International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:5, No:11, 2011

# Next Generation IP Address Transition Mechanism for Web Application System

Mohd. Khairil Sailan, Rosilah Hassan and Zuhaizal Zulkifli

***Abstract*—**Internet Protocol version 4 (IPv4) address is decreasing and a rapid transition method to the next generation IP address (IPv6) should be established. This study aims to evaluate and select the best performance of the IPv6 address network transitionmechanisms, such as IPv4/IPv6 dual stack, transport Relay Translation (TRT) and Reverse Proxy with additional features. It is also aim to prove that faster access can be done while ensuring optimal usage of available resources used during the test and actual implementation. This study used two test methods such asInternet Control Message Protocol (ICMP)ping and ApacheBenchmark (AB) methodsto evaluate the performance.Performance metrics for this study include aspects ofaverageaccessin one second,time takenfor singleaccess,thedata transfer speed and the costof additional requirements.Reverse Proxy with Caching featureis the most efficientmechanism because of it simpler configurationandthe best performerfrom the test conducted.

***Keywords*—**IPv4, IPv6, network transition, apache benchmark andreverse proxy

## I. Introduction

TODAY, there is still exists legacy web application systems with limited support for the Next Generation Internet Protocol address or Internet Protocol version 6 (IPv6). This includes usage of Services and Operating Systems (OS) such as Internet Information Service (IIS) version 5.0 on Microsoft Windows 2000, and IIS 4.0 on Windows NT. Internet Engineering Task Force (IETF) Request for Comments (RFC) 4213 stated that a Dual Stack and Tunnelingof IPv6 over IPv4can be usedduring network transitionprocess from IPv4 to IPv6.This situation willrequire additional hardware and software support between the end userandthe web application server. This method willsaddload on network administrators, system developers, will increase cost of training and maintenance operations.Therefore evaluation should be made to find the best solution that can suite with the current situation.

The main objectives of this study are todesign, simulate and identifysuitableIPv4toIPv6 transition mechanismforlegacy web application system.

Mohd. Khairil Sailan is a PhD student at Faculty of Information Science and Technology,Universiti Kebangsaan Malaysia and also with Jabatan Perkhidmatan Awam (e-mail: mkhairils@gmail.com)

Assoc. Prof. Dr. Rosilah Hassanis a senior lecturer at the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor(e-mail: rosilah@ftsm.ukm.my).

Zuhaizal Zulkifli is with Jabatan Perkhidmatan Awam, Blok C1 & C2, Kompleks C, Pusat Pentadbiran Kerajaan Persekutuan, 62510 W.P. Putrajaya (e-mail: zuhaizal@jpa.gov.my).

The remainder of this paper is structured as follows. Section II discussed with related transition mechanism. Section III, describedthe experimentprocess. In Section IV, we present the simulation resultsand analysis. Finally, we summarize our findings and conclude the paper in Section V.

## II. Transition Mechanism

There are many mechanisms for IPv6 network transition such as Dual stack, IPv6 over IPv4 tunneling, Transport Relay Translation (TRT), Stateless IP/ICMP Translation, 6to4, Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), Network Address Translation (NAT) 64 and Teredo, but in this paper we explain few of the mechanisms whichare related to this study.

### *A. Dual-Stack*

Dual-Stack IPv4/IPv6 or known as RFC4213 can be defined as a technique to produce full support for both IPv4 and IPv6 hosts and routers [1]. The main purpose of this technique is, a smooth transition can be made between IPv6 with IPv4 hosts and routers through even though it has a different environment and configuration.

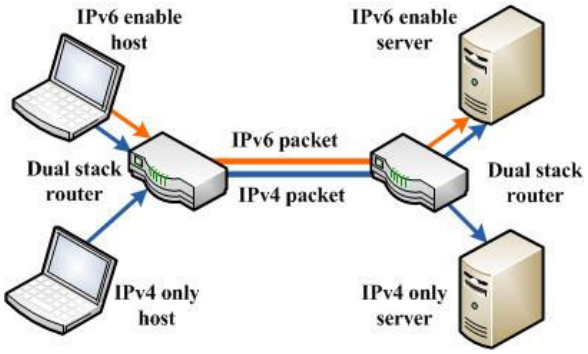


Fig. 1 Dual stack network

Fig.1 is an example of using a dual stack network.This method requires the preparation or configuration of each IPv4 and IPv6 protocols independently in advance. Host that has finished the process of configuration preparation is called IPv4/IPv6 host, also known as dual stack host. After the IPv6/IPv4 host is established, it can receive and transmit both IPv4 and IPv6 packets simultaneously [2]. This IPv4/IPv6 host is then able to communicate directly with IPv4 host as well as directly with IPv6 host using the original protocol packets according to the receiver. Dual Stack mechanism requires the availability of equipment and operating systems with the

ability to fully support it works with IPv4 and IPv6 addresses simultaneously. This may disruptthe daily operations due to the preparation and configuration of the Operating System. A study done by [3] shows that IPv6 performance is lower compared to IPv4 performance on dual stack environment. There is also a study shown that dual stack is vulnerable to worm attack and allow it to spread more easily in the network. Based on dual-stack worm attack mechanism, the researchers concluded the attack can be made in two stages of attacks in IPv6 and IPv4 attacks [4].

### *B. IPv6 over IPv4 Tunneling*

IPv6 over IPv4 tunneling allow access to the IPv6 networkover unmodified IPv4routing infrastructures [5]. Advantages IPv6 over IPv4 tunneling is this mechanism enables the Internet Service Provider (ISP)to deploy IPv6 as well as maintaining large existing domain of IPv4 network, but the disadvantage of this mechanism are it is hard to perform content filtering for packet flowing inside the tunnel and in some cases the tunnel cannot be establish when there is an intermediate IPv4 network devices that does not support tunneling. It is because tunneling is just an optional feature for IPv4 standard.

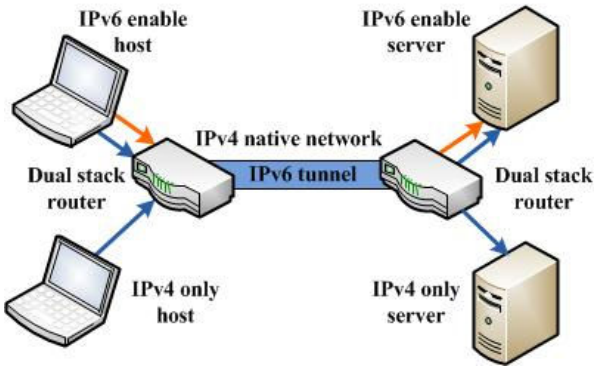


Fig. 2 IPv6 over IPv4 tunneling network

### *C. Transport Relay Translation*

Transport Relay Translation (TRT)or RFC 3142 mechanism proposed by IETF enables IPv6-only hosts to exchange Transmission Control protocol (TCP) and User Datagram Protocol (UDP) traffic with IPv4-only host or server [6]. Advantages of TRT are, no extra modification on IPv6-only initiating host, or that on IPv4-only destination host or server. TRT mechanism also does not have path Maximum Transfer Unit (MTU) and fragmentation issues. Disadvantages of TRT are, TRT does not support unidirectional multicast datagrams, TRT needs a stateful TRT system between the communicating peers similarto NAT systems and harder to relay IPsec tunnel. Fig.3 shows Domain Name Server-Application Layer Gateway (DNS-ALG) is required to translate IPv4 addresses into prefix IPv6 addresses containing the IPv4 destination. Gateway router is set up to route this prefix IPv6 address to TRT server which will allow the IPv6 traffic to communicate to the IPv4 only Internet or server.

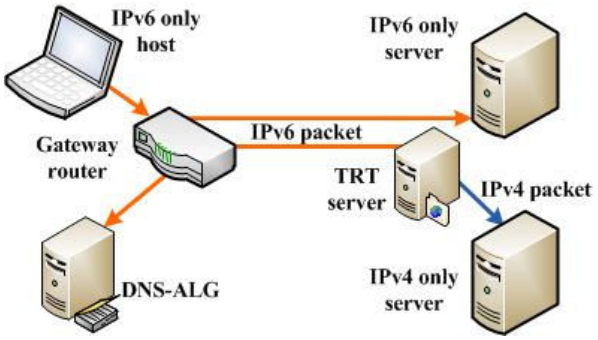


Fig. 3 TRT network

### *D. Dual Stack Reverse Proxy*

This method is nearly the same asDualStack but with additional reverseproxyfeature. Reverse proxy usually receive user request from Internet and placed at Service Provider's network or closer to server, whereas forward proxy generally receive request from local user and located in local network or closer to user. Fig. 4 is an example of computer network with dual stack reverse proxy sited near the servers.

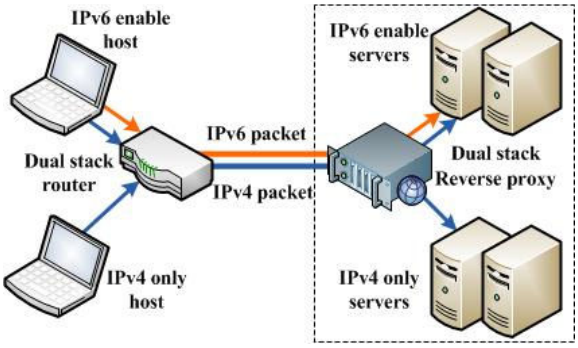


Fig. 4 Dual stack reverse proxy network

Advantages of reverse proxy are, load balancing can be configuredto distribute workload across multiple server, Secure Socket Layer (SSL) encryption, compression and content caching canbe implemented at the proxy thus reduce server processing load.

## III. Experiment Process

This study was carried out based on real-world problems which involve legacy web application system. Information was gathered from the problems faced by the Malaysian Public Service Department (PSD) during the transition from IPv4 to IPv6. Sample problems will be simulated for the purpose of this study.

Initially, the network information will be collected and the structure of the virtual network will be built using VMware software. Real-world situations will be simulated in the laboratory to find the optimum solution. Expected micro sample solution will be able to provide additional information to the macro problems involving other organizations to find solutions of the similarissues.

TABLE I
HARDWARE SPECIFICATION

| | Physical spec. | Virtualspec. (IPV6) | Virtual spec. (IPV4) |
|---|---|---|---|
| Model | HP Elite 8440p | VMware (FreeBSD 32bit) | VMware (FreeBSD 32bit) |
| CPU | Intel Core i7 | Intel | Intel |
| Memory | 8GB | 256MB | 256MB |
| HDD | 500GB | 8GB | 8GB |
| NIC | 1 x 10/100/1000 BaseT | 1 x 10/100/1000 BaseT (IPv6) | 1 x 10/100/1000 BaseT (IPv4) |

Table I shows the notebook physical specification and configured virtual specification used for the test. The notebook running Windows 7 Operating System (OS), the main software used for the simulation is VMware Workstation 7, FreeBSD for virtual OS,Lighttpd for web test, ICMP Ping, Apache Benchmark (AB), Faith for TRT/RFC 3142 test and Nginx for reverse proxy test.

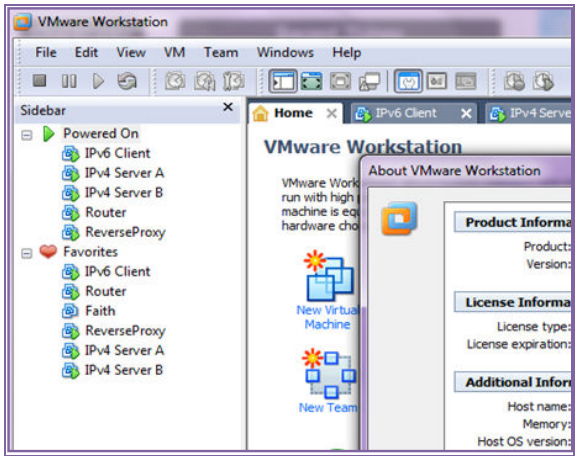


Fig. 5 VMware Workstation Software

Fig. 5 shows the main interface of the VMware Workstation software used for the test. There is no IPv6 server and no IPv4 client in Fig 5 because this example demonstrate actual scenario happened in Malaysian Public Service Department which still running a large legacy web application system on IPv4 domain and needs to serve users on IPv6 network.

Ping test was used to check the path connectivity between the IPv6 only client and the IPv4 only server and theApache benchmarktestswill only be madeif thepingtestsucceeds. The parameters used for the Apache benchmark are10000 requests with 5 requests to perform at a time. Fourtestscenarioswere selectedthat are TRT mechanism, reverse proxy without any additional feature, reverse proxy with caching feature, reverse proxy with compression and reverse proxy with load balancing mechanism. The test was conducted 5 times for each scenario and the average result was used to plot the graph. Apache benchmarktests for dualstackmechanismis notdone because itwas failed inthe Ping test. There is no connectivity between IPv6 only client and IPv4 only legacy server.

## IV. RESULTS

This section will assessthe performance ofdifferenttransition mechanism. The metrics are average access in one second, time taken for single access,data transfer speed and cost for additional requirements.

### *A. Average Access in One Second*

Average access in one second means the average number of access can be executed by a mechanism within a period of one second. The results of the comparison metricswill show which mechanism that could provide transition most services in a period of time. This is important to ensure there is no bottle-neck on the access request unit intermediary server located between the actual IPv6Client and IPv4Server. The higher the number of access per second indicates higher performance.
Reverse Proxy with Caching feature was recorded the highest average access of a second among all of the mechanism, a total of 367.84 accesses in a second. This followed the TRT mechanism which was recorded at 272.97 accesses in a second. Reverse proxy with compression at 136.18 accesses and reverse proxy with load balancing at 134.69 accesses in a second.Whilethe averageaccess ofa lowestaccess recorded by theReverseProxywith noadditional features mechanism at 131.53accesses in a secondaccess.

This proves caching feature is very useful for improving the performace of web application access during IPv4 to IPv6 transition process. Based on this test, the difference between the highest and lowest performance was vpt.[367.84-131.53)/131.53x100] =180%

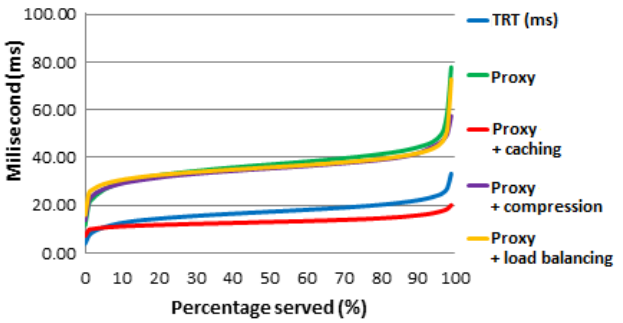


Fig. 6 Comparison Graphof time taken for 10,000 accessof Apache Benchmark test for each mechanism

The graph (Fig.6) shows the Proxy with caching mechanism is the fastest compared to the others. It startsmuch slower than theTRTdue tonewcachingdata storageprocessstarts. Then it begins to speed up. This isbecause the Ipv6 client starts to accessthe datafrom thecacheinstead ofthe actualIPv4server.

### *B. The Time Taken for Single Access*

The second factoraffecting theperformance ofaccessis the timetakenfor singleaccess.Thismetricis defined asthe average time in millisecond (ms) taken by eachaccess.As the hardwareand virtual serverhave theOperating System, CPUresources, hard drive andRAMarethe samesize, thismatrixcan assist us to choose thebestoptimal mechanism

for the next generation IP address transition.Inthis metric, lowertime taken (ms) is actually the better performance.

Based on the test, ReverseProxy with cachingfeaturesis the best which took 2.72ms to complete a single access. This followed byTRT at3.66 ms and Reverse Proxy with compression at 7.35 ms. The two lowest performance mechanism are Reverse Proxy with balancing and Reverse Proxy with no additional feature at 7.42 ms and 7.60 ms respectively. This provescachingfeatureis also usefulin ensuringhigh performancefor single access time.

### C. Data TransferSpeed

The third factor affecting the performance of web applications access isData TransferSpeed. This factor is defined as the size of application data can be transferred to the IPv6 client within 1 second. High-speed mechanism demonstrates the ability to use the resource processing and network optimally.

Reverse Proxy with caching feature once again recorded the highest speedat 31204.61 kilobytes per second (KBps), followed by the Reverse Proxy with compression at 11552.06 KBps, Reverse proxy with load balancingat 11425.64 KBps, Reverse Proxy without additional feature at 11157.60 KBps and the slowest speed is TRT mechanism at 134.36 KBps.

### D. Cost for Network Transition

Comparison from the main three metrics shows that Reverse Proxy with caching is the best mechanism, but it is also important to add cost as a consideration during the IPv6 transition process. This is because it has a big impact on business annual operating budget.For example, currently there are 9 legacy web application servers running on Windows 2000 OS. Without transition mechanism, the OS should be upgrade to Windows Server 2008 Enterprise to support the IPv6 clients. Total cost to upgrade for 9 unitsof servers is (9 x MYR 5,500) = MYR 49,500. If the transition mechanism was used, the total cost should be for 1 unit of server hardware for the Reverse proxy with caching feature unit which is, 1 x MYR 8,000 = MYR 8,000. There is no need to spend on OS license and tool as both of the items are open source and can be downloaded from the Internet for free. Thus,the total saving would be MYR 49,500 – MYR 8,000 = MYR 41,100.

## V. Conclusion

The test conducted for this study shows that Dual Stack Reverse Proxy with caching feature is the best solution for the next generation IP address transition mechanism. It perform better than the other mechanism, simpler to implement because there is no need to do reconfiguration on client and server site, lower in cost and suited with those who need to enable IPv6 clients to access legacy web application servers running on IPv4 network address.

Ongoing and future researcharea that we will embark on isa test scenario which involves a test bed with a multi service router and experiment of wired and mobile IPv6 network performance test. Once all data from test scenarios have been collected and analyzed, detail characteristic will be applied in the next simulation process. Simulation result will be evaluated with formal method. Then accurate model and simulation process will be used for network acceleration and extrapolation.

## Acknowledgment

This research is funded by Jabatan Perkhidmatan Awam (JPA) and Universiti Kebangsaan Malaysia. The research group is known as Network Management Group of Computer Science Department, Universiti Kebangsaan Malaysia. Please visit the website at http://www.ftsm.ukm.my/network for further detail.

## References

[1] E. Nordmark, and R. Gilligan “Basic Transition Mechanisms for IPv6 Hosts and Routers”, RFC4213, Oct 2000.
[2] M.K. Sailan, R. Hassan and A. Patel. “A Comparative Review of IPv4 and IPv6 for Research Test Bed,” International Conference on Electrical Engineering and Informatics 2009,pp. 427-433.
[3] M.K. Sailan and R. Hassan. "Impact of TCP Windows Size on IPv4 and IPv6 Performance," International Journal of Computer Science and Network Security 2009, pp. 129-133.
[4] Q. Zheng, T. Liu, X. Guan, Y. Qu, and N. Wang. "A New Worm Exploiting Ipv4-Ipv6 Dual-Stack Networks," ACM 2007, pp 9-15.
[5] R.Gilligan and E. Nordmark. "Basic Transition Mechanisms for Ipv6 Hosts and Routers," RFC 4213, Citeseer2005.
[6] J. Hagino and K. Yamamoto. "An Ipv6-to-Ipv4 Transport Relay Translator," RFC 3142 2001.

**Mohd. Khairil Sailan** received his Diploma in Electrical Engineering, B.S. in Data Comm. Networking and M.S. degree in Information Technology from Universiti Teknologi MARA (UiTM) Malaysia in 1998, 2003 and 2006 respectively. Currently, he is a PhD student at the Computer Science Department of Universiti Kebangsaan Malaysia (UKM). His research interest is in IPv6 Network Performance Management.

**Dr. Rosilah Hassan** received her first degree from Hanyang University, Seoul, Republic of Korea in Electronic Engineering (1996). She work as an Engineer with Samsung Electronics Malaysia, Seremban before joining Universiti Kebangsaan Malaysia (UKM) in 1997. She obtains her Master of Electrical Engineering (M.E.E) in Computer and Communication from UKM in 1999. In May 2008, she received her PhD in Mobile Communication from University of Strathclyde. Her research interest is in mobile communication, networking, 3G, and QoS. She is a senior lecturer at UKM for more than 10 years.

**Mohd Zuhaizal Zulkifli** received his Matriculation in Sains, B.Eng. in Computer and Communication System degree from Universiti Putra Malaysia(UPM) Malaysia in 1997 and 2001 respectively. Currently, he is a Master student at the Computer Science Department of Universiti Kebangsaan Malaysia (UKM). His research interest is in IPv6 Network Performance Management.