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 transition mechanisms, 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 as Internet Control Message Protocol (ICMP)ping and ApacheBenchmark (AB) methodto evaluate the performance. Performance metrics for this study include aspects of averageaccess time in one second, time taken for singleaccess, the data transfer speed and the cost of additional requirements. Reverse Proxy with Caching feature is the most efficient mechanism because of its simpler configuration and the best performer from the test conducted.

Keywords—IPv4, IPv6, network transition, apache benchmark and reverse 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 Tunneling of IPv6 over IPv4 can be used during network transition process from IPv4 to IPv6. This situation will require additional hardware and software support between the end user and the web application server. This method will add load 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 to design, simulate and identify suitable IPv4/IPv6 transition mechanisms for legacy 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: mksailan@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@fsnm.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 described the experiment process. In Section IV, we present the simulation results and 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 which are 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 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 disrupt the 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 network over unmodified IPv4 routing 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.

Advantages of IPv6 over IPv4 tunneling are:

1. Enables the Internet Service Provider (ISP) to deploy IPv6 as well as maintaining large existing domain of IPv4 network.
2. Provides a way to connect IPv6 networks that are not directly connected.
3. Allows for gradual migration from IPv4 to IPv6.

Disadvantages of IPv6 over IPv4 tunneling are:

1. Requires configuration and setup on both ends of the tunnel.
2. Can be vulnerable to certain types of attacks.

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 similar to 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.

Advantages of TRT are:

1. No extra modification on IPv6-only initiating host, or that on IPv4-only destination host or server.
2. Does not have path MTU and fragmentation issues.

Disadvantages of TRT are:

1. Requires extra configuration and setup.
2. Relies on stateful systems.

D. Dual Stack Reverse Proxy

This method is nearly the same as DualStack but with additional reverse proxy feature. 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.

Advantages of reverse proxy are:

1. Load balancing can be configured to distribute workload across multiple server.
2. Secure Socket Layer (SSL) encryption, compression and content caching can be 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 similar issues.
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](image)

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 the Apache benchmarkstestwill only be madeif thepingtestsucceeds. The parameters used for the Apache benchmark are 10000 requests with 5 requests to perform at a time. Four testscenarioswere 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 benchmarkstests for dual stack mechanismsnotdone because it was failed in the ping test. There is no connectivity between IPv6 only client and IPv4 only legacy server.

### TABLE I

<table>
<thead>
<tr>
<th>Model</th>
<th>Physical spec.</th>
<th>Virtual spec. (IPV6)</th>
<th>Virtual spec. (IPV4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP Elite 8440p</td>
<td>VMware (FreeBSD 32bit)</td>
<td>VMware (FreeBSD 32bit)</td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>Intel Core i7</td>
<td>Intel</td>
<td>Intel</td>
</tr>
<tr>
<td>Memory</td>
<td>8GB</td>
<td>256MB</td>
<td>256MB</td>
</tr>
<tr>
<td>HDD</td>
<td>500GB</td>
<td>8GB</td>
<td>8GB</td>
</tr>
<tr>
<td>NIC</td>
<td>1 x 10/100/1000</td>
<td>BaseT (IPv6)</td>
<td>BaseT (IPv4)</td>
</tr>
</tbody>
</table>

This section will assess the performance of different transition 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 metrics will show which mechanism that could provide transition most services in a period of time. This is important to ensure there is no bottleneck on the access request unit intermediary server located between the actual IPv6 client and IPv4 server. 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. While the average access of a lowest access recorded by the Reverse Proxy mechanism at 131.53 accesses in a second accesss.

This proves caching feature is very useful for improving the performance of web application access during IPv4 to IPv6 transition process. Based on this test, the difference between the highest and lowest performance was $\frac{367.84-131.53}{131.53} \times 100 = 180\%$

The graph (Fig. 6) shows the Proxy with caching mechanism is the fastest compared to the others. It starts much slower than the TRT due to new caching data storage processes. Then it begins to speed up. This is because the IPv6 client starts to access the data from the cache instead of the actual IPv4 server.

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

The second factor affecting the performance of access is the time taken for single access. This metric includes time to connect, time to establish a connection, and time to receive data. The hardware and virtual server have the operating system, CPU resources, hard drive and RAM. The server size, metrics such as speed, time and server size assist us to choose the best optimal mechanism.
for the next generation IP address transition. In this metric, low time taken (ms) is actually the better performance.

Based on the test, ReverseProxy with caching feature is the best which took 2.72 ms to complete a single access. This followed by TRT at 3.86 ms and Reverse Proxy with compression at 7.35 ms. The two lowest performance mechanisms are Reverse Proxy with balancing and Reverse Proxy with no additional feature at 7.42 ms and 7.60 ms respectively. This proves caching feature is also useful in ensuring high performance for single access time.

C. Data Transfer Speed

The third factor affecting the performance of web applications access is Data Transfer Speed. 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 speed at 31206.61 kilobytes per second (Kbps), followed by the Reverse Proxy with compression at 11552.06 Kbps, Reverse proxy with load balancing at 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 upgraded to Windows Server 2008 Enterprise to support the IPv6 clients. Total cost to upgrade for 9 unit of 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 performs better than the other mechanism, simpler to implement because there is no need to reconfigure 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 research area that we will embark on is a test scenario which involves a test bed with a multi 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


Mohd. Khaирil 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. Rosi лah 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 Zuhairal Zuliπli 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.