2012 International Conference on Innovation, Management and Technology Research (ICIMTR2012), Malacca, Malaysia : 21-22 May, 2012

Network Performance Evaluation of 6to4 Tunneling

Nazrulazhar BAHAMAN, Erman HAMID
Faculty of Information and Communication Technology,
Universiti Teknikal Malaysia Melaka,
Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia
nazrulazhar@utem.edu.my

Anton Satria PRABUWONO
Faculty of Information and Science Technology,
Universiti Kebangsaan Malaysia, 43600 UKM Bangi,
Selangor D.E., Malaysia
antonsatria@ftsm.ukm.my

***Abstract*--Several types of IPv6 transition mechanisms have been developed to facilitate the migration of IPv4 to the new protocol, IPv6. 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 6to4 tunneling in terms of data transmission. The assessment is based upon experimental work that is conducted on a controlled 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 performance of TCP and UDP through 6to4 tunnel is then compared over the native IPv4 and IPv6 environment. As a result, the findings prove the ease of TCP data transmission via the tunnel compared to both native networks. In contrast, the UDP implementations show the slight difference for them.**

***Index Terms*-- Tunneling, Protocol-41, 6to4, TCP, UDP**

I. INTRODUCTION

In recent years, the number of unused Internet Protocol (IP) addresses is nearly depleted. As an alternative, Internet users have started some efforts to find a solution by introducing IPv6. Referring to [1], they believed that IPv6 is a great potential as a replacement to the current IPv4. The main reason is to fulfill the needs of the number of addresses while reducing other weaknesses the protocol have. Since a decade ago, many attentions possessed to ensure IPv6 reliability for future IP implementations. Until present, both IPv6 and IPv4 protocol are used concurrently in the Internet network.

The implementation of a dual-stack protocol on IPv4-IPv6 network uses both protocols simultaneously. This method is called the transition mechanism. The transition mechanism is proposed to create a smooth transition from IPv4 to IPv6. Consequently, the Internet Engineering Task Force (IETF) has established a working group named the Next Generation Transition (NGTRANS) which aims to develop mechanisms that support operations between IPv4 and IPv6 [2]. As regards, numerous corresponding transmission mechanisms have been created. As stated earlier, this paper focuses on the transition that uses the tunneling method with protocol type 41 as data transmission. Besides, 6to4 tunneling router-to-router is preferred to avoid the encapsulation at end users. The primary objective of this research is to analyze and evaluate the network performance of this transition mechanism.

The following sections of this paper are constituted as follows: section 2 will explain the background of the Internet protocols and Transition Mechanisms. In section 3 is the explanation on the hardware and software setup in detail. The testing procedure is described in section 4. Next, section 5 will be the thorough analysis of the results obtained. Finally, section 6 will conclude the overall study.

II. BACKGROUND

In year 1981, TCP/IP is built on version 4 of the Internet Protocol. Over the years, IPv4 has evolved from a small experimental linkages within the IPv4 network to the world-wide Internet and has shown its performance, capability and led on to occupy a predominant position within the growth of internet usage. However, IPv4 has come to its limitation critically when the number of unused addresses decreased and nearly extinct.

The main purpose of designing a new Internet Protocol (IPv6) is to grow the number of IP addresses. Moreover, IPv6 is outperformed in generating more than 3.4x1038 unique addresses as compared only 4.3x109 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 but it has reduced the number of required fields and also introduced header connection.

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 [1], Teredo [3] and 6to4 [4] are transition mechanisms that give more performance compared to others such as 6over4 [5], ISATAP [6], DTSM [7], SIIT [8], BIS [9], BIA [10], NATPT [11], MTP [12] and TRT [13]. These transition mechanisms can be categorized into three types namely Tunneling Mechanism, Dual Stack and Translation Mechanism.

The Tunneling Mechanism [4] 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 [14] 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 move across a router or Network Address Translation (NAT) device that blocks protocol-41 traffic. The tunneling mechanism allows an IPv6 to process as well maintain the IPv4 network infrastructure. One of the reasons to guarantee the need of the mechanism is to bring the data to the transmission across networks that are incompatible. In other word, a safe route is provided under the insecure network.

6to4 is one of tunnel technology used to provide unicast IPv6 connectivity between IPv6 sites and hosts across the IPv4 Internet. It encapsulates IPv6 packet as IPv4 payload and uses protocol number neither 6 (TCP) nor 17 (UDP) but 41(Protocol-41) in protocol field of the IPv4 header. 6to4 assumes the entire IPv4 Internet as a link. The simplest implementation of 6to4 is applicable for multiple networks. Each of them is connected with IPv4 Internet connection. The networks may belong to the global Internet or corporate network. Among various networks, the vital behavior is their capabilities to send protocol-41 packet each others. At the end of 6to4 tunnel consists of a 6to4 Host/Router, 6to4 Router, or 6to4 Relay Router. Once configuration of 6to4 tunnels is done at any interfaces the router, it will be identified as 6to4 router. Meanwhile, by adding the configuration they are able to communicate with the IPv6 internet and known as 6to4 relay router. Figure 1 shows the tunneling components and their position on the IPv4 and IPv6 Internets.

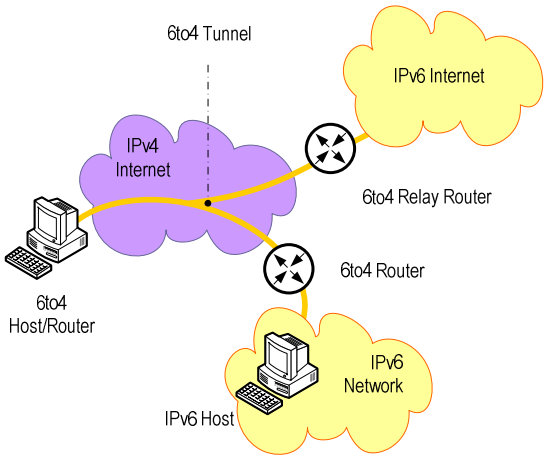

Fig. 1 Scenario of 6to4 tunneling

III. METHOD

The networks' performance assessment procedure is explained in details in this section. 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 Figure 2.

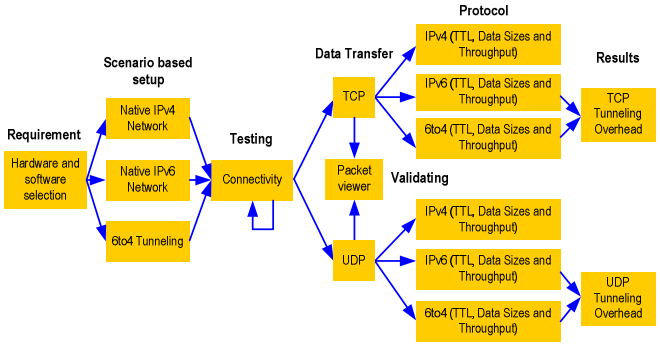

Fig. 2 Experiments work flow for networks performance evaluation

A. Hardware and Software Requirement

The first phase describes the detailed description of the infrastructure to provide 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.

B. Scenario Based Setup

This section explains the method of installation and set-up requirement. 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 has been done in 3 different environments 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 remained the same. This was to accumulate an accurate result and to be used in comparing the relation between each environment. The description of these environments is depicted in Figure 3.

Mainly, the testbed was constructed by a number of capable devices of both protocols (versions 4 and 6) and the packet viewer has been placed between RouterB and RouterC for monitoring the right packets. In figure 3(a), all devices were arranged to three different IPv4 networks. These networks were named as IPv4 NetworkA, IPv4 NetworkB and IPv4 Network. Here, the user identified as a sender has been placed at IPv4 NetworkA and a receiver located at IPv4 NetworkB. Then, the IPv4 Network contained several routers, which have the role of an internetwork transmission and positioned between IPv4 NetworkA and IPv4 NetworkB.

The same experiment was conducted in figure 3(b) but configured into IPv6 environment. The three different networks were named IPv6 NetworkA, IPv6 Network B and IPv6 Network. In this environment, the sender has been sited at IPv6 NetworkA while the receiver was at IPv6 NetworkB. The transmission network between these networks was called

the IPv6 Network. From figure 3(c), the network has been configured with both protocol version 4 and version 6. The sender and receiver were configured by using IPv6 (IPv6 NetworkA and IPv6 NetworkB) while the internetwork between them was configured with IPv4 (IPv4 Network). Tunneling configuration has been setup between RouterA and RouterC, this tunnel was operating under both IPv4 and IPv6 protocols.

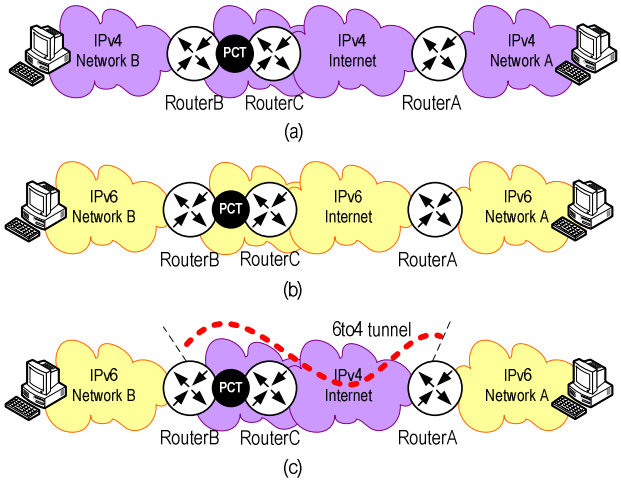

Fig. 3 (a) Entirely IPv4 (b) Entirely IPv6 (c) IPv6 with 6to4 tunneling

IV. Measurement Procedures

In this research, the testing phase is important to make sure that all items are operating well. In order to meet all objectives of this implementation, several tests were selected based on similar researches. Initially, connectivity [15] and Packet Flow [16] tests were aimed to monitoring traffics activity. After that, as referred to the previous works, some procedures such as Round Trip Time [17], Throughput [18, 19] and Tunneling Overhead [20] had been conducted to achieve the aim of this study.

A. Connectivity

In this test, command *ping* and *ping6* were used to examine the connectivity of two end nodes. In order to ensure that it operates in multi-platform, testing has been conducted on all nodes that involved.

B. Packet Flow

During the process, the packet viewer was used to monitor the packet flow to confirm that all packets would go through the tunnel as expected. Figure 4 depicts the example of the packet flow activities gathered, where *a* represents source IP address, *b* represents destination IP address, *c* represents packet type, *d* represents protocol type and *e* represents load size.

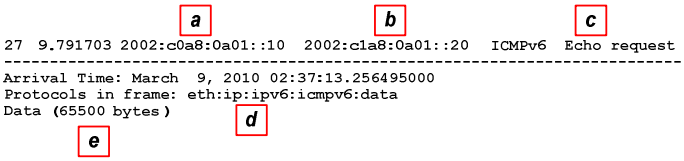

Fig. 4 Sample ICMPv6 packet through tunneling captured

C. Throughput

The basic Transfer File Protocol (FTP) is used to download files across the networks. The consideration for unbiased results must be taken into account by downloading files from server through the different operating systems. The corresponding throughput calculation is presented in (1).

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

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

D. Round Trip Time (RTT)

The response time in this test was to identify the quality-of-service experienced by nodes in the 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 is also known as a Ping time and according to [21], next RTT can be defined by the following calculation.

$$RTT_{next} = (a * RTT_{old}) + ((1 - a) * RTT_{new}) \quad (2)$$

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

E. Tunneling Overhead

It is defined as a combination amount of several overheads that are involved in tunneling matters such as creating tunnels, deleting tunnels, encapsulation, decapsulation, refreshing and maintaining tunnels. As in equation (3), the tunneling overhead emerges through subtraction of each protocol's round trip time against the round trip time of untunneled/direct traffic [23].

$$TO = RTT_{tunnel} - RTT_{native} \quad (3)$$

where TO represents the tunneling overhead, RTT_{tunnel} represents round trip time IPv6 network with tunneling and RTT_{native} represents the round trip time in native IPv6 network.

V. Result

All tests were repeated 20 times to ensure high data accuracy. Each run have had 20,000 numbers of buffers to be sent under the similar testbed to guarantee an accurate result for given packet sizes. Broadly, the overhead tunneling was measured in accordance with the type of transmission protocol, TCP and UDP.

Figure 5 refers to TCP throughput values of the three internet protocols. The graph of throughput values illustrates the same pattern. IPv6 gives the higher throughput values of from 64 Bytes to 1024 Bytes and then decreases slightly lower than that of IPv4 for the rest of the packet sizes. However, all plotted points of throughput values produced by tunneling are almost 50 percent lower than those of IPv4 and IPv6.

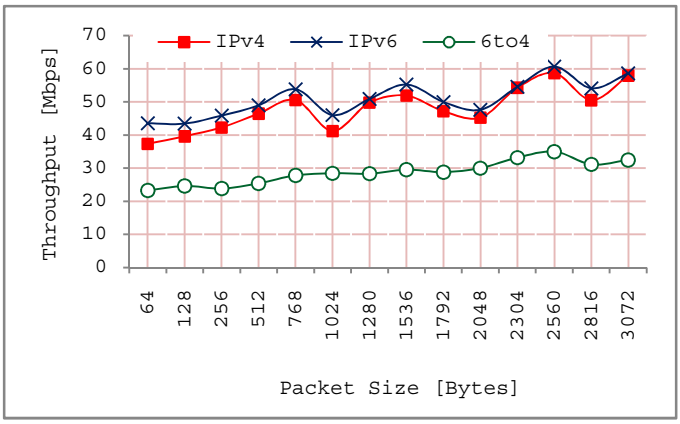

Fig. 5 TCP throughput

Figure 6 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 describes that there is hardly any difference in throughput values between the scenarios. There are gradual increments 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.

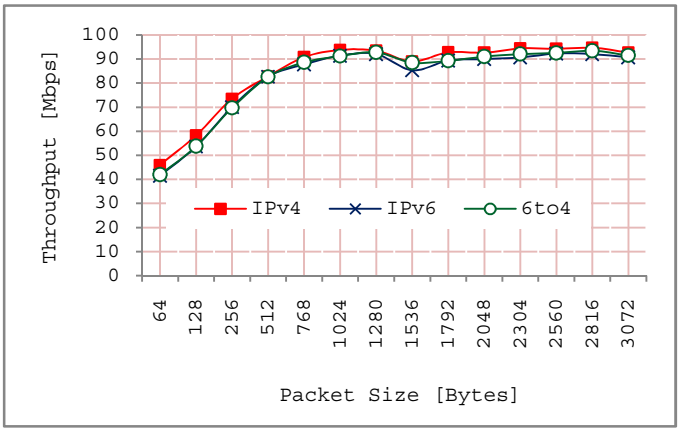

Fig. 6 UDP throughput

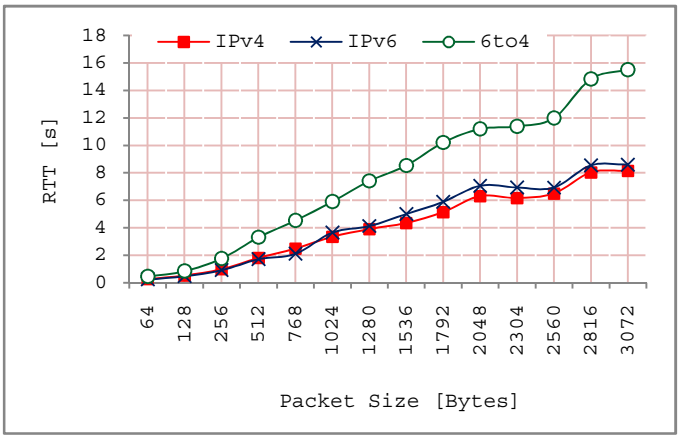

Fig.7 Round trip time (RTT) on TCP

The RTT of both protocols and tunneling using TCP that transmit all given packets are plotted in Figure 7. From the graph, the results show that all RTT are regularly increased with an increment of packet sizes. The RTT of IPv4 and IPv6 produce almost the same pattern and value. While, the result of RTT tunneling shows the same at the beginning, but then it keeps getting larger.

Under the same procedure and architecture, the given scales of packets are sent using UDP. Figure 8 shows the plotted RTT are leisurely increased with an increment of packet sizes. In term of pattern, the same values of RTT are carried out for the tunneling, IPv4 and IPv6 at all levels of packet sizes.

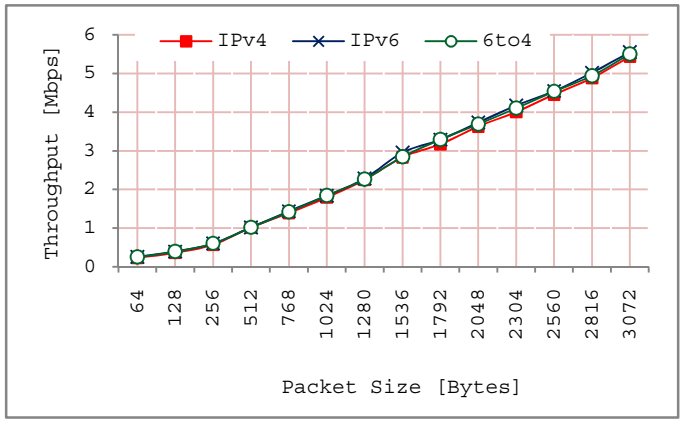

Fig. 8 Round trip time (RTT) on UDP

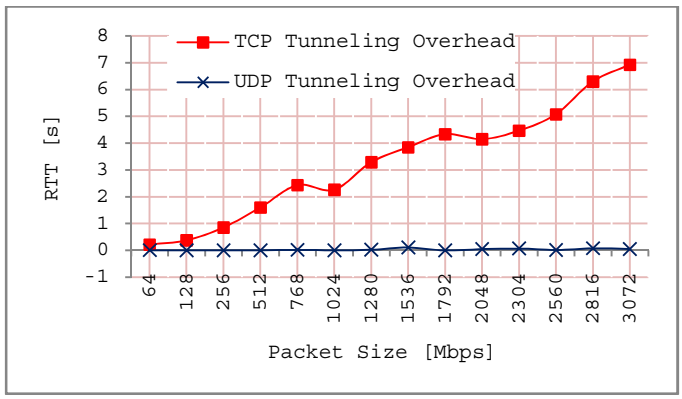

Fig. 9 Tunneling Overhead

The resultants RTT above are used in equation (3) to obtain 6to4 tunnel overhead values as shown in table 1. Accordingly, the plotted result highlights significant difference between these two protocols as shown in Figure 9. The TCP tunneling overheads show that the values of tunneling overhead generated are increased by the value of packets sent. In other words, the higher the size of packets sent will generate more overheads. However at UDP, their overhead yields equivalent values of approximately zero at all levels of data sizes. The result also verifies that the UDP overhead is lower than TCP. Likewise, the finding proves the fact that tunneling overhead exists at the UDP is not influenced by data sizing.

TABLE 1
TUNNELING OVERHEAD VALUES FOR TCP AND UDP

TCP			UDP		
RTT_{native}	RTT_{tunnel}	*TO*	RTT_{native}	RTT_{tunnel}	*TO*
0.241	0.452	0.211	0.253	0.25	0.003
0.483	0.854	0.371	0.391	0.39	0.001
0.915	1.762	0.847	0.599	0.602	-0.003
1.715	3.311	1.596	1.015	1.016	-0.001
2.105	4.533	2.428	1.434	1.42	0.014
3.649	5.907	2.258	1.836	1.839	-0.003
4.125	7.409	3.284	2.279	2.261	0.018
4.69	8.531	3.841	2.951	2.844	0.107
5.879	10.209	4.33	3.285	3.289	-0.004
7.05	11.193	4.143	3.73	3.687	0.043
6.924	11.386	4.462	4.167	4.101	0.066
6.92	11.993	5.073	4.544	4.534	0.01
8.533	14.829	6.296	5.014	4.938	0.076
8.589	15.509	6.92	5.549	5.501	0.048

VI. DISCUSSION

As mentioned previously, this paper focuses on the capabilities of the 6to4 tunneling compared with native IPv4 and IPv6 network. In addition, 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. Firstly, the simulation involved on TCP and UDP traffics are using packet generator. Secondly, the evaluations are over UDP and TCP traffic performance. While the understanding through analysis is done on tunneling overhead, throughput, and Round Trip time (RTT).

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

In table 1, the different outcome is tabulated for the UDP transmission. As referred, the obtained results are difficult to distinguish since the throughput and RTT values of each protocol tested are almost similar. Hence, it means that the UDP transmission data via selected tunneling does not affect the real performance of both protocols.

VII. CONCLUSION

Since the TCP packet is the largest contributor to the traffic network communication, it can be concluded that the 6to4 tunnel improper tool in industry or business needs. This clearly proves that the real ability of the TCP transmission data through the tunneling is reduced. However, the 6to4 tunneling mechanism is suitable to be implemented for early of transition period. This is because of such implementations mostly are based on research or related to the development of IPv6 experiment which not considering the network capabilities. In the near future, the necessity detail investigation will cover on the 6to4 tunneling overhead to identify the breakdown of overhead in order to improve the mechanism.

VIII. REFERENCES

[1] E. Karpilovsky, Gerber A., Pei D., Rexford J., and Shaikh A., "Quantifying the Extent of IPv6 Deployment," in *Passive and Active Network Measurement*. vol. Volume 5448/2009: Springer Berlin / Heidelberg, 2009, pp. 13-22.

[2] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," R. f. C. 2460, Ed.: Internet Engineering Task Force, 1998.

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

[4] B. Carpenter and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds," R. f. C. 3056, Ed.: Internet Engineering Task Force, 2001.

[5] B. Carpenter and C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels," R. f. C. 2529, Ed.: Internet Engineering Task Force, 1999.

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

[7] R. AlJaafreh, J. Mellor, and I. Awan, "Evaluating BDMS and DSTM Transition Mechanisms," in *UKSIM European Symposium, Computer Modeling and Simulation*, 2008, pp. 488-493.

[8] N. Shen and H. Smit, "Dynamic Hostname Exchange Mechanism for IS-IS," R. f. C. 2765, Ed.: Internet Engineering Task Force, 2000.

[9] K. Tsuchiya, H. Higuchi, and Y. Atarashi, "Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)," R. f. C. 2767, Ed.: Internet Engineering Task Force, 2000.

[10] S. Lee, M.-K. Shin, Y.-J. Kim, E. Nordmark, and A. Durand, "Dual Stack Hosts Using "Bump-in-the-API" (BIA)," R. f. C. 3338, Ed.: Internet Engineering Task Force, 2002.

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

[12] D. G. Waddington and C. Fangzhe, "Realizing the transition to IPv6," *Communications Magazine, IEEE,* vol. 40, pp. 138-147, 2002.

[13] J. Hagino and K. Yamamoto, "An IPv6-to-IPv4 Transport Relay Translator," R. f. C. 3142, Ed.: Internet Engineering Task Force, 2001.

[14] N. Bahaman, A. S. Prabuwono, and M. Z. Mas'ud, "Implementation of IPv6 network testbed: Intrusion detection system on transition mechanism," *Journal of Applied Sciences,* vol. 11, pp. 118-124, 2011.

[15] J. Udhayan and R. Anitha, "Demystifying and Rate Limiting ICMP hosted DoS/DDoS Flooding Attacks with Attack Productivity Analysis," in *Advance Computing Conference, 2009. IACC 2009. IEEE International*, 2009, pp. 558-564.

[16] Y. Xinyu, M. Ting, and S. Yi, "Typical DoS/DDoS Threats under IPv6," in *Computing in the Global Information Technology*, 2007, pp. 55-55.

[17] K. Cho, M. Luckie, and B. Huffaker, "Identifying IPv6 network problems in the dual-stack world," in *Proceedings of the ACM SIGCOMM 2004 Workshops*, Portland, OR, 2004, pp. 283-288.

[18] I. Raicu and S. Zeadally, "Evaluating IPv4 to IPv6 transition mechanisms," in *Telecommunications, 2003. ICT 2003. 10th International Conference on*, 2003, pp. 1091-1098 vol.2.

[19] L. Yuk-Nam, L. Man-Chiu, T. Wee Lum, and L. Wing Cheong, "Empirical Performance of IPv6 vs. IPv4 under a Dual-Stack Environment," in *Communications, 2008. ICC '08. IEEE International Conference on*, 2008, pp. 5924-5929.
[20] M. Aazam, I. Khan, M. Alam, and A. Qayyum, "Comparison of ipv6 tunneled traffic of Teredo and ISATAP over test-bed setup," in *Information and Emerging Technologies (ICIET), 2010 International Conference on*, 2010, pp. 1-4.
[21] C. M. Kozierok, *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference*, First ed.: No Starch Press, 2005.

IX. BIOGRAPHIES

Nazrulazhar Bahaman received the B.Eng. (hons.) degree in Electrical and Electronic Engineering and M.Sc. in Information Technology from Universiti Teknologi Mara, Malaysia in 1998 and 2002, respectively. He is a senior lecturer at Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka. He is currently doing his Ph.D. at Universiti Kebangsaan Malaysia. He was with the Faculty of Electrical Engineering, Universiti Teknologi Mara in 2000-2003. Before joining the university, he spent more than three years in industries such as Sapura IT and Hicom Communication. His research interests include computer networks and artificial intelligence.

Anton Satria Prabuwono received Engineer's degree in Electronics with cum laude (the Best Student Award) from Institute of Technology National Yogyakarta (Indonesia) in 1995 and BSc. in Computer Science with distinction from Padjadjaran University Bandung (Indonesia) in 2000. He holds Master in Management from University of Muhammadiyah Prof. Dr. Hamka Jakarta (Indonesia). He then received his PhD. in Industrial Computing (Machine Vision) from Universiti Kebangsaan Malaysia in 2006. He is currently an Associate Professor in the School of Information Technology, and Researcher in Center for Artificial Intelligence Technology (CAIT), Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM). He was with Institute of Electronics, National Chiao Tung University (Taiwan) in 2006 and the Department of Industrial Computing, Universiti Teknikal Malaysia Melaka (UTeM) in 2007-2008. He received Excellent Author Award from UTeM for his publications and research contributions in 2008 and Excellent Service Award from UKM in 2010. Before joining the university, he spent more than six years in industries such as Bumi Kaya Steel, Samsung Electronics, and The Coca-Cola Company. He was a Technical Manager at Coca-Cola Bottling Indonesia in 1997-2002. He was a Visiting Professor in European Union Master's Course in Mechatronic and Micro-mechatronic Systems (EU4M) at the Department of Mechanical Engineering and Mechatronics, Karlsruhe University of Applied Sciences (Germany). He is an author and co-author for more than 120 scientific papers in International Journals and Conferences. His research interests include machine vision, robotics, and automation.

Erman Hamid received the Bachelor's in Information Technology (with honours) from Universiti Utara Malaysia and Master's in Computer Science from Universiti Kebangsaan Malaysia, in 1998 and 2005, respectively. He is a senior lecturer at Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka. He is in the academics field since 1998 till now and his research interest includes computer networks and human computer interaction for networks area