Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 12 (5): 459-465, 2012
ISSN 1812-5654 / DOI: 10.3923/jas.2012.459.465

Network Performance Evaluation of Tunneling Mechanism

[1]Nazrulazhar Bahaman, [1]Anton Satria Prabuwono,
[1]Raed Alsaqour and [2]Mohd Zaki Mas'ud
[1]Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia,
43600 UKM Bangi, Selangor D.E., Malaysia
[2]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka,
Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

Abstract: Internet Protocol version 6 (IPv6) is introduced to replace the services offered by the Internet Protocol version 4 (IPv4) and it is aimed to improve the current provisions as well as providing better services to the Internet's users. Several types of IPv6 transition mechanisms have been developed to migrate the IPv4 technology to IPv6 technology. Although all transition mechanisms have the same objective, the process necessitates compliance with their respective capabilities. This paper focuses on the evaluation of the transition mechanisms namely Tunneling Mechanism in terms of data transmission. The evaluation is based on an Experimental work that is conducted on a controlled testbed environment. User-to-user network performance software is used to obtain the throughput, round trip time and tunneling overhead for TCP and UDP transmission protocol. The transition mechanism performance results are then compared with the performance of native IPv4 and IPv6 environment.

Key words: Tunnelling, Protocol-41, transmission control protocol, user datagram protocol

INTRODUCTION

In recent years, the numbers of unused Internet Protocol (IP) addresses is nearly depleted. To overcome this matter, Internet users have started looking for another alternative and the solution is by introducing IPv6 (Kusin and Zakaria, 2011). IPv6 is considered as a great potential to replace the current IPv4. The reason to replace IPv4 is to fulfil the needs of the number of addresses while reducing other the weaknesses the protocol have. Even though the research on IPv6 has been started more than 10 years ago, the study is still going on to ensure that it is really suitable for future IP implementations. Today we can sees that both IPv6 and IPv4 protocol is use concurrently in the Internet network.

The implementation of a dual-stack protocol on IPv4-IPv6 network uses both protocols at the same time. This method is called the transition mechanism. The transition mechanism is implemented in order to create a smooth transition from IPv4 to IPv6 (Bahaman *et al*., 2012). The Internet Engineering Task Force (IETF) has established a working group called the Next Generation Transition (NGTRANS) which aims to develop mechanisms to support joint operations between IPv4 and IPv6 (Deering and Hinden, 1998). As a result, different kinds of transition mechanisms have been created. This study is focuses on the transition that uses the tunneling method with protocol type 41 as data transmission. In ensuring that the encapsulation process will not taken place at the end user, tunnelling on router-to-router is preferred. This objective of this research was to analyse and evaluate the network performance of this transition mechanism.

BACKGROUND

TCP/IP is built on version 4 of the Internet Protocol in year 1981. Since a decade ago, IPv4 has evolve from a small experimental linkages within the IPv4 network to the world-wide Internet and has shows its performance, capability and led on to occupy a predominant position within the growth of internet usage. However, IPv4 has come to its limitation especially when the number of unused addresses decreased and nearly extinct.

Corresponding Author: Nazrulazhar Bahaman, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor D.E., Malaysia

Table 1: The summary desription of transition mechanisms site operations

Type	Transition mechanism	Site operations	IETF reference
Tunnel mechanism	6 over 4	• Between End-node and network-device	RCF 2529
	Intra-site automatic tunnel addressing protocol (ISATAP)	• Between End-node and network-device	RCF 5214
	Dual stack transition mechinsm (DTSM)	• Between End-node and network-device • Between End-node and network-device • Between End-node and network-device • Between End-node and network-device	RCF 4380
	6 to 4	• Between network-devices	RFC 0356
	6 in 4	• Between network devices	RFC 4213
	Tunnel Setup Protocol (TSP)	• Between end-nodes	RFC 5572
Dual stack	Dual stack	• On end-node only • On network-device only	RFC 4213
	Dual stack lite (DSLite)	• On end-node only	ID-dual stack-lite-10
Translator mechanism	Stateless IP/ICMP translations (SIIT)	• On end-node only • On network-device only	RFC 2765
	Bump-in-the-stack (BIS)	• On end-node only	RFC 2762
	Bump-in-the-API (BIA)	• On end-node only	RFC 3338
	Network address translation-protocol translation (NAT-PT)	• On network-device only	RFC 2766
	Multicast translator proxving (MTP)	• On network-device only	ID mtp-03
	Transport relay translator (TRT)	• On network-device only	RFC 3142

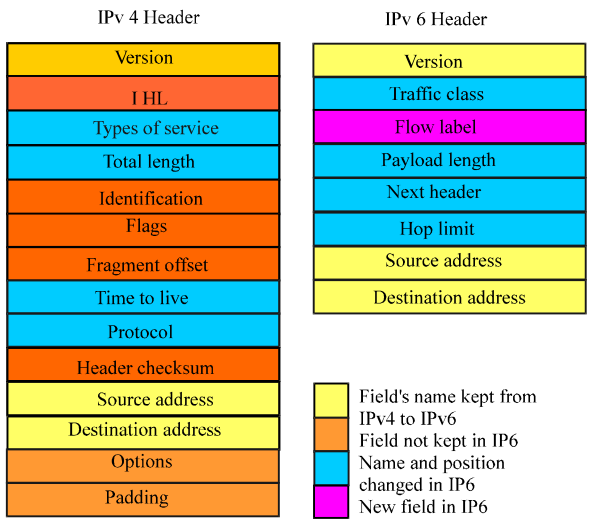

Fig. 1: Comparison between the two versions of protocol headers

The main purpose of designing a new Internet Protocol (IPv6) is to increase the number of IP addresses (Lee and Chen, 2008). IPv6 is capable of generating more than 3.4×1038 unique addresses compared to the 4.3×10^{9} addresses in IPv4. This is because IPv6 addresses have been designed as 128-bit (16-byte) address whereas IPv4 only provides 32-bit (4-byte) addresses. The major difference in layout between the IPv4 and IPv6 packages is that IPv4 has a 20 byte header while IPv6 has a 40 byte header. Even though the IPv6 address space is four times larger than IPv4, IPv6 has reduced the number of required fields and introduced header connection. The comparison between the two versions of the protocol headers is depicted in Fig. 1.

All the transition mechanisms are considered as a set of methods to enable a smooth transition to the new version of IP. Unfortunately, not all of them are amenable to user's options. According to Karpilovsky *et al*. (2009), Teredo (Huitema, 2006) and 6 to 4 (Carpenter and Moore, 2001) are transition mechanisms that give more performance compared to others such as 6over4 (Carpenter and Jung, 1999), ISATAP (Templin *et al*., 2008), DTSM (AlJaafreh *et al*., 2008), SIIT (Shen and Smit, 2000), BIS (Tsuchiya *et al*., 2000), BIA (Lee *et al*., 2002), NATPT (Tsirtsis and Srisuresh, 2000), MTP (Waddington and Chang, 2002) and TRT (Hagino and Yamamoto, 2001). These transition mechanisms can be categorized into three types named Tunneling Mechanism, Dual Stack and Translation Mechanism. Site operational of the transition mechanisms are summarized in Table 1.

The Tunneling Mechanism (Carpenter and Moore, 2001) is a kind of transition mechanism that encapsulates the IPv6 packet in IPv4 packet. The IP protocol number 41 or also known as Protocol-41 (Bahaman *et al*., 2011) is used by the IPv6 transition mechanism to operate in the IPv4 network. It can also be encapsulated within UDP packets, for instance for a packet to across a router or Network Address Translation (NAT) (Dongping *et al*.,

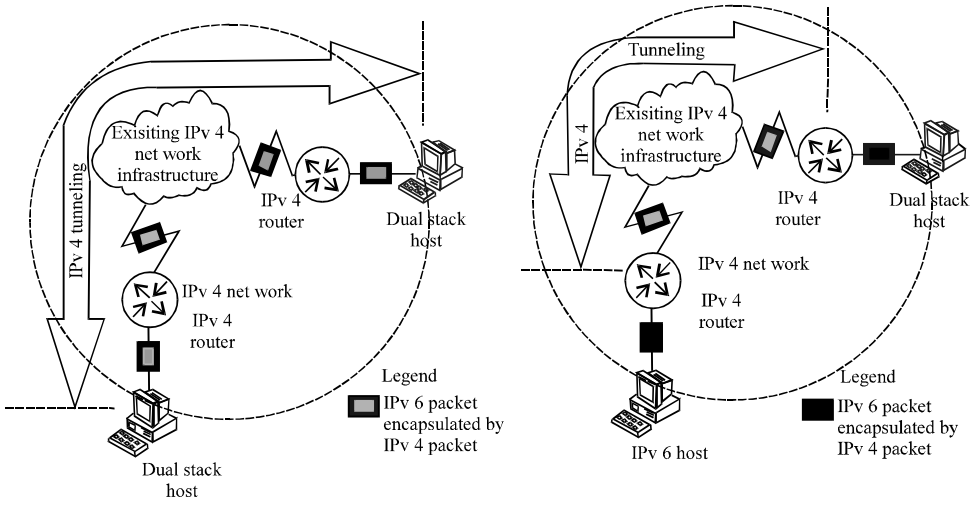

Fig. 2(a-b): (a) Host-to-host tunneling and (b) Router-to-router tunneling

2006) device that blocks protocol-41 traffic. The tunneling mechanism allows an IPv6 to operate and at the same time maintain the IPv4 network infrastructure. There are several reasons why this mechanism is needed in the present network; one of them is to bring the data to the transmission across networks that are incompatible or to provide a safe route through the insecure network.

Host-to-host tunneling is a method in which the encapsulation process is done at the host source while the de-encapsulation process is done at the destination host (Raicu and Zeadally, 2003a). IPv6 packets are covered with the IPv4 packet and are sent through the Ipv4 network using UDP port 3544 packets (Huitema, 2006). Figure 2a illustrates how the IPv4/IPv6 hosts encapsulate IPv6 packets into IPv4 packets and are sent over the network as IPv4 packets. This transition mechanism supports the use of IPv6 on the hosts dual-stack protocols and while maintaining the existing IPv4 infrastructure. This study excludes Host-to-host tunnelling from the research because the encapsulation process occurs at the end user and this will affect the performance of workstation tested during the experiments.

According to Raicu and Zeadally (2003a), the router-to-router tunneling mechanism involves the process of encapsulation performed by the router and de-encapsulation occurs at the destination router. The tunnel was built between two routers to support the dual-protocol stack (IPv4 and IPv6). Therefore, the source host and destination host can be assigned to a native IPv6 environment. The activated tunneling between the two dual-stack routers is shown in Fig. 2b.

Basically, the process of transmitting packets using router-to-router tunneling is as follows: First, the hosts on the IPv6 network send the packet to the sender router as a gateway. After referring to the routing table, the packet is forwarded to the configured sender router interface as a route tunnel. In the next step, the router encapsulates the IPv6 packet with the IPv4 header. Consequently, the encapsulated packet is forwarded through the tunnel. Then, at the end of the tunnel, the receiver router de-encapsulates the packet by removing the IPv4 packet header. Finally, based on the routing table, the receiver router sends a packet to the IPv6 network.

EXPERIMENTAL METHODS

In order to reduce disturbances that may affect the results, all experiments were conducted under a controlled environment. The networks' performance evaluation process is divided into several procedures as shown in Fig. 3.

Hardware and software requirement: The first phase describes the detailed description of the infrastructure in order to provides a good insight towards the selection of suitable hardware and software that are compatible with IPv6. The hardware and software used in this experiment are Operating System: Microsoft Windows 7, Router: Cisco 2821 with IOS 12.2(2) T, Switch: Cisco Catalyst 2960-24TT 24-Port Ethernet Switch, Network performance: D-ITG, Packet viewer: WireShark 1.2.6.

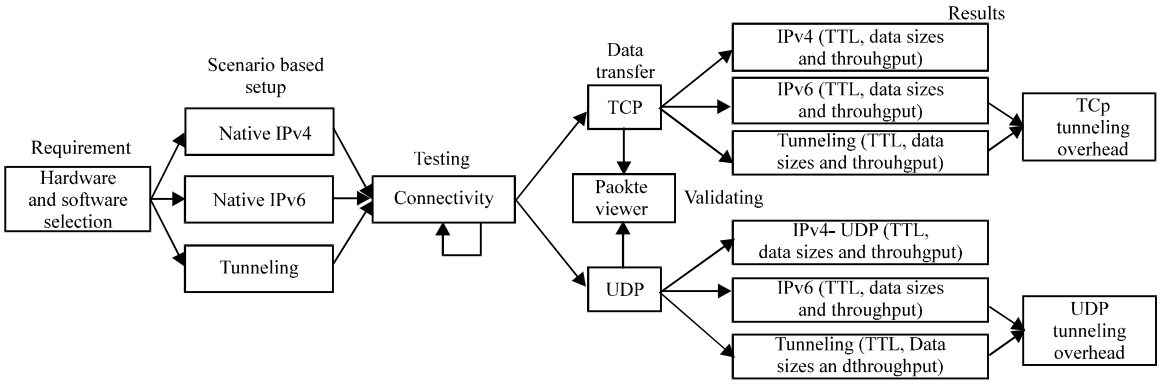

Fig. 3: Experiments work flow for networks performance evaluation

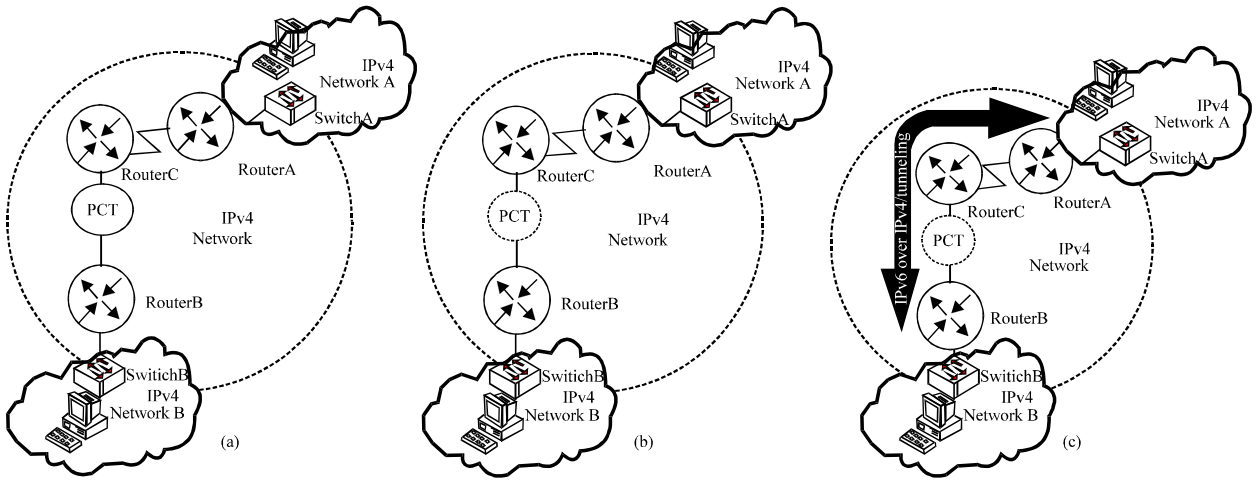

Fig. 4(a-c): (a) Entirely IPv4, (b) Entirely IPv6 and (c) Tunneling methods

Scenario based setup: The implementation was prepared under a controlled environment in accordance with basic network components. The network included users (sender and receiver), protocols (IPv4, IPv6 and IPv6 in IPv4), transmission devices (router and switch), packet monitor (Packet viewer) and packet generator (D-ITG). The experiment was done in 3 difference of environment namely environment in full IPv4, an IPv6 environment entirely and an environment using tunneling methods. Although the experiments were conducted within different environments, the types of equipment and network remain the same. This is to provide an accurate result and to be used in comparing the relation between each environment. The description of these environments is depicted in Fig. 4.

Mainly, the testbed was constructed by a number of capable devices of both protocols (versions 4 and 6) and the packet viewer is placed between RouterB and RouterC for monitoring the right packets. In Fig. 4a, all devices are arranged to three different IPv4 networks. These networks are named as IPv4 NetworkA, IPv4 NetworkB and IPv4 Network. Here, the user identified as a sender is placed at IPv4 NetworkA and a receiver was located at IPv4 NetworkB. Then, the IPv4 Network contains several routers which have the role of an internetwork transmission and positioned between IPv4 NetworkA and IPv4 NetworkB.

The same experiment was conducted in Fig. 4b but configured into IPv6 environment. The three difference networks are named IPv6 NetworkA, IPv6 Network B and IPv6 Network. In this environment, the sender is sited at IPv6 Network A while the receiver is at IPv6 NetworkB. The transmission network between these networks is called the IPv6 Network. From Fig. 4c, the network is configured with both protocol version 4 and version 6. The sender and receiver are configured using IPv6 (IPv6 NetworkA and IPv6 NetworkB) while the internetwork

between them is configured with IPv4 (IPv4 Network). Tunneling configuration is setup between RouterA and RouterC, this tunnel is operating under both IPv4 and IPv6 protocols.

Testing procedures: The testing phase is important to ensure that all items are operating in a good condition. In order to meet all objectives of this implementation, several tests were selected based on similar previous research. From the literature, several similar research has been done; Connectivity test (Udhayan and Anitha, 2009), Packet Flow (Xinyu *et al*., 2007), Round Trip Time (Cho *et al*., 2004), Throughput (Raicu and Zeadally, 2003b; Law *et al*., 2008) and Tunneling Overhead (Aazam *et al*., 2010).

Connectivity: In this test, ping and ping6 are used to investigate the connectivity of the transition mechanism, as compared to IPv4. In order to ensure that it operates in multi-platform operating systems, testing is conducted on all nodes that are involved.

Packet Flow Here, the packet viewer is used to monitor the packet flow in detail. This is to ensure that all packets went through the tunnel as expected. Example of the packet flow activities gathered are depicted in Fig. 5, where a represents source IP address, b represents destination IP address, c represents packet type, d represents protocol type and *e* represents load size.

Round trip time (RTT): The response times in this test provide an indication of the quality-of-service experienced by nodes in the IPv6 and IPv4 networks. All nodes on different networks are involved by means of sending and receiving the ICMP and ICMPv6 packets to each other.

Throughput: In this test, the basic Transfer File Protocol (FTP) is used to download files across the networks. In order to have an unbiased result, the files are downloaded from servers using different operating systems. The throughput is then calculated using:

$$T = P/L \quad (1)$$

where, T represents the throughput, P represents the transferred data size and L represents the time cost in transfer.

Tunneling overhead: It is a combination amount of several overheads that are involved in tunneling matters such as creating tunnels, deleting tunnels, encapsulation, decapsulation, refreshing and maintaining tunnels. The tunneling overhead emerges through subtraction of each protocol's round trip time against the round trip time of untunneled/direct traffic.

$$TO = RTT_{tunnel} - RTT \quad (2)$$

where, TO represents the tunneling overhead and RTT represents the round trip time.

RESULTS AND DISCUSSION

All tests are repeated 20 times to ensure high data accuracy. In order to get an accurate result for given packet sizes, each run had 20,000 numbers of buffer to be sent under the same testbed. In this study, the overhead tunneling was measured in accordance with the type of transmission protocol, TCP (Abdelrahman *et al*., 2002) and UDP (Ren *et al*., 2009). When the results are taken and plotted, there is apparently a significant difference between these two protocols as shown in Fig. 6. The TCP tunnelling overheads show that the values of tunnelling overhead generated are increased by the value of packets sent. Therefore, the higher the size of packets sent then the higher the overhead is generated. At the UDP, however, overhead yields had equivalent values of approximately zero at all levels of data sizes. This explains the fact that tunnelling overhead exists at the UDP while it is not just lower than at the TCP, it is also not influenced by size of data.

Figure 7 refers to TCP throughput values of the three different internet protocols. The graph of throughput values illustrates the same pattern. IPv6 gave the higher throughput values of from 64 Bytes to 1024 Bytes and then decreases slightly lower than that of IPv4 for the rest

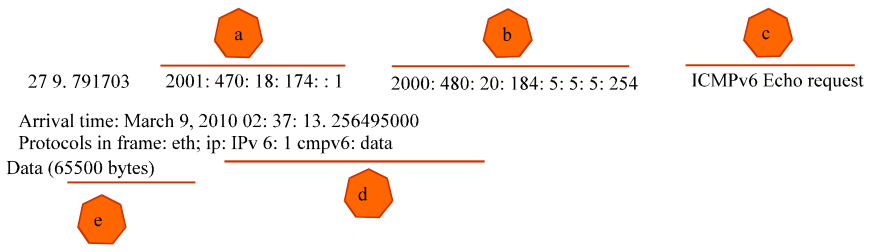

Fig. 5: Sample ICMPv6 packet through tunneling captured

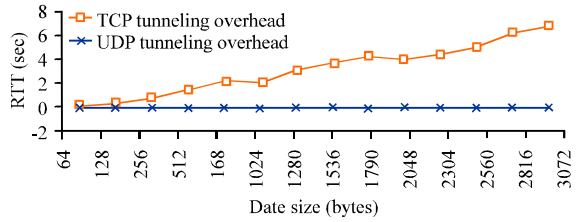

Fig. 6: Tunneling Overhead

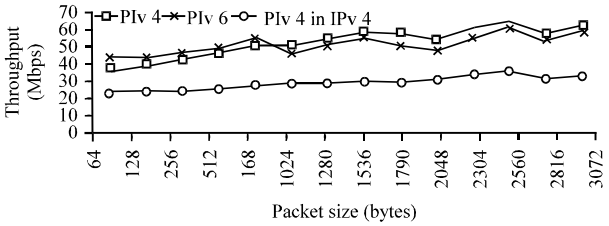

Fig. 7: TCP throughput

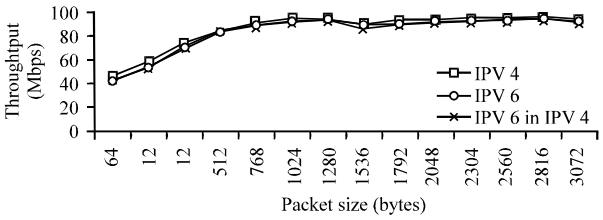

Fig. 8: UDP throughput

of the packet sizes. However, all plotted points of throughput values produced by tunnelling are almost 50 percent lower than those of IPv4 and IPv6.

Figure 8 shows the UDP performance metric values. The plotted graph confirms that throughput values for both internet protocol and transition mechanisms give a similar line. The indication explains that there is hardly any different in throughput values between the scenarios. There are gradual increases existing from packet sizes between 64 Bytes to 1024 Bytes. Besides, throughput values remain for all larger packet sizes but slightly decreased at 1536 Bytes.

The RTT of both protocols and tunnelling using TCP to send all given packets are plotted in Fig. 9. From the graph, the results show that all RTT are gradually increased with an increment of packet sizes. The RTT of IPv4 and IPv6 produce almost the same pattern and value. At the beginning, the tunnelling result shows the same, but then it kept getting larger. The result is slightly deferent in Fig. 10 when using the UDP. It is because the same values of RTT are carried out for the tunnelling, IPv4 and IPv6 at all levels of packet sizes.

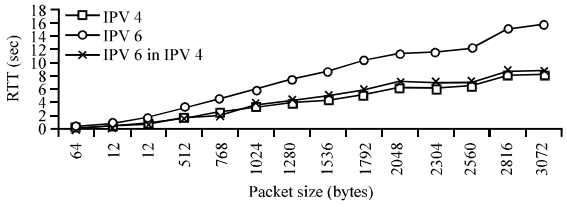

Fig. 9: Round trip time (RTT) on TCP

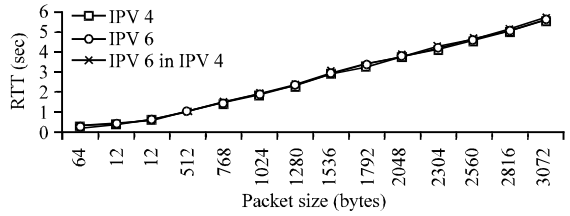

Fig. 10: Round trip time (RTT) on UDP

CONCLUSION

This paper is focused on the capabilities of the IPv6 tunneling mechanisms compared with those of the current (IPv4) and future Internet Protocol (IPv6). The assessment is conducted in a controlled environment on the testbed that is configured based on a real process of transmitting IPv6 packets over the IPv4 network. Then, the analysis is done on tunnelling overhead, throughput and Round Trip time (RTT). The TCP and UDP traffic is simulated using D-ITG on the testbed. The result of the experiments conducted can be summarized into 3 conclusions.

First, the comparison of transmission data between the tunneling mechanism and the native IPv4 and IPv6 networks revealed an increment to Tunneling Overhead and RTT when the size of packets grew, while the gained throughput is less than half. In the other words, the performance of the tunneling mechanism is lower than the two existing protocols in the context of TCP data transmission.

Second, a different outcome is obtained for the UDP transmission. Then results are difficult to distinguish since the throughput and RTT values of each protocol tested are almost similar. Hence, the explanation is that the UDP transmission data via selected tunneling does not affect the real performance of both protocols.

Finally, it can be concluded that the tunneling mechanism is only suitable to be implemented for research and experiment during the transition period. This proves that the real ability of the TCP transmission data through the tunneling is reduced. In the near future, it will be necessary to explore the tunnelling overhead in detail in

order to identify the breakdown of overhead in order to improve of the transition mechanism.

REFERENCES

Aazam, M., I. Khan, M. Alam and A. Qayyum, 2010. Comparison of ipv6 tunneled traffic of teredo and ISATAP over test-bed setup. Proceedings of the International Conference on Information and Emerging Technologies (ICIET), June 14-16, 2010, Karachi, pp: 1-4.

Abdelrahman, A.M., M.S. Abdalla, B.M. Ali, V. Prakash and R.K.Z. Sabudin, 2002. Improving the performance of TCP in LEO satellite environment. Inform. Technol. J., 1: 250-254.

AlJaafreh, R., J. Mellor and I. Awan, 2008. Evaluating BDMS and DSTM transition mechanisms. Proceedings of the UKSIM European Symposium, Computer Modeling and Simulation, September 8-10, 2008, IEEE., pp: 8-10.

Bahaman, N., A.S. Prabuwono and M.Z. Masud, 2011. Implementation of IPv6 network testbed: Intrusion detection system on transition mechanism. J. Applied Sci., 11: 118-124.

Bahaman, N., A.S. Prabuwono, M.Z. Mas`ud and M.F. Abdollah, 2012. Effectiveness of security tools to anomalies on tunneled traffic. Inform. Technol. J., 11: 191-199.

Carpenter, B. and C. Jung, 1999. Transmission of IPv6 over IPv4 domains without explicit tunnels: R. f. C. 2529. Internet Engineering Task Force.

Carpenter, B. and K. Moore, 2001. Connection of IPv6 domains via IPv4 clouds: R. f. C. 3056. Internet Engineering Task Force.

Cho, K., M. Luckie and B. Huffaker, 2004. Identifying IPv6 network problems in the dual-stack world. Proceedings of the ACM SIGCOMM workshop on Network Troubleshooting: Research, Theory and Operations Practice Meet Malfunctioning Reality, Aug. 30-Sept. 3, Portland, Oregon, USA., pp: 283-288.

Deering, S. and R. Hinden, 1998. Internet protocol, version 6 (IPv6) specification. R. f. C. 2460. Internet Engineering Task Force.

Dongping, Z., Z. Deyun and H. Lin, 2006. Applying application level gateways for real-time service. Inform. Technol. J., 5: 1088-1092.

Hagino, J. and K. Yamamoto, 2001. An IPv6-to-IPv4 transport relay translator. R.f.C. 3142. Internet Engineering Task Force.

Huitema, C., 2006. Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs): R. f. C. 4380. Internet Engineering Task Force.

Karpilovsky, E., A. Gerber, D. Pei, J. Rexford and A. Shaikh, 2009. Quantifying the extent of IPv6 deployment. Passive Active Network Measurement, 5448: 13-22.

Kusin, Z. and M.S. Zakaria, 2011. Distance based mobility anchor point selection scheme with dynamic load control in hierarchical mobile IPV6. Inform. Technol. J., 10: 1817-1823.

Law, Y.N., M.C. Lai, W.L. Tan and W.C. Lau, 2008. Empirical performance of IPv6 vs. IPv4 under a dual-stack environment. Proceedings of the IEEE International Conference Communications, May 19-23, Beijing, pp: 5924-5929.

Lee, L.T. and C.W. Chen, 2008. The web services with security mechanisms base on IPv4 and IPv6. Inform. Technol. J., 7: 1188-1193.

Lee, S., M.K. Shin, Y.J. Kim, E. Nordmark and A. Durand, 2002. Dual stack hosts using bump-in-the-API (BIA). R.f.C. 3338. Internet Engineering Task Force.

Raicu, I. and S. Zeadally, 2003a. Evaluating IPv4 to IPv6 transition mechanisms. Proc. 10th Int. Conf. Telecommun., 2: 1091-1098.

Raicu, I. and S. Zeadally, 2003b. Impact of IPv6 on end-user applications. 10th Int. Conf. Telecommun., 2: 973-980.

Ren, Y., H. Tang, J. Li and H. Qian, 2009. Performance comparison of UDP-based protocols over fast long distance network. Inform. Technol. J., 8: 600-604.

Shen, N. and H. Smit, 2000. Dynamic hostname exchange mechanism for IS-IS. R.f.C. 2765. Internet Engineering Task Force.

Templin, F., T. Gleeson and D. Thaler, 2008. Intra-Site Automatic Tunnel Addressing Protocol (ISATAP): R. f. C. 5214. Internet Engineering Task Force.

Tsirtsis, G. and P. Srisuresh, 2000. Network Address Translation-Protocol Translation (NAT-PT). R.f.C. 2766. Internet Engineering Task Force.

Tsuchiya, K., H. Higuchi and Y. Atarashi, 2000. Dual stack hosts using the bump-in-the-stack technique (BIS). R.f.C. 2767. Internet Engineering Task Force.

Udhayan, J. and R. Anitha, 2009. Demystifying and rate limiting ICMP hosted DoS/DDoS flooding attacks with attack productivity analysis. Proceedings of the IEEE International Advance Computing Conference, March 6-7, 2009, Patiala, pp: 558-564.

Waddington, D.G. and F. Chang, 2002. Realizing the transition to Ipv6. IEEE Commun. Magazine, 40: 138-147.

Xinyu, Y., M. Ting and S. Yi, 2007. Typical DoS/DDoS threats under IPv6. Proceedings of the International Multi-Conference on Computing in the Global Information Technology, March 4-9, 2007, Gosier, Guadaloupe, pp: 55-55.