ESTABLISHMENT OF IPV6 NETWORK USING TUNNELLING MECHANISM ON INTRANET

Erman, H., Zaki, M.M., Nazrulazhar, B., Faizal, M.A., Nor Azman, M.A., and Yahaya, A.R.

Faculty of Information and Communcation Technology
Universiti Teknikal Malaysia Melaka (UTeM)
Ayer Keroh, Melaka

Author e-mail: erman@utem.edu.my,

ABSTRACT: The emerging Internet Protocol version six (IPv6) has promises several benefits that can overcome the weaknesses of the current Internet Protocol IPv4. Among the solution provided by IPv6 are solving the depleted IPv4 addresses and providing strong security mechanism in the network. Despite the hype and promises, there is still some issues need to be resolved before an organization can migrate over to IPv6 and still allowing the IPv4 infrastructure to exist. One of the issues to be considered are the transition mechanism to be use in switching over to IPv6 as there are several transitions mechanisms to be choose by an organization to allow the coexistence of IPv6 and IPv4 in the same network infrastructure. Therefore this paper describes the setting up of IPv6 test bed (Test6-T) in an intranet environment using the tunneling mechanism in order to find the best solution for providing an IPv6 environment in an existing IPv4 network infrastructure.

KEYWORDS: IPv6, TEST6-T, Transition Mechanism, Tunelling

1.0 INTRODUCTION

The current Internet Protocol (IP) which is known as IPv4 has been used for almost 30 years, published in 1981, the RFC 791 document, explained the Internet Protocol has not been substantially changed. With its robustness, easy to implement and interoperable, IPv4 has given a significance contribution to the rapid growth of the today's Internet usage. Yet, the initial design of IPv4 does not expecting the growth of the network to be rapidly increasing and causing the number of IPv4 addresses depleting day by day (www.potaroo.net) is expecting the IPv4 addresses scheme will be totally exhausted at the end of 2011.

Due to this reason, a Request For Comments (RFC) 1752 (Parkhurst, B., 2005), has issued "The Recommendation for the IP Next Generation Protocol" in 1994, to developed a suite of protocol and standard to cater the exhaustion of address and the security issue of IPv4. Which then The Internet Engineering Task Force (IETF) introduced the new version of IP, known as the IP- The Next Generation (IPng) and later known as IPv6. Other than providing larger address space, IPv6 also provide the fundamental features needed on network infrastructure, these include the issues on security, mobility, extensibility and dynamic re-configurability. With it capability and promises, it is now seen as the preferred solution for the evolving Internet.

Since IPv4 has dominating the network infrastructure for some time, migrating from IPv4 to IPv6 is not a simple task; there are some issues to be resolved before the whole network infrastructure can support IPv6. During this phase the two networks will coexist in the same network infrastructure, hence there is a need to have a transition mechanism that let this two network to be operating in the same infrastructure. Currently there are several transition mechanisms that can be used to addresses specific transition and interoperability of IPv6 with IPv4. Among of the transition mechanisms are dual stack, translation and tunneling. This paper evaluates and deployed one of the transitions mechanisms, namely tunneling mechanism as the first step in finding the preeminent transition mechanism for an existing IPv4 intranet network to support IPv6 network.

The rest of the paper is structured as follows. Section 2 discuses the background of transition mechanism, Section 3 presents the methodologies and the technique use in creating the fast attack module. Section 4 elaborates on the result validation. Finally, section 5 conclude and discuss the future directions of this work.

2.0 LITERATURE REVIEW

2.1 IPv4 and IPv6 Infrastructure

IPv4 network has been contributing a lot in ensuring information and resources being shared among the Internet user across the continent and has been an important integral part of the Internet revolution. Even

though it has been develop with careful plan and consideration, still at one point it has becoming to a stagnant level and walking towards declination phase. Among the major drawback of IPv4 is its IP addressing scheme that has it limitation. Expected to be obsolete in these few years, IPv4 addressing scheme uses 32 bits address number to identified host and differentiated the type of host via 5 types of classes. The class's concept wasted the address number availability, yet there are some works that tries to solve the IP shortages still it is not enough to fulfill the demand of the ever increasing Internet users who wanted to be always connected to the Internet anywhere and at anytime. As the number of hosts connected to the Internet are increasing, techniques such as Subnetting, Classless Inter-Domain Routing (CIDR), Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT) just slowing down IPv4 address exhaustion process but not solving the problem at hand which is the exhaustion of IP address. The need of IPv6 cannot be denied especially in providing huge number of addresses; 128 bits address scheme can provide enough unique address for every molecule on the surface of the earth address (Tanenhaum, A.S., 1996).

The packet layout in IPv4 and IPv6 is also difference; IPv4 has minimum 20 bytes header and maximum 60 bytes while IPv6 has only 40 bytes with optional extension header. The extension header provides IPv6 with flexibility and expandability in adding up a new option for the future whereas in IPv4 this is impossible. Ioan and Sherali (www.ietf.org.) stated that the performance overhead in processing these two headers is minimal.

IPv6 ease the user in connecting to the network, only a small configuration need to be done on the host site. This is provided by the auto configuration properties of IPv6, although the host in IPv4 can provide the same properties, it still needs a DHCP server to dedicate the IP address to the host while in IPv6 the addressing is done via its router discovery and solicitation. This creates "plug and play" scenarios which simplify the user to use the network. The administration task is also minimize as the reconfiguration of IP addressing within the network can be done in the routing devices only and the rest of the host connected to the router will be updated automatically with the new address scheme.

Another issue addresses by IPv6 is the security of the information travel through the network. IPv4 depends on the security application provided by the upper layer, if the upper layer is not providing any security measure to conceal the information, subsequently the information is transfer nakedly over the network and any man in the middle attack will result in exposure of information. Despite the IPSec availability in IPv4, it still needs to be enabled on both the client and server before the connections between them are secure. IPSec (Raicu, I. and Zeadally, S., 2003), provide data encapsulation on network layer, its provide access control, connectionless integrity, data origin authentication, protection against replays and confidentiality. In IPv6, IPSec is mandatory, consequently providing security for the information from the upper layer automatically.

2.2 Transition Mechanism

IPv4 network has supported the network and Internet for quite sometimes making the sudden migration to IPv6 is costly and impossible as lot of the resources and devices are currently running on IPv4. A careful and detail planning need to be done for the transition phase so that IPv4 and IPv6 network can exist in the same infrastructure without disturbing the availability of the services. In general there are three transition mechanisms that can be choose in establishing IPv6 and at the same still maintaining IPv4 network infrastructure. The three mechanisms are Dual Stack, Network Address Translation/Protocol Translation (NAT-PT) and Tunneling mechanism.

2.2.1 Dual stack

In this transition mechanism, the network permits the host to communicate using either IPv6 or IPv4 packet as long as the destination is also configured with the same type of IP. This provides easiness and flexibility in the network; once the IPv6 is fully deployed the IPv4 can be removed. The only drawback is that all the network resources and devices must be fully supported IPv6 and IPv4. An organization has to bear some cost in upgrading all the old machines and network resources so that it can supported IPv6, these includes the hosts, routers, switches and firewall. The whole backbone infrastructure needs to be upgraded.

2.2.1 Dual stack

In this transition mechanism, the network permits the host to communicate using either IPv6 or IPv4 packet as long as the destination is also configured with the same type of IP. This provides easiness and flexibility in the network; once the IPv6 is fully deployed the IPv4 can be removed. The only drawback is that all the network resources and devices must be fully supported IPv6 and IPv4. An organization has to bear some cost in upgrading all the old machines and network resources so that it can supported IPv6, these includes the hosts, routers, switches and firewall. The whole backbone infrastructure needs to be upgraded.

2.2.2 NAT-PT

NAT-PT provide transition mechanism through a translation table that match the IPv6 address with it IPv4 counterpart. The NAT router or server to be in the same network to provide the translation, if it is failed then the whole packet send through the network stumble. Even though this is the simplest transition mechanism and the cost is minimal, it is not suitable for future advancement of IPv6 establishment since it is not supporting the future expansion of IPv6 features. NAT-PT is only suitable for temporary solution until one of the other techniques can be implemented.

2.2.3 Tunneling

Marcus, G., and Kitty, N., (Marcus, G., 1998), state that tunneling can happen between two IPv6/IPv4 routers or between IPv6/IPv4 host and IPv6/IPv4 router. This transition mechanism also considered as configured tunnel in which the IPv6 packet send by the host is encapsulate inside an IPv4 packet by the router before it send through the network cloud and when it reached the router at the other end, the packet will be decapsulated from the IPv4 packet and the remaining IPv6 packet is process normally via IPv6 topologies. Tunneling permits isolated IPv6 nodes or networks to communicate without changing the underlying IPv4 infrastructure and thereby provides a transitional method of implementing IPv6 while retaining IPv4 connectivity. According to Weith, W.R., and James, F.K., (Weith, W.R., and James, F.K., 2001), the tunneling concept can be illustrated as below:

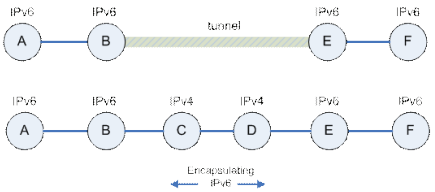


Figure 1: Tunneling Concept

For the purpose of this paper the researcher has choose the Tunneling mechanism as its translation mechanism. The main reason for this consideration is that the existing network in our facility is not fully ready with IPv6 since the overall backbone is only supporting IPv4. Moreover, the test bed developed should be able to support the future expansion of IPv6. Hence the only transition mechanism that can support both of the reason above is only tunneling.

3.0 IMPLEMENTATION AND TESTING

3.1 Implementation

The deployment of intranet IPv6 testbed (Test6-T) in an intranet environment using the tunneling mechanism takes several steps. One of them is designing an infrastructure which is IPv6 compatible. The Test6-T was setup with sequences techniques in basic networking approach. The deployment of Test6-T started with the logical and physical design as well as the IP addresses distribution as depicted in Fig. 2 and Table I. Fig. 2 illustrated the physical design of Test6-T network, from the figure it is shown than in the test bed we have two native IPv6 network, namely Site A and Site B, the two sites is connected through our existing IPv4 intranet Infrastructure. Each site has a switch and a router that is IPv6 and IPv4 compatible, this router will be configured with tunneling configuration. Site A consist of a network printer and a host whereas site B consist of a host and a server containing a DNS and web server, the entire node is IPv6 enabled. The two hosts are installed with windows vista as it operating system and the server operating system is installed with windows server 2008 with the DNS and IIS web server is enable. Both the DNS and web server is merely for testing the network.

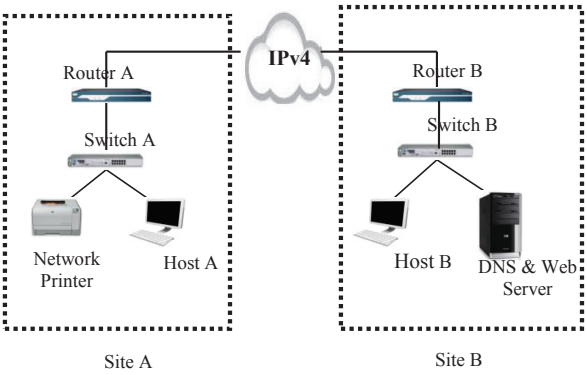


Figure 2: Test6-T Physical design

Table 1. shows the IP distribution for the entire network.

Node	IPv6 Address	IPv4 Address
Router A - Serial 0/2/0		192.168.1.13/30
Router A - Fa 0/0	2001:DB8:C19:1::5/64	192.168.3.1/24
Router A - Tunnel 0	2002:C0A8:2101::1/128	
Router B Fa 0/0	2001:DB8:C18:1::3/64	192.168.2.1/24
Router B Serial 0/1/1		192.168.1.22/30
Router B Tunnel 0	2002:C0A8:6301::1/128	
Client A	2001:DB8:C19:1::6/64	
Client B	2001:DB8:C18:1::6/64	
Network Printer	2001:DB8:C19:1::7/64	
Web and DNS server	2001:DB8:C18:1::4/64	

Router A and Router B is configured with tunneling configuration,

Figure 3. shows the configuration done on both router.

RouterA> enable RouterA#configure terminal RouterA(config)#ipv6 unicast-routing RouterA(config)#interface FastEthernet0/0 RouterA(config-if)#ip address 192.168.2.1 255.255.255.0 RouterA(config-if)#ipv6 address 2001:DB8:C18:1::3/64	RouterB> enable RouterB#configure terminal RouterB (config)#ipv6 unicast-routing RouterB (config)#interface FastEthernet0/0 RouterB (config-if)#ip address 192.168.3.1 255.255.255.0 RouterB (config-if)#ipv6 address 2001:DB8:C19:1::5/64
RouterA(config-if)#ipv6 enable RouterA(config-if)#no shutdown RouterA(config-if)#exit	RouterB (config-if)#ipv6 enable RouterB (config-if)#no shutdown RouterB (config-if)#exit

```
RouterA(config)#interface Serial 0/2/0
RouterA(config-if)#ip address
192.168.1.22 255.255.255.252
RouterA(config-if)#ipv6 enable
RouterA(config-if)#no shutdown
RouterA(config-if)#exit

RouterA(config)#router rip
RouterA(config-router)#version 2
RouterA(config-router)#network
192.168.1.0
RouterA(config-router)#network
192.168.2.0
```

(a) Router A configuration

```
RouterB (config)#interface Serial 0/1/1
RouterB (config-if)#ip address
192.168.1.13 255.255.255.252
RouterB (config-if)#clockrate 64000
RouterB (config-if)#no shutdown
RouterB (config-if)#exit

RouterB (config)#router rip
RouterB (config-router)#version 2
RouterB (config-router)#network
192.168.1.0
RouterB(config-router)#network
192.168.3.0
```

(b) Router B configuration

Figure 3: Router Configuration

The following configuration is used for enabling the IPv6 and the tunneling mechanism in the Router A and Router B.

```
Router(config)#interface Tunnel0
Router(config-if)#ipv6 address
2002:C0A8:6301::1/128
Router(config-if)#ipv6 enable
Router(config-if)#tunnel source
Serial 0/2/0
Router(config-if)#tunnel destination
192.168.1.13
Router(config-if)#tunnel mode
ipv6ip
Router(config-if)#exit

Router(config)#ipv6 route
2001:DB8:C19:1::/64 Tunnel0
Router(config)#ipv6 route ::/0
Tunnel0
```

(a) Router A configuration

```
Router(config)#interface Tunnel0
Router(config-if)#ipv6 address
2002:C0A8:2101::1/128
Router(config-if)#ipv6 enable
Router(config-if)#tunnel source Serial
0/1/1
Router(config-if)#tunnel destination
192.168.1.22
Router(config-if)#tunnel mode ipv6ip
Router(config-if)#exit

Router(config)#ipv6 route
2001:DB8:C18:1::/64 Tunnel0
Router(config)#ipv6 route ::/0 Tunnell
```

(b) Router B configuration

Figure 4: IPv6 Configuration in the router

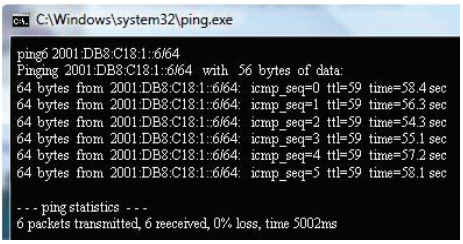
In order to make the DNS server works in the IPv6 environment Forward Lookup Zones file has to be added with the windows server 2008 IP address which is *2001:DB8:C18:1::4*.

3.2 Testing

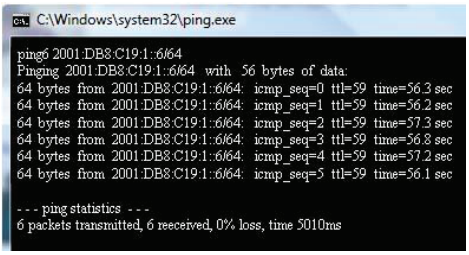
These network connectivity testing ping was done with difference network connection and the result obtained are as follow. For the

3.3 Ping

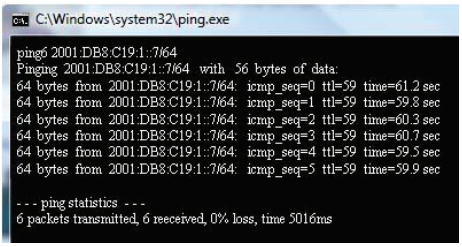
All connectivity testing using *ping* command is successful and the results are depicted in fig 5.



(a) Host A **PING** Host B



(b) Host B **PING** Host A



(c) Host A **PING** Network Printer

Figure 5: Ping testing on Test6-T

3.4 Web server testing

The implementation of DNS server and Web server can be shown by using a web browser in host A. The IPv6 address and the URL address of the web server is type into the address bar. Figure 6 illustrated the successful result for this testing .

(a) Accesing web server using IP address

(b) Accesing web server using URL address

Figure 6: Web Server Testing

4.0 CONCLUSION

In this paper, we presented the preliminary work in establishing IPv6 Network using Tunnelling Mechanism on Intranet Environment that is supported fully by IPv4 backbone infrastructure. From the implementation shown in the previous section, it becomes clear that IPv6 networking with tunnelling mechanism can be successfully implemented in intranet environment. It has been proven from the implementation that each IPv6 host can ping the other host even though it is separated by an IPv4 infrastructure. The web server application testing also shown that the client in site A can successfully connected with the web server in site B. These proved that we can implement IPv6 network in an existing IPv4 infrastructure without having to disturb the running services and application and both the network can be coexist at the same time. In conclusion, base on our implementation, it shown that there is no difficulty in implementing an IPv6 network in an intranet environment. This could be the preliminary step towards the migrating from IPv4 to IPv6.

5.0 REFERENCES

Parkhurst, B., 2005. Routing first-step, Cisco Press.

Tanenhaum, A.S., 1996. Computer Networks, Third Edition, Prentice Hall Inc., pp. 686, 413-436,437-449

Raicu, I. and Zeadally, S., 2003. Evaluating IPv4 to IPv6 transition mechanisms, 10th International Conference on Telecommunication, ICT 2003 volume 2.

Marcus, G., 1998. IPv6 Networks. New York: McGraw Hill

Weith W.R., and James F.K., 2001. Computer Networking: a top-down approach featuring the Internet. United States of America: Addison Wesley Longman

loan, and Sherali, http://www.ietf.org/rfc/rfc2401.txt
http://www.potaroo.net/tools/ipv4/index.html