Corresponding Author: D. Sivaganesan, Department of CSE/IT, SVS College of Engineering, JP Nagar, Arasampalayam, Coimbatore, India

communication is carried out amongst the two chosen hosts and not interrupted in the middle. The HTTP is a fundamental application protocol used by the world wide web for distributed collaborative, hypermedia information systems, hence it is known as the foundation of data communication for the world wide web. The protocol deeply defines how the messages that are to be sent are formatted and transmitted along with the needed actions that are provided by the web servers and browsers.

SSH is a cryptographic network protocol for a secure data communication, remote command line login as well as execution and other secure network services between devices in two networks. SSH connects using a secured channel over an unsafe network, a server and a client running SSH server and SSH client programs,respectively. Television uses video on demand. SNMP is an internet-standard protocol for managing various devices on IP networks.

Devices such as router, switches, servers, modem, printers and more support SNMP. It is used to monitor network attached devices in network management. SMTP is an internet standard used for electronic-mail (E-mail) transmission. SFTP is a designed network protocol that provides file access, file transfer, file management by the IETF working group. VoIP is a technology that is used for voice communications and multimedia sessions over Internet Protocol networks.

MATERIALS AND METHODS

Port dependent decision device (P3D): Two networks, network A and B, both comprising of network Ipv4/6 are connected to the deciding device 'A' and 'B' respectively which is known as the Port Dependent Decision Device (P3D). Each network has N number of nodes that work on different applications.The three transition techniques of IPv4 and Ipv6 (Colitti *et al*., 2010) between the P3D. Based on the decision of the P3D, the best transition technique is chosen. P3D which acts as a decisive device is the device which stores the updated availability of nodes in the network by repeated ICMP polling. It also helps the input to choose the transition technique with the help of the port number. It will also communicate with the network on the other hand and will have the updated details of the destination node.

The P3D will have the updated details of the endpoints which are behind the source and destination router. When a packet is transmitted to the destination network which is not alive, it will not be transmitted. This will prevent congestion and packet loss. Once the packet enters the P3D, the address length is checked and verified. If the length of the address is of 32 bits, the packet is considered as an IPv4 packet and if the length of the address is of 128 bits, the packet is considered as an IPV6 packet. The packet is then checked for destination address in the header. If the destination node lies in the IPv4 network, the availability is checked in the table. Only if the node is available the packet is transmitted or else the packet is dropped. In the same manner if the destination node lies in the IPv6 network then the flow label, traffic class is checked in the IPv6 packet header as shown in Fig. 1.

The flow label is originally created for giving a special service to the real time application. The flow identification is used for umpteen numbers of controls, one of which is the priority control. All packets belonging to the same "flow" MUST have the same flow-label value; Flow = {src_ip, dst_ip, protocol, src_port, dst_port}. Only if flow-label = 0, a router may set a (non-unique, stateless)

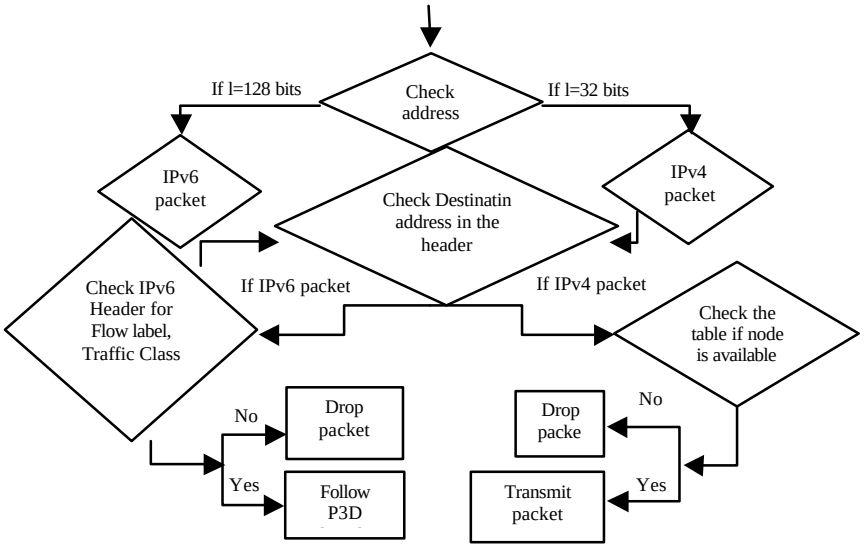

Fig. 1: Flow diagram of Port Dependent Decision Device (P3D) algorithm

originated by that upper-layer protocol. The default value must be zero for all of the 8 bits. Once, the packets are sent to the router the router inspects the packets, checks the destination address and port number with the port uniformly distributed flow-label value. Once set to a non-zero value, flow label values are not be changed. Similarly the traffic class bits must be in packets that are dependent decision device and if the acknowledgement is received as per the routing table based on the port number. The router then forwards the packet to the network consisting of the transition mechanisms. Depending upon the services the packets are forwarded to the respective network having appropriate transition mechanism. The packet is then forwarded to the destination.

Port Dependent Decision Device (P3D) algorithm:

Step 1-Availability of the network and device is checked
Step 2-The IP data packet is directed to network router
Step 3-Router inspects the packets, checks destination address and port number with the
Step 4-P3D and if the achkowledgement is received then go to step 4
Step 5-Router forwards the packet to the network where the three transition mechanisms are available. Dual stack, translation and tunneling
Step 6-If the services are TELNET, HTTPS, SSH, SFTP, then the packets are forwarded through Dual Stack
Step 7-If the services are HTTP, SMTP, RTP, VoD then the packets are forwarded through translation
Step 8-If the services are FTP, TFTP, SNMP, VoIP then the packets are forwarded through tunneling technique
Step 9-The packet is then forwarded to the destination network
Step 10-The router checks the availability of the destination node in the deciding device. If yes then go to step 10
The packet is then forwarded to the destination network

Automated routing infrastructure based on Port dependent decision device (P3D): The automated routing Infrastructure comprises of two networks A and B respectively, a device comprising of dual stack mechanism, a device comprising of translation mechanism, a device comprising of tunneling mechanism, two routers and two a Port Dependent Decision Device (P3D) are present in either network. The data packets are transmitted from network A to network B.

The ping command and traceroute commands are used in the GNS3. The traceroute command is used to discover the links along a path. Once, the packets leave the network, there is no control over the path they actually take to reach their destination.The traceroute program depends on TTL field in the IP packet's header.

When a router fails or is misconfigured, a routing loop or a circular path may result which is prevented by the TTL fields. The TTL field prevents packets from remaining on a network indefinitely which are the reason for loop occurrence.

The proposed and designed scenario is shown in Fig. 2. The packets from network 'A' are sent to the router which forwards the packets to P3D depending upon the network service and the required port number. The P3D checks the packet for IPv4 and IPv6. If the packet is IPv4 then P3D directly forwards the packet to the dual stack. If the packet is IPv6, the P3D inspects the packet and checks the port number based on the port number it follows the proposed algorithm.

The P3D is capable of doing the following things: inspecting the packet for IPv4/IPv6, Port number, checking for continuity of all nodes probing through ICMP requests, hence ensuring that for the non available nodes the packets are not being transmitted. Implemented in real time simulator GNS3. The P3D network also fetches the updated routing table and stores it. Hence, in case of router failure the latest updated routing table can be retrieved from the device and restored on the new router. The packet is ultimately sent to the destination network and finally reaches the destination node.

The traffic source to destination flows from the source to router 1 and then to R2 through R3 as shown in Fig. 3. Before reaching R1 and R3 the pcket is checked with P3D which is the decisive device is the device which stores the updated availability of nodes in the network by repeated ICMP polling. It also helps the input to choose the transition technique with the help of the port number. It will also communicate with the network on the other hand and will have the updated details of the destination node. The P3D will have the updated details of the

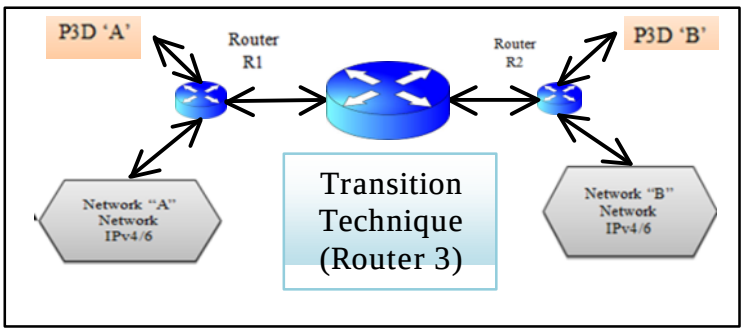

Fig. 2: Automated routing infrastructure built on port dependent decision device scenario

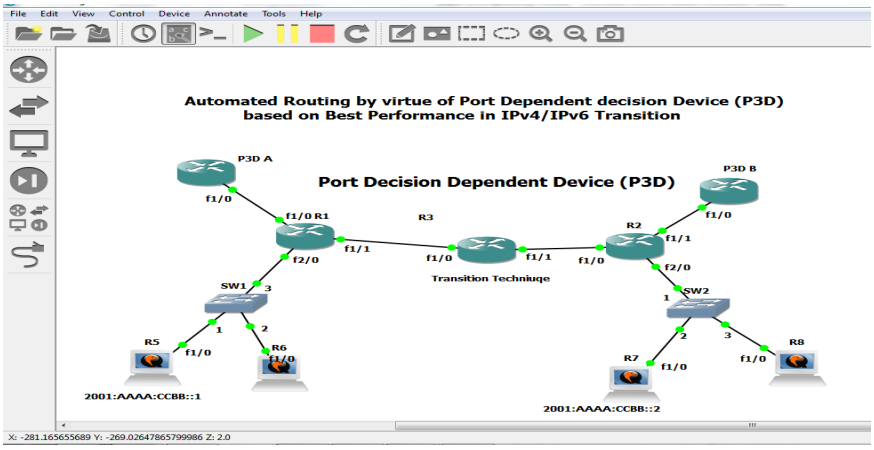

Fig. 3: Automated routing infrastructure built on Port Dependent Decision Device (P3D)

endpoints which are behind the source router and destination router. When a packet is transmitted to the destination network which is not alive, it will not be transmitted. This will prevent congestion and packet loss. Similarly, the command ping 2001: aaaa:ccbb::2 is used to connect source to symmetric network. In order to trace the route by which the packets are sent, the command trace 2001:aaaa:ccbb::2. Though, the tunnel runs over IPv4 network, it is not visible. The weighted pinging response in IPv6 network is obtained by using the command ping 2001:aaaa:ccbb::2 –c (number of times) –l (data size). The output is obtained by sending packets of different size over the network n number of times. The sequence number, time to live and Round trip time is obtained for various packet size.

RESULTS AND DISCUSSION

Real time simulation analysis: The proposed device was analyzed and tested over GNS3, a real time simulator. The throughput, round trip time, latency, loss rate, CPU utilization and end to end delay was analyzed. The throughput which is definedas the total number of packet that has been delivered successfully per unit time seems to be high for the tunneling via P3D when compared to the other techniques. The throughput is considered from Eq. 1:

$$T_i = [P_i / L_i]; \text{ For } i = 1,2,3...n \quad (1)$$

Where:

T_i = Indicates the throughput
P_i = Indicates the packet per network
L_i = Indicates the latency per network
i = Indicates the data packets
N = Indicates the total number of the packets in the network

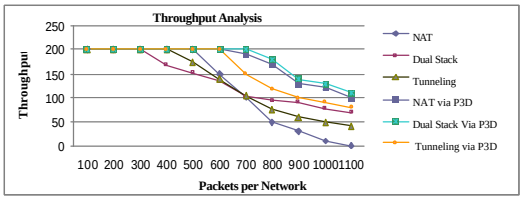

Fig. 4: Throughput analysis

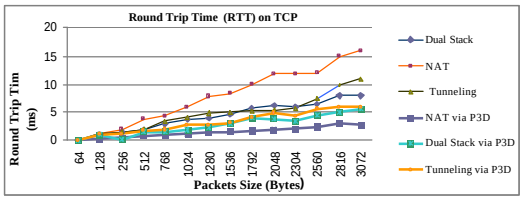

Fig. 5: Round Trip Time (RTT) on TCP

The throughput for different packets per network was calculated by means of Eq. given 2 below:

$$T_i = [P_1/L_1 + P_2/L_2 + P_3/L_3 + ... + P_N/L_N] \quad (2)$$

Initially, there occurs no congestion and no packet is dropped. Hence, the throughput increases for all the techniques as shown in Fig. 4. The packets that are not alive at the destination get discarded at the source. For these reasons the RTT also good enough for the techniques as shown in Fig. 5.

The RTT is the response time to identify the QoS experienced by the nodes in IPv6 and IPv4 networks. The RTT is also known as a Ping time and according to, next RTT can be defined by the following calculation. Where, a is the smoothing factor that lies between 0 and 1):

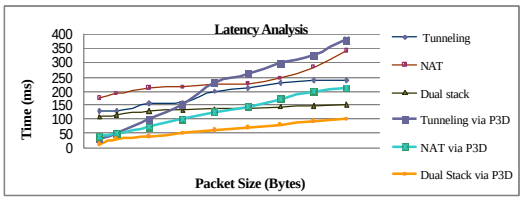

Fig. 6: Latency analysis

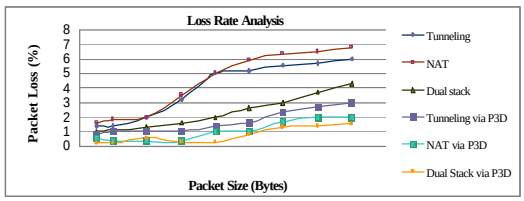

Fig. 7: Loss rate analysis

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

Figure 6 shows the latency analysis. Samples such as 64, 128, 256, 384 kbps data are taken and transmitted over the testbed in the real time simulator. On transmitting data of higher packet size the latency increased for all the three transition mechanisms.

The loss analysis was measured by increasing the packet size and analysis the corresponding change in the loss rate. Most of the packets are delivered successfully; where as some of the packets are dropped without any cause. The loss rate for a datagram packet of size NX64 are taken as a sample data and are made to transmit over the testbed.

Before entering the network the destination node is checked whether it is alive. Table in the router updates if the node is alive, by having this the loss rate can easily be measured. Figure 7 shows the loss rate analysis. The CPU utilization, U is the amount of time not in idle task as shown in Eq. 4. The idle task has the absolute lowest priority in multitasking systems. The percentage of time spent in the idle task can be calculated using the Eq. 4, the CPU utilization is high for all the transition techniques than the techniques via P3D as shown in Fig. 8:

$$U = 100\% - (\%\text{ of time spent in idle task}) \quad (4)$$

The end to end delay is the metric measured for the time taken for the packet to be transmitted across a network form source to destination:

$$D_{End-End} = N(D_{Trans} + D_{Prop} + D_{Proc}) \quad (5)$$

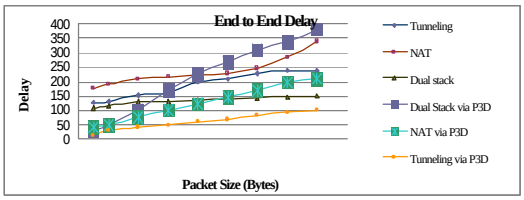

Fig. 8: CPU utilization

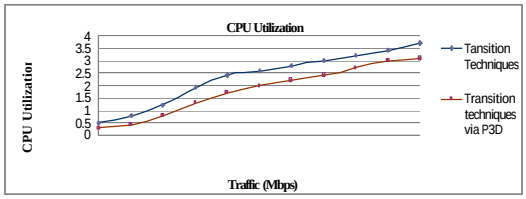

Fig. 9: End to end delay

Where:

N = Stands for the number of links which is the number of routers added by 1

D_{trans} = Stands for the transmission delay

D_{prop} = Stands for the Propagation delay

D_{proc} = Stands for the processing delay

Each router has its own D_{trans} D_{prop} and D_{Proc}. Hence, the end-to-end delay is the calculated using Eq. 5.The graph obtained is shown in Fig. 9.

CONCLUSION

This study describes testbed automated routing infrastructure built on Port Dependent Decision Device (P3D) over a Real time Simulator for IPv4-IPv6 coexistence for tunneling transition techniques. We have achieved a transmission of packets between two different networks with low latency, high throughput and low data loss over symmetric and asymmetric NATed network.

The router was made capable to handle both symmetric and asymmetric NAT. We have achieved low data loss and have ensured that data is delivered at the destination immaterial of the NAT network it travels through. Test analysis wasattained using a real time simulator.

The high availability of the particular network can be ensured by adding one more router at the source and destination in Hot Standby Router Protocol (HSRP) which will help us in growing the number of nodes in source and destination without any downtime. HSRP is a Cisco proprietary redundancy protocol for launching a fault-tolerant default gateway. This can be considered as a future work.

REFERENCES

Colitti, L., S.H. Gunderson, E. Kline and T. Refice, 2010. Evaluating IPv6 Adoption in the Internet. In: Passive and Active Measurement. Krishnamurthy, A. and B. Plattner (Eds.). Springer Berlin Heidelberg, Berlin, Germany, ISBN: 978-3-642-12333-7, pp: 141-150.

Durand, A., 2001. Deploying IPv6. IEEE Internet Comput., 5: 79-81.

Durand, A., R. Droms, J. Woodyatt and Y. Lee, 2011. Dual-stack lite broadband deployments following IPv4 exhaustion. Internet Eng. Task Force, 1: 1-31.

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.

McFarland, S., S. Muninder, S. Nikhil and S. Hooda, 2011. IPv6 for Enterprise Networks. Cisco Press, Indiana, USA., ISBN: 9781587142277, Pages: 372.

Phu, N.M., Q.A. Nguyen, T. Rantapuska, J. Utriainen and M. Matilainen, 2012. Transition from IPv4 to IPv6: The method for large enterprise networks. Proceedings of the INNOV 2012 First International Conference on Communications, Computation, Networks and Technologies, October 21-26, 2012, Lahti University of Applied Sciences, Venice, Italy, ISBN: 978-1-61208-244-8, pp: 5-14.

Punithavathani, D.S. and K. Sankaranarayanan, 2009. IPv4/IPv6 transition mechanisms. Eur. J. Sci. Res., 34: 110-124.