UACEE International Journal of Advances in Computer Science and its Applications – IJCSIA
Volume 3 : Issue 2 [ISSN 2250 – 3765]
Publication Date : 05 June 2013

Performance Measurements Analysis of Dual Stack IPv4-IPv6

Febby Nur Fatah
Department of Electrical Engineering
Gunadarma University
Depok, Indonesia
feby@staff.gunadarma.ac.id

Adang Suhendra
Department of Informatics Engineering
Gunadarma University
Depok, Indonesia
adang@staff.gunadarma.ac.id

M Akbar Marwan
Department of Information Systems
Gunadarma University
Depok, Indonesia
akbar@staff.gunadarma.ac.id

Henki Firdaus
Department of Information Systems
Gunadarma University
Depok, Indonesia
henki@staff.gunadarma.ac.id

Abstract*—Internet Protocol version 6 (IPv6) is the IP Next Generation Protocol (IPng) that will replace the current IPv4 which has been used for 30 years, but there is problem in IPv4 on the allocation of IP addresses. This problem can be overcome by utilizing various strategies in IPv4 to IPv6 migration such as dual stack IPv4-IPv6. This research analyzed the performance of dual stack IPv4-IPv6 system in University network by using of jitter and delay period in interconnection. We calculated the jitter and delay period by transferring various files with different size and the result shows that average of jitter period is around sizes transfer The result shows that dual stack system is reliable implementation for migration of IPv4 to IPv6 system.

***Keywords*—IPv6, IPv4, dual stack, migration strategy IPv6, jitter**

I. Introduction

Internet Protocol version 6 (IPv6) is an improvement of IPv4, which currently faces many challenging issues. The rapid diffusion of the Internet and development of high-speed broadband networks have posed the problem of limited IPv4 address space on the Internet, while many applications have been developed for million devices which consume huge number of IP address allocations, such as mobility, tiny server nodes, appliances, global reachability and end-to-end communications. IPv6 has been developed to overcome this problem, because IPv6 is an important building block for these new applications. At the same time, the current deployment of IPv4 network and applications will remain dominant for a significant part of the network protocol. The IPv4 address structure is based on a 32-bit address length. It can manage about 4 billion addresses, but cannot be assigned to everyone living in the world, which contains about 6.3 billion people. However, the IPv6 address structure is based on a 128-bit address length and therefore can be used to assign more than 5x1028 addresses to every person in the world. This brings to an almost infinite address space offering.

In order to migrate the huge user properties (e.g., applications, network environments) built into IPv4 to IPv6, operating systems, middleware, and applications adapted for address length and IPv6 must be upgraded. These major changes tend to a high risk, and many subjects remain to be resolved before achieving a smooth migration from existing IPv4 properties to IPv6. Accordingly, this project will design a simple network that runs simultaneously on IPv4 and IPv6 end-to-end network as a solution of IPv4 to IPv6 migration strategy. The measurement and analyze network performance as well of dual stack IPv4-IPv6 are the basic knowledge of applying one of migration strategies[2].

II. Theoretical Background

IP version 4 (IPv4) is the current TCP/IP addressing technique being used on the Internet[5]. Address space for IPv4 is quickly running out due to the rapid growth of the Internet and the development of new Internet-compatible technologies such as the IP addressable telephone. IP version 6 (IPv6) is the proposed solution for expanding the possible number of users on the Internet. IPv6 is also called IPng, the next generation IP [1].

IPv6 uses a 128-bit address technique, compared to IPv4's 32-bit address structure[3]. IPv6 provides for a large number of IP addresses (2^{128}) and written in hexadecimal rather than dotted decimal. For example, the following is a 32 hexadecimal digit IPv6 address (Note: 32 hex digits x 4 bits/hex digit = 128 bits):

6789:ABCD:1234:EF98:7654:321F:EDCB:AF21

Such address noted is classified as a full IPv6 address. The full means that all 32 hexadecimal positions contain a value other than 0. The difference between IPv4 and IPv6 can be seen briefly in the following table 1.

TABLE I. THE DIFFERENCE IN IPV4 AND IPV6

Type of Comparison	IPv4	IPv6
Address Length	32 bits	128 bits
Notation	Decimal (4 fields)	Hexadecimal (8 fields)
HostID Length	2-24 bits	64 bits
NetID Length	7-30 bits	61 bits
Number of host	3.7×10^{9}	4.25×10^{37}
Number of subnet	2^{7}- 2^{30}	2^{61}
Header	20 octets (changeable)	40 octets (fixed)

Migration Strategies Towards IPv6

IP migration to IPv6 can be divided into two ways, namely the aggressive migration and passive migration. In the aggressive migration, the entire infrastructure to be replaced with IPv6 and IPv4 directly disposed. This method is obviously not possible to be implemented at this time, because only a few of the user, server, and service providers that already support IPv6. In the passive migration, new services and/or infrastructure of IPv4, which migrated to IPv6, are not discarded but still conserved. IPv4 and IPv6 of an address are implemented simultaneously [4].

There are several technologies in the passive migration, including dual-stack, tunneling, or translator.

- Dual-stack is the most basic method to build a network of IPv6 and IPv4 simultaneously during the migration process. Many devices that support IPv6, such as terminals, network devices, or servers, features a dual-stack. In this method, all devices from end to end must support dual-stack.
- Tunneling can be interpreted as building a direct line of communication that between the second virtual site. Tunneling makes communication possible with a packet encapsulation protocol into another protocol on the network. Encapsulation and decapsulation packets are automatically in both ends of the tunnel. Both sites can be connected without depending on the type of communication used between the two. This technology is the most widely used because of connections with any protocol can be built on either site which depend on the configuration without relaying network. Several types of such tunneling are 6to4, Teredo, 6rd, DS-Lite, and ISATAP. Figure 1 is IPv4 in IPv6 tunneling technology. At this stage, service providers have to build an IPv6 network to connect the gateway router and the CPE. However, the customers do not use IPv6.

Figure 1. DS-Lite configuration
Source: Permana (2011)

Translator makes communication possible with protocol conversion that does not fit the protocol border. This method is used for communication between devices with IPv4 only and IPv6 only. In dual-stack method and the second tunneling, device user has the same protocol (IPv4 or IPv6 with IPv4 with IPv6). This method can be classified into three layers depending on which one is used for termination and protocol conversion. All these three are conversion header in the IP layer, transport layer TCP relay, and proxies at the application layer. Figure 2 namely NAT64, it is the translation on the router from the metro network (IPv4) to network service provider (IPv6). At this stage the end-users already use the device IPv6.

Figure 2. NAT64 configuration
Source: Permana (2011)

III. Methodology

The methodology of this project is divided into two huge stages: network design and performance measurements. We developed the dual stack model of network that connected to two hosts with dual stack feature through dual stack network which connected to two routers. As addition, to determine the performance of dual-stack network we designed dual stack network connection between host on the internal dual stack network model, with a campus server that has been running as a dual stack devices under one of ISP in Indonesia. Connection is provided by using direct server which remotely access from a host residing on the internal network.

From this connection prototype, the second stage as the results of measurements of various parameters which also be used to measure the performance of the internal dual stack network model. These performance parameters are round trip time, jitter, packet loss, and throughput. We measure the results of dual stack network model with minimal hops and with many hops.

A. *Mechanism of Network Design*

The design of dual stack network composed by five main stages:

1. Dual stack network configuration that considers number of end-user and router in a network.
2. Determine the network address for each component. We implemented two different networks: from NOC1 host to Router1 and from Router2 to a laptop host.
3. Determine routing path by using static routing path.
4. IP forwarding function to enable connectivity for IPv4 and IPv6 network on each router and each host as dual stack devices.
5. Conduct the simple network for one of local network which built by dividing two hosts with two routers in the different address network adjustment.

Figure 3 describes the dual stack network model for the experiment.

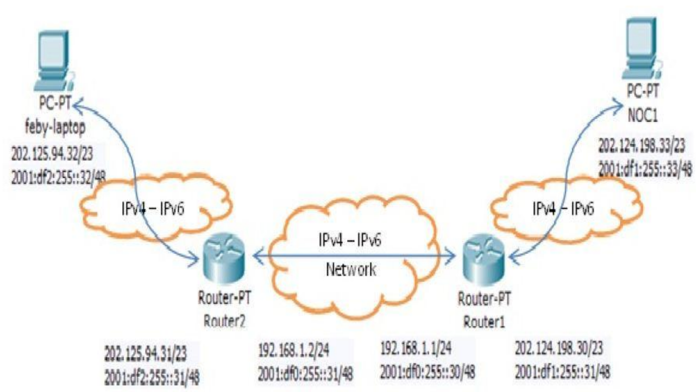

Figure 3. Dual stack network model

B. *Dual Stack Network Implementation*

In this research we used static address configuration which includes the IP address, prefix length (or subnet mask) and DNS servers. IPv6 nodes can be manually configured as IPv4 nodes [Blanchet, 2006]. Our model consists of two hosts and two routers connected through two different networks with own address.

C. *Routing Path*

The routing table of the dual stack is manually defined and utilizes the IBM System x3250 M3. Figure 3 describes the basic implementation of routing in the network. Router1 has two interfaces, which of each connected to the network 192.168.1.0/24 and 202.124.198.0/23 for IPv4, and connected to the network 2001:df0:255::0/48 and 2001:df1:255::0/48 for IPv6. Router2 is connected directly to the network 192.168.1.0/24 and 202.125.94.0/23 for IPv4, as well as network 2001:df0:255::0/48 and 2001:df2:255::0/48 for IPv6. The Table II through Table V are configuration of routing entries for the routing table on each router.

TABLE II. ROUTER1'S IPV4 ROUTING TABLE

Destination	Gateway	Genmask	Flags	Iface
192.168.1.0	0.0.0.0	255.255.255.0	U	eth1
169.254.95.0	0.0.0.0	255.255.255.0	U	usb0
202.124.198.0	0.0.0.0	255.255.254.0	U	eth0
202.125.94.0	192.168.1.2	255.255.254.0	UG	eth1
169.254.0.0	0.0.0.0	255.255.0.0	U	eth1
0.0.0.0	202.124.198.1	0.0.0.0	UG	eth0

TABLE III. ROUTER2'S IPV4 ROUTING TABLE

Destination	Gateway	Genmask	Flags	Iface
192.168.1.0	0.0.0.0	255.255.255.0	U	eth1
169.254.95.0	0.0.0.0	255.255.255.0	U	usb0
202.124.198.0	192.168.1.1	255.255.254.0	UG	eth1
202.125.94.0	0.0.0.0	255.255.254.0	U	eth0
169.254.0.0	0.0.0.0	255.255.0.0	U	eth0
0.0.0.0	202.125.94.1	0.0.0.0	UG	eth0

TABLE IV. ROUTER1'S IPV6 ROUTING TABLE

Destination	Next Hop	Flag	If
2001:df0:255::/48	::	U	eth1
2001:df1:255::/48	::	U	eth0
2001:df2:255::/48	2001:df0:255::31	UG	eth1
fe80::/64	::	U	eth0
fe80::/64	::	U	eth1
fe80::/64	::	U	usb0
::/0	::	!n	lo
::1/128	::	Un	lo
2001:df0:255::/128	::	Un	lo
2001:df0:255::30/128	::	Un	lo
2001:df1:255::/128	::	Un	lo
2001:df1:255::31/128	::	Un	lo
fe80::/128	::	Un	lo
fe80::/128	::	Un	lo
fe80::/128	::	Un	lo
fe80::5cf3:fcff:fe2d:d2c9/128	::	Un	lo
fe80::5ef3:fcff:fe2d:d2c6/128	::	Un	lo
fe80::5ef3:fcff:fe2d:d2c7/128	::	Un	lo
ff00::/8	::	U	eth0
ff00::/8	::	U	eth1
ff00::/8	::	U	usb0
::/0	::	!n	lo

TABLE V. ROUTER2'S IPV6 ROUTING TABLE

Destination	Next Hop	Flag	If
2001:df0:255::/48	::	U	eth1
2001:df1:255::/48	2001:df0:255::30	UG	eth1
2001:df2:255::/48	::	U	eth0
fe80::/64	::	U	usb0
fe80::/64	::	U	eth1
fe80::/64	::	U	eth0
::/0	::	!n	lo
::1/128	::	Un	lo
2001:df0:255::/128	::	Un	lo
2001:df0:255::31/128	::	Un	lo
2001:df2:255::/128	::	Un	lo
2001:df2:255::31/128	::	Un	lo
fe80::/128	::	Un	lo

fe80::/128	::	Un	lo
fe80::/128	::	Un	lo
fe80::5cf3:fcff:fe2d:db20/128	::	Un	lo
fe80::5ef3:fcff:fe2d:db1d/128	::	Un	lo
fe80::5ef3:fcff:fe2d:db1e/128	::	Un	lo
ff00::/8	::	U	usb0
ff00::/8	::	U	eth1
ff00::/8	::	U	eth0
::/0	::	!n	lo

D. *IP Forwarding*

After the network address and routing path statically configured, then a command is sent to each router to enable IPv4 and IPv6 network and to communicate all devices using both protocols. Similar to the router, each host has a command to activate the two pathways on the IPv4 and IPv6. This is the interface configuration to enable all devices in a dual stack network.

E. *Dual Stack Remote Server*

This scenario describes an incoming host on the Internet network, connecting with a dual stack server remotely. A host that has not been functioning as a dual stack devices, need to utilize the existing tunnel broker on the internet to get IPv6 address on its network configuration.

After receiving an IPv6 address, the host can be said to serve as a temporary dual stack devices. Then we can make the connectivity between a host and dual stack server, using the same tools within the experiments on the dual stack model that was built previously.

As seen on the dual stack model that has routing path on each IP address, this dual stack remote server also has its own routing path. Routing configuration can be known by using `traceroute` command to the server from host side. The configuration are summarized in figure 4. That figure describes how many hops are needed to reach the server. In IPv4 connection, there are shown a few number of hops. Otherwise in IPv6 connection, shown almost twice number of IPv4 hops. It caused by in IPv6 connection, host must to reach server of tunnel broker first, then go back to campus server, surely it tooks many hops to go through.

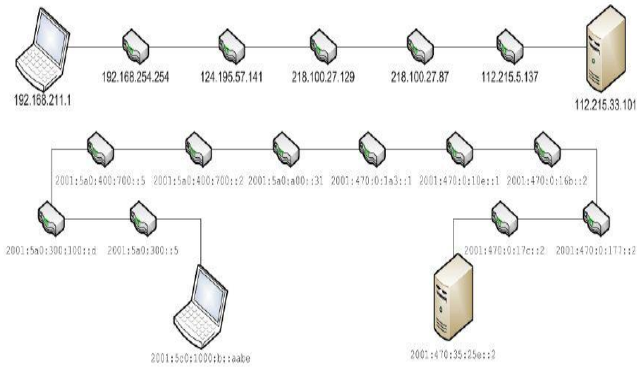

Figure 4. Traceroute IPv4-IPv6 address from client to remote server

IV. Result and Discussion

A. *Performance Measurements and Network Analysis*

Network performance analysis techniques used in this research is the method by direct measurement of performance on the model or network prototype has been designed and implemented. In this section also directly measured the performance of dual-stack network of connections between hosts on the internal network model with one server on campus that has been running as a dual-stack devices. On these dual stack network is measured several parameters of performance that became a benchmark in analyzing network performance. Those parameters are round trip time (RTT), jitter, packet loss, and throughput.

- RTT is the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgement of the signal to be received. RTT is measured by using `ping` command on each host to flood traffic each other.

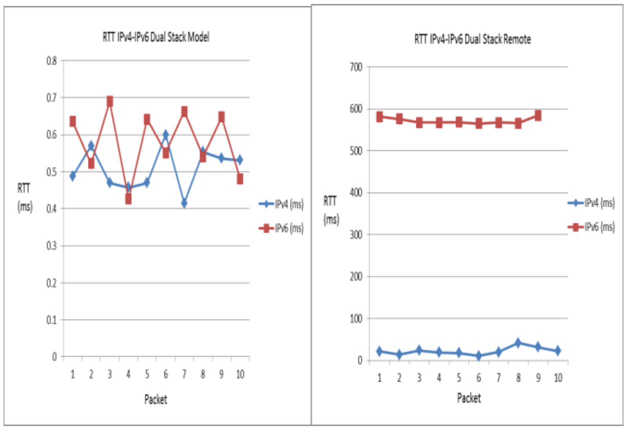

Figure 5. RTT IPv4-IPv6 address on client network model and client-remote server

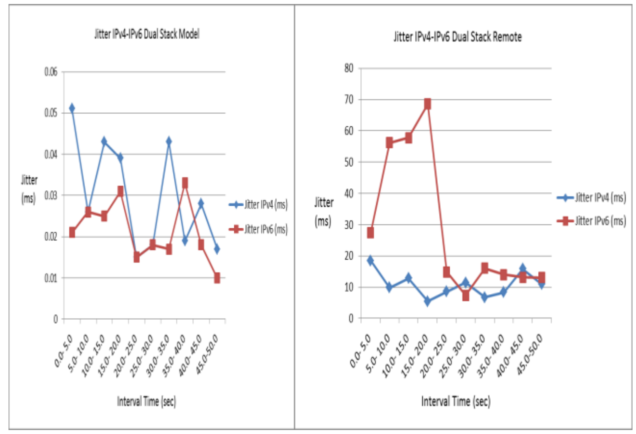

Figure 6. Jitter IPv4-IPv6 address on client network model and client-remote server

Figure 5 is the result of testing round trip time on a dual stack network model that has been built. In general, the difference in round trip time on IPv6 connection do not show significant differences. Round trip time of IPv6 connection obtained to within 13.75% longer time than the IPv4 connection. This difference occurs because it basically has IPv6 packet header 20 bytes larger than the packet header of IPv4. In the result of client-remote server, it shows what a far the differences between IPv4 and IPv6 connections. The difference is absolutely high even reach 2445.94 %. It is certainly strongly in influenced by the routing paths are used, either by IPv4 networks and IPv6 networks.

Routing path difference is caused by the use of tunnel broker on the host to obtain an IPv6 address so that the host can communicate with a server that has been running as dual stack devices.

- Jitter is the delay variation caused by the long queues in a data processing and reassemble packets data in the late delivery due to failure before. Jitter between the start and end points communication must be <150 ms.

Figure 6 represents the difference in jitter that occurs on both IPv4 and IPv6 connections on a simple network model. Fluctuations are seen suggests that the spread of the jitter on IPv4 connection larger, meaning that the spread on IPv6 connection better and more stable. The differences shows 28.43% better for IPv6 connection. The mean jitter of IPv6 is counted also smaller than the IPv4 connection. This is due to the flow label field in IPv6 packet header, which allows the routers have direct access to the flow label and don't have to guess or find the flow using the transport and application data.

And the next figure shows also what a high jitter time which resulting in dual stack IPv4-IPv6 remote server. It reaches 165.60% differences. These jitter caused also caused by routing path and variances of data sizes.

- Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss can be caused by a number of factors including congestion, corrupted packets rejected in transit, faulty networking hardware, and distance between the transmitter and receiver.

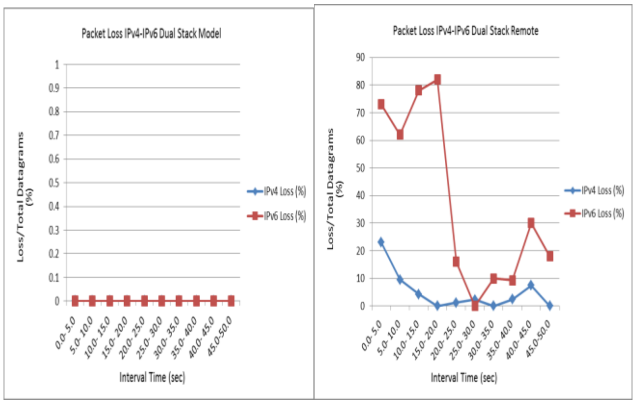

Figure 7. Packet loss IPv4-IPv6 address on client network model and client-remote server

As shown in figure 7 can be ascertained that there is no packet loss on a simple network model. The absence of packet loss that occurs in this model is due to both networks are connected only through two routers with a very close distance. Not many hops that must be passed by a packet to reach the destination address. So, with the existing minimum hop, then the percentage obtained 0% loss per total datagrams is sent, both for IPv4 and IPv6 connections.

Otherwise, for dual stack IPv4-IPv6 with server remotely, next figure shows a significant fluctuating of packet loss between IPv4 and IPv6 connections. It reaches 655.09% differences packet loss IPv6 to IPv4.

- Throughput used to refer to the actual bandwidth that is available to a network, as opposed to theoretical bandwidth. Throughput is the total time used to send bits of data packets successfully per unit time.

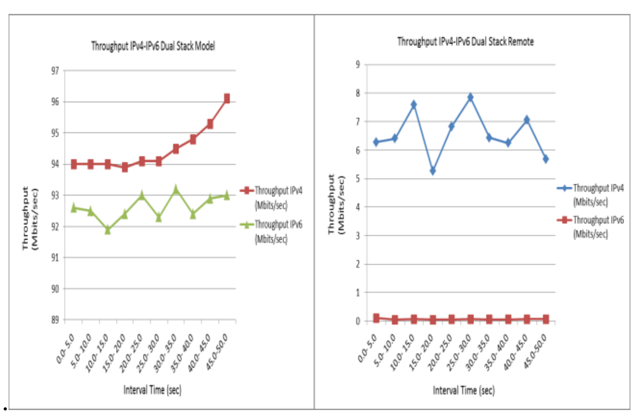

Figure 8. Throughput IPv4-IPv6 address on client network model and client-remote server

Figure 8 is the result of testing throughput on a dual stack network model that has been built. In general, the difference in throughput on IPv6 to IPv4 connection do not show significant differences. Throughput of each network are recorded on this dual stack network, has a light distinction for 1.97 % better for IPv4 connections. This is also possible because basically the IPv6 packet has a header 20 bytes larger than the IPv4 packet.

And again, otherwise of dual stack network model, dual stack remote server in the next figure shows a very high percentages of differences between IPv4 and IPv6. It reaches 99.08% better for IPv4 connection. Also caused by routing path with data taken per 50 seconds interval time.

V. Conclusion

The implementation and measurement of dual stack network model has been accomplished. A number of findings has been identified during the implementation and measurement phases as follows:

1. In order to build a dual stack network, it is necessary devices and network infrastructures that has supported IPv6 connections. The whole system of dual stack must be IPv6 compatible from source address to destination address.
2. Dual stack network that has been built with server remotely couldn't be compared because it has been clearly have different routing paths between its IPv4 and IPv6 connections. This network scenario is just an example of a dual stack network where the server has been getting a real IPv6 address of the provider. But can not be said to be the real dual stack network because in the host side still use tunnel broker for getting IPv6 addresses.
3. In general, dual stack network performance parameters that showed the most influential is the jitter. Which recorded an IPv6 connection is more stable and there is less jitter than IPv4.
4. Dual stack is the most basic and simple method that feasible to build an IPv6 network and IPv4

simultaneously during the migration process, particularly in the university area.

The IPv6 header doubles in size to 40 octets compared to the IPv4 header is an important issue on limited bandwidth. For the next researches, it may possible using multiple header compression schemes that have been designed over time to reduce header size for the higher performance of IPv6 connection.

References

[1] Beasley, Jeffrey S. *Networking Technology 2nd Edition*. Pearson Education, Inc., Boston, MA.. 2009

[2] Blanchet, Marc.. *Migrating to IPv6 : A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks*. John Wiley and Sons, Ltd, London. 2006

[3] Forouzan, Behrouz A.. *Data Communications and Networking 4th Edition*. The McGraw-Hill Companies, Inc., New York.,2007

[4] Permana, Rama. *Strategi Implementasi IPv6 Pada Jaringan Akses Broadband Telkom*. Institut Teknologi Telkom, Bandung, 2011.

[5] Postel, Jon. *Internet Protocol*. IETF RFC 791, California, 1981