COST-BENEFIT ANALYSIS OF ORGANISATIONAL MIGRATION TO IPV6

By

YEE HONG WENG

A thesis submitted to the Department of Internet Engineering & Computer Science,

Faculty of Engineering and Science,

Universiti Tunku Abdual Rahman,

in partial fulfilment of requirement for the degree of Master of Information Systems in May 2012

ABSTRACT

COST-BENEFIT ANALYSIS OF ORGANISATIONAL MIGRATION TO IPV6

Yee Hong Weng

As the Internet rapidly becomes the preferred way to communicate in this information age, the cyberspace is being crowed. Millions of computers and networks effortlessly exchange vast amount of information using the Internet Protocol Version 4 (IPv4). However, IPv4 exhibits a shortage of IP addresses and it is starting to reach its limit. Therefore, the next generation Internet Protocol, IPv6 is needed to support new applications and new users. At the moment, the adoption of IPv6 is not being widely implemented due to lack of business case and the unclear cost of migration. Hence, this research is carried out to examine the cost of IPv6 migration, hidden and unexpected costs during migration and the benefits of IPv6 migration. In this research, in-depth interviewing would be used as primary data collection from participants. The interview data was analysed using Glaser and Strauss' method of grounded theory. The basic procedure used was open coding which involved reading and re-reading interview scripts for identification and labelling. The labelling was then combined into a single theme and to create a model to perform data analyse. The result showed that an IPv6 deployment cost consists of four main components such as hardware cost, software cost, labour cost, and other unexpected cost. Each main component is divided into several sub-components. A general recommendation for organisational migration to IPv6 is suggested based on the findings at the end of the report. A customise recommendation for organisation was planned in future studies.

ACKNOWLEDGEMENTS

I could not have come to the completion of this research project without close interactions and advice from numerous individuals to whole I owe a debt of gratitude.

I would like to express my deep appreciation to my supervisor Mr. Ooi Ean Huat who has dedicated his valuable time and assistance throughout this paper. Without his guidance, critical comments and assistance, this project paper would never have been completed.

Lastly, I would like to thank all the lecturers who have taught and imparted invaluable knowledge to me throughout the whole MIS program.

FACULTY OF ENGINEERING AND SCIENCE

UNIVERSITI TUNKU ABDUL RAHMAN

Date: May 3, 2012

SUBMISSION OF THESIS

It is hereby certified that **Yee Hong Weng** (ID No: **09UEM09066**) has completed this thesis entitled "Cost-benefit of Organisational Migration to IPv6" under the supervision of Mr. Ooi Ean Huat (Supervisor) from the Department of Internet Engineering and Computer Science, Faculty of Engineering and Science.

I understand that University will upload softcopy of my thesis in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

Yours truly,

_____

Yee Hong Weng

DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citations, which has been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UTAR or other institutions.

Name Yee Hong Weng

Date 3rd MAY 2012

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AfriNIC	African Network Information Centre
APAC	Asia Pacific
APNIC	Asia Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
BIS	Bump-in-the-stack
BIA	Bump-in-the-API
DNS	Domain Name Server
DOS	Denial-of-Service
FQDN	Fully Qualified Domain Name
GTM	Grounded Theory Method
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Intrusion Prevention System
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPSec	Internet Protocol Security
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol

ISOC	Internet Society
ISP	Internet Service Provider
LACNIC	Latin America and Caribbean Network Information Centre
MCMC	Malaysian Communications and Multimedia Commission
MTU	Maximum-transmission-unit
NAT	Network Address Translation
NPO	Non-profit Organisation
RFC	Request for Comments
RIPE NIC	Reseaux IP Europeans Network Coordination Centre
RIR	Regional Internet Registry
ROI	Return On Investment
SIIT	Stateless IP/ICMP Translation
SME	Small and Medium Enterprise
SMTP	Simple Mail Transfer Protocol
VoIP	Voice over Internet Protocol

CHAPTER 1

INTRODUCTION

As the Internet rapidly becomes the way to communicate, cyberspace is getting crowded. Millions of computers and networks effortlessly exchange vast amount of information using the Internet Protocol (IP). Yet, IPv4 has a shortcoming, and it is starting to reach its limitations. Each networked device needs to have a unique address to distinguish it from every other device on the Internet. Due to rapid growth of Internet IPv4 address space held by Internet Registries will run out in the year 2012 (Huston, 2012).

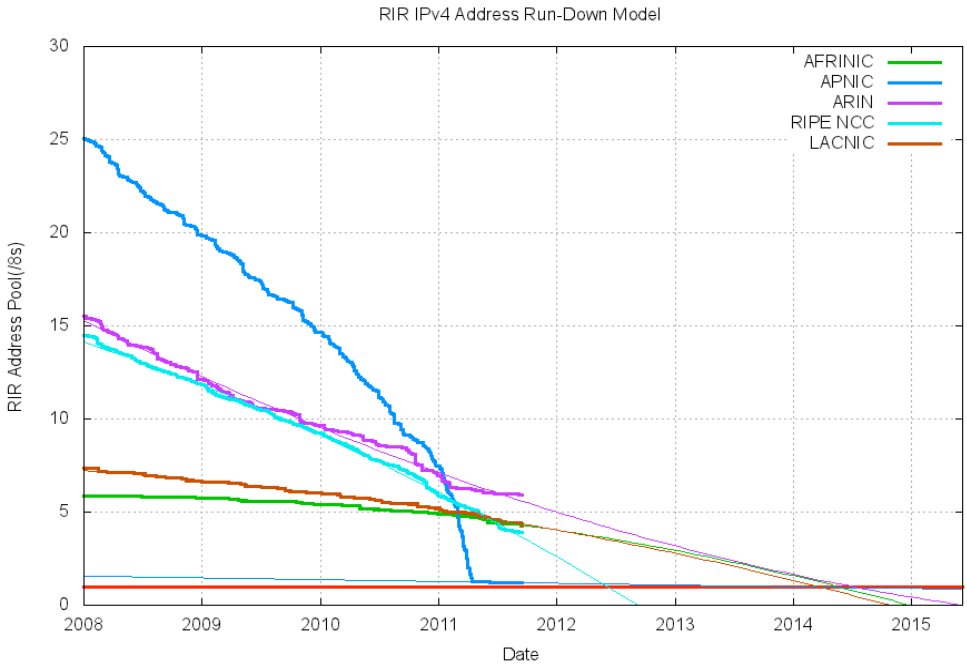


Figure 1.1: Projected RIR and IANA Consumption (/8s) (Huston, 2012)

The actual date of Internet Assigned Numbers Authority (IANA) unallocated IPv4 address pool was exhausted on February 3, 2011 (Huston, 2012). The last 5 blocks of unallocated IPv4 addresses was allocated to each RIR such as APNIC, RIPE NCC, ARIN, LACNIC, and AfiNIC (Appendix I). The prediction of unallocated IPv4 addresses will be exhausted in each RIR is difficult, but based on BGP Report (2012), the remaining of unallocated IPv4 addresses in APNIC region will be exhausted within year 2012.

This will affect a major part of the current Internet using of IPv4 addressing, and it is impossible to directly connect to the Internet without IPv4 addresses. This issue will arise when IPv4 addresses space runs out and new IPv4 addresses will no longer be available to service providers and users can be straightforwardly expresses as new hosts cannot directly connect to the Internet (JPNIC, 2007). However, end user will not have much affect on that, as ISPs have reserve enough IPv4 addresses for their customers in extend the lifetime in short period of time.

Who	Issue
Connection providers who want to accommodate new users	Cannot meet customers' demand = Cannot expand business
Server providers who want to install new servers	Cannot provide new services, enhance, or expand services
New entrant service provider	Cannot join the Internet

Figure 1.2: Who Will be Directly Affected by IPv4 Address Space Exhaustion and How? (JPNIC, 2007)

Therefore, the next generation Internet Protocol is needed, which is IPv6. IPv6 stands for Internet Protocol version 6 is the next generation protocol for the Internet, which was defined in December 1998 by the Internet Engineering Task Force (IETF) with the publication of an Internet standard specification, RFC 2460 (Deering & Hinde, 1998). It was developed to meet the rising global demand for IP addresses and will replace Internet Protocol version 4 (IPv4), which is today's dominant IP.

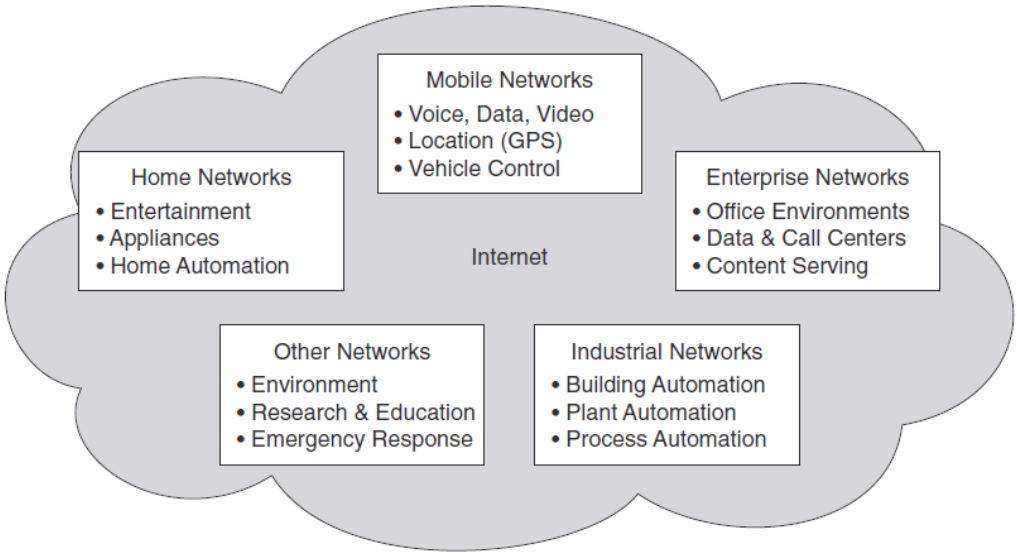


Figure 1.3: Internet Today

Some of the reasons that cause insufficient of IPv4 addresses space due to the widespread growth of networks and communication devices in the Asia Pacific (APAC) region, there is an increased demand for IP addresses. For example, China and India will need many IP addresses to become presence on the Internet. This rapid growth is creating unique challenges for the APAC

region due to the very limited number of IP addresses assigned to them during the early days of address allocations (Juniper Networks & Microsoft Corporation, 2007). Besides this, developed countries such as U.S., Korea, and Japan need additional IP addresses for mobile phones and other mobile devices to stay connected.

In March 2009, the Internet Society (ISOC) had studied the operational characteristics of IPv6 in its organisation member's networks. This was done through a questionnaire sent to the organisation members. According to the study, some of the respondent states that they would make more extensive use of network address translation (NAT) technology when there are not possible to get more IPv4 addresses in a future request. However, this will only provide temporary workarounds and increase costs of infrastructure by installing multiple layers of NAT on the routers. Besides this, almost half of the respondents stated that demand from customers was the main driver for their deployment of IPv6 and a need to be prepared for the next large technology step in the evolution of the Internet (Roberts, 2009).

According to the ISOC study, there are some respondent from the organisations state that implementing IPv6 was less complicated than they had anticipated. Still, they emphasised that operating IPv6 in a network or part of a network is a new experience for the individuals involved and that training and that training is perhaps the most important need because there are new aspects to operating an IPv6 network (Roberts, 2009).

However, according to IETF, IPv6 is not backward compatible with IPv4, which means an IPv6 host cannot directly communicated with an IPv4

host. The IETF worked on ways to achieve this through intermediaries, such as a protocol to translate NATs. However, this approach has been declared as "historic" because of technical and operational difficulties (Aoun & Davies, 2007).

Therefore, if a host wants to talk to the IPv4 world, it needs to have a local IPv4 protocol stack, a local IPv4 address, a local IPv4 network and IPv4 transit. If an IPv4 host wants to talk to IPv6 host, IPv6 has the same set of prerequisites as IPv4. This approach to transition through replication of the entire network protocol infrastructure is termed Dual Stack. Therefore, organisations need to buy a set of prerequisites network infrastructure for IPv6 to communicate with IPv4.

1.1 IPv6 Technology Features

IPv6 protocol features include larger number of addresses, end-to-end connectivity, IPSec security, efficient routing, auto-configuration, and mobility support in IPv6. The following sub sections discuss the features of the IPv6 protocol.

1.1.1 Larger Number of Addresses

IPv6 has 128-bit addresses compared to 32 bits for IPv4 addresses. This results in a very large increase in the number of IP addresses available, and this creates a number of advantages (Deering & Hinde, 2003). It eliminates scenarios where there is an IP address scarcity and NAT must be deployed to fix the issue. Getting rid of NAT, this results in a simplified network configuration and reduced hardware and software complexity. In addition, increasing deployment of wireless and mobile devices will not be cramped by IP address scarcity issues.

1.1.2 End-to-end Connectivity

IPv4 needed NAT in certain situations to conserve scarce IP addresses. Unfortunately, NAT does not work well with peer-to-peer applications such as VoIP (Cisco, 2006). IPv6 eliminates the need for NAT and thus, restores end-to-end connectivity. As a result, peer-to-peer applications work well with IPv6.

1.1.3 Security

IPSec is a part of IPv6 standards, thus providing a solid security framework for Internet communication. IPSec can be used to implement both encryption and authentication (Kent & Atkinson, 1998).

1.1.4 Efficient Routing

IPv6 has a more streamlined header compared to IPv4. Intermediate routing nodes do not re-compute network-layer checksum, fragment or reassemble packets, or parse through headers (Deering & Hinde, 1998). This reduces the processing overhead for routers, which reduces hardware complexity and enables faster packet processing. In addition, hierarchical addressing in IPv6 allows for proper address space allocation, which results in smaller routing tables and more efficient routing in the overall network. In addition, IPv6 makes it easier for network administrators to assign and track addresses.

1.1.5 Auto-configuration

IPv6 provides auto-configuration of IP addresses on IPv6-enabled devices. This greatly improves scalability and manageability of networks. New devices can be connected directly to the network without manually configuring IP addresses or having a DHCP server (Thomson & Narten, 2007).

1.1.6 Mobility Support in IPv6

IPv6 provides further enhancements for mobile IPv6, which helps with today's wireless networks. It allows nodes to remain reachable while moving around in the IPv6 Internet and each mobile node is always identified to the Internet (Johnson & Perkins, 2004).

1.2 Address Format Comparison Between IPv4 and IPv6

In this section will compare address format between IPv4 and IPv6, as IPv6 is not backward compatible with IPv4. Therefore, IPv6 needs a new address format. As mentioned in Section 1.1.1, IPv6 addresses are 128 bits long compared to IPv4 address, which is only 32 bits long. With 128 bits long, this gives IPv6 about 3.4 x 10^{38} of IP addresses while 32 bits IPv4 only gives 4.3 x10^{9} (4.3 billions) of IP addresses.

For IPv4 address format, it is represented in dot-decimal notation, which consists of 4 decimal numbers, each ranging from 0 to 255, separated by dots (Bakke et al, 2004). For example, 192.0.2.2. However, for IPv6 address format, it is represented by 8 groups of 16-bit hexadecimal value separated by colon (:) (Hinden et al, 2006). For example, 2001:DB8:0:0:8:800:200C:417A.

In addition, there are 3 conventional forms for representing IPv6 addresses as text strings. The preferred form is x:x:x:x:x:x:x:x, where the 'x's are the hexadecimal value of the eight 16-bit hexadecimal value. Another form of is the use of "::" indicates one or more groups of 16 bits of zeros. The "::"

can only appear once in an IPv6 address. For example, 0:0:0:0:0:0:0:1 can be represented as ::1. The last form of representing IPv6 address could be use as alternative form when dealing with a mixed environment of IPv4 and IPv6 node, which is x:x:x:x:x:d.d.d.d, where the ‘x’s are the hexadecimal value of the 16 bits address, and the ‘d’s are the decimal value of IPv4 address (Hinden et al, 2006). For example, 2001:DB8:0:0:8:800:115.1.68.3.

In the next section will discuss about the IPv6 adoption in worldwide and IPv6 adoption in Malaysia. In next section also will include a detail statistics for IPv6 adoption in Malaysia.

1.3 IPv6 Adoption in Worldwide

After discussed about features about IPv6 and shortage of IPv4 addresses, this section will discuss about the IPv6 adoption in worldwide and IPv6 adoption in Malaysia. The statistics figures are getting from IPv6Forum IPv6 enabled program (IPv6 Forum, 2012). All statistics figure are up-to-date. The objective of IPv6 Enabled Program is to accelerate the deployment of IPv6 at enterprise, ISP, and private users helping them to test and check their proper of IPv6 readiness and adoption. All figures are cited in Appendix A to Appendix D.

Based on Appendix C, there are total of 140 IPv6 enabled ISP are listed in the worldwide list, which mean 140 of them are already migrate their Internet backbone to IPv6 and each of them is already assigned a block of IPv6 addresses by their own Regional Internet Registry (RIR).

Beside this, based on Appendix D, there are total of 1482 IPv6 enabled websites are listed in the list, which mean their website is IPv6 enabled and Internet user around the world can access their website using IPv6 address.

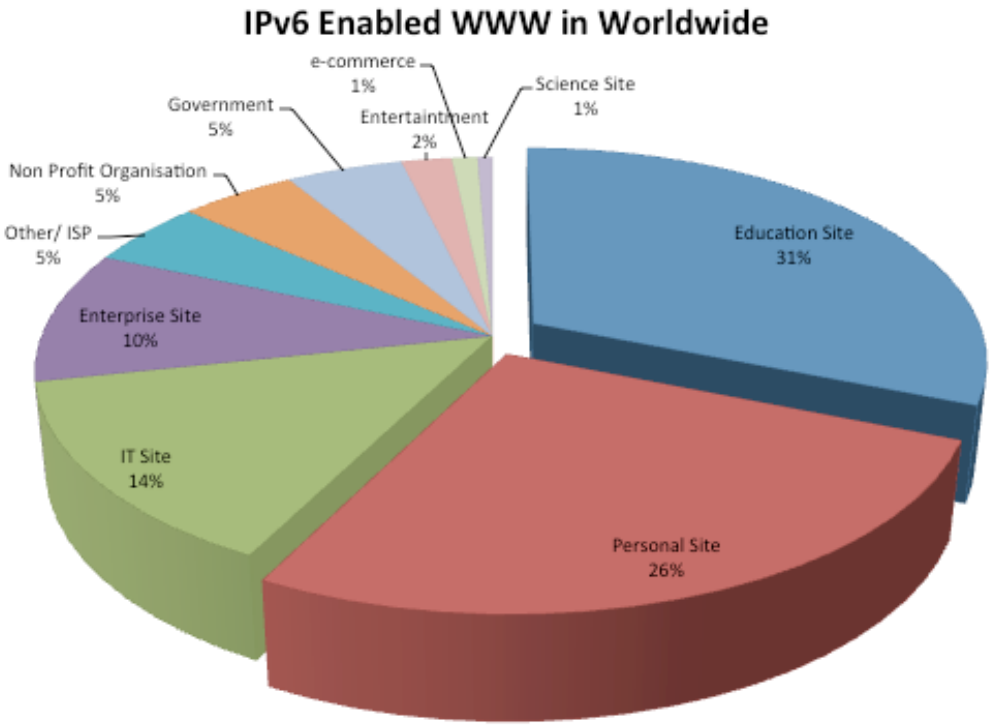


Figure 1.4: IPv6 Enabled WWW in Worldwide

Based on Figure 1.4 above, it shows that among 1482 IPv6 enabled websites, educational site has the highest percentage, which is 31% followed by personal site, IT site, enterprise site, ISP, and others. From the figure, we know that educational industry plays an important role in IPv6 migration and usually educational institution has more experts compared to other industry (KanREN, 2009). Personal site will not discussed, as it is not in the scope. For IT and enterprise sites, both having very close numbers in term of IPv6 enabled website. One of the reasons both IT and enterprise sites are not doing well in IPv6 migration compared to educational sites is because lack of expertise in this field and lack of vendor support.

In the next section, will discuss about IPv6 adoption specifically in Malaysia and a chart of IPv6 enabled websites will be provided.

13.1 IPv6 Adoption in Malaysia

Based on Appendix A, there are total of 13 IPv6 enabled ISPs are listed in the list and each of them is already assigned a block of IPv6 addresses by APNIC. Besides this, based on Appendix B, there are total of 32 IPv6 enabled WWW are listed in the list.

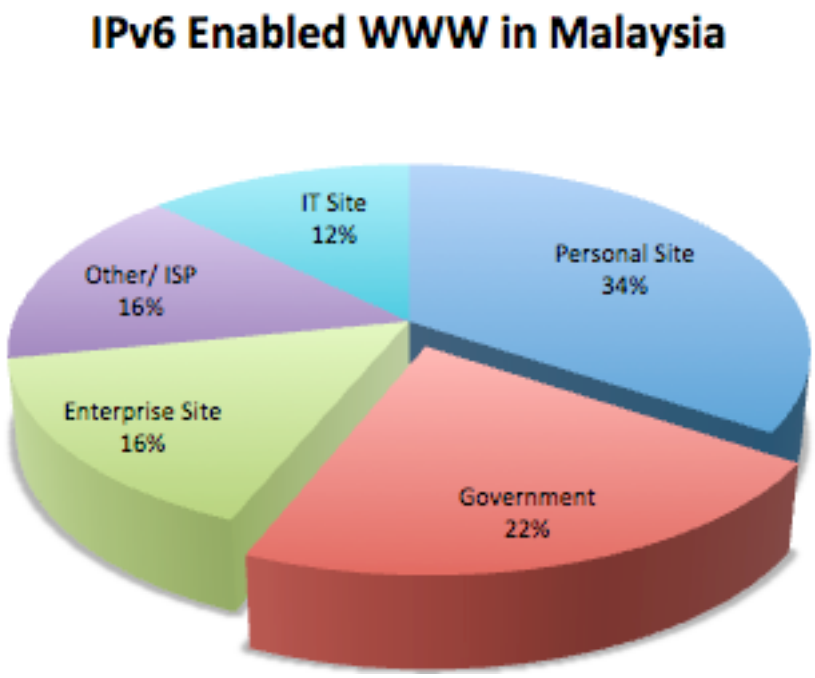


Figure 1.5: IPv6 Enabled WWW in Malaysia

Based on Figure 1.5 above, it shows that government site has the second highest percentage, which is 22% followed by enterprise site, ISP, and IT site. In 2008, Malaysia government agencies websites start IPv6 pilot projects and some of them are already successfully migrate to IPv6 based on Appendix B (Raj Kumar, 2010). In 2009 December, most of the ISP in Malaysia had IPv6 enabled and validated by Malaysian Communications and Multimedia Commission (MCMC) (Raj Kumar, 2010).

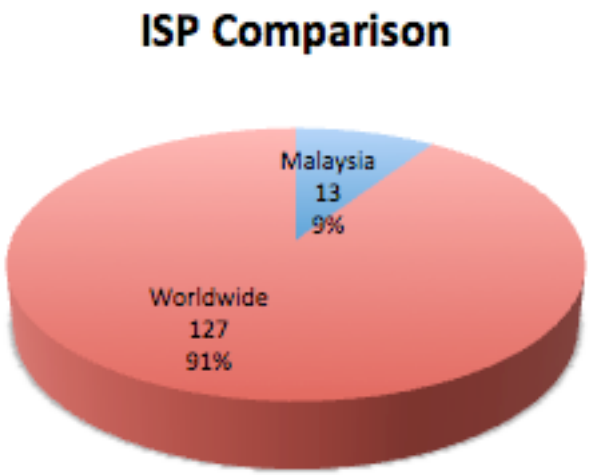


Figure 1.6: IPv6 Enabled ISP Comparison Between Malaysia and Worldwide

Based on Figure 1.6 above, it shows that Malaysia's ISPs own 9% with 13 ISPs enabled, which contribute quite a lot in worldwide.

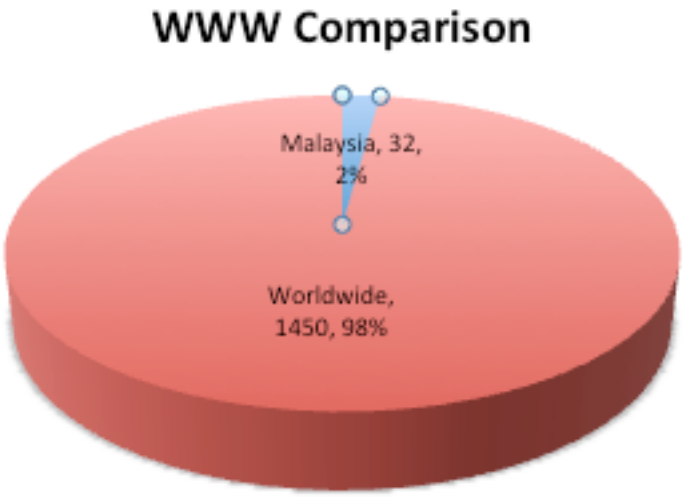


Figure 1.7: IPv6 Enabled WWW Comparison Between Malaysia and Worldwide

Based on Figure 1.7 above, it shows that Malaysia's IPv6 enabled websites only contribute small percentage, which is 2% compare to worldwide 98%.

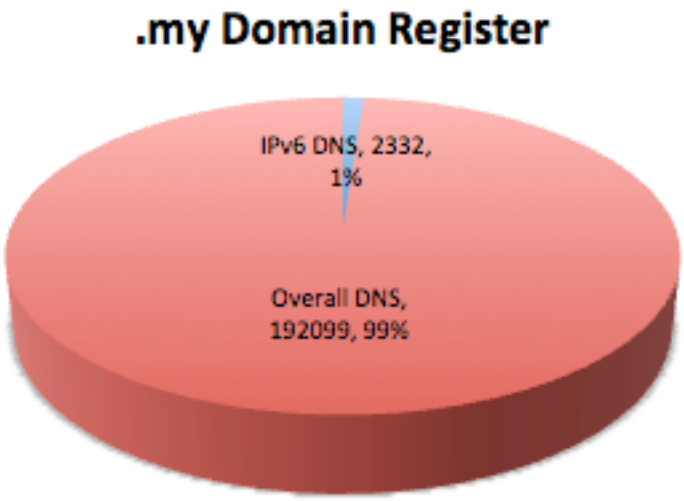


Figure 1.8: .my Domain Name Register

When look at total domain name register in .my, IPv6 domain name only contribute 1% and based on Appendix B there are only a small portion of website are IPv6 enabled. From the statistics from Appendix B and Figure 1.8 However, based on Appendix E, number of IPv6 domain name is increasing every month. Therefore, it seems that Malaysia doesn't have a big push to deploy IPv6.

1.4 Motivation

IPv6 will be the future of IP sooner or later due to the IPv4 the depleting addresses even though some organisations remain to use IPv4 by applying more layer of NAT internally. In the end, these workarounds carry high costs as NAT adds complexity and impedes flexibility.

For some years, leading manufactures such as Cisco, Foundry, Nortel, Huawei, Alexala, and Juniper have been adding the necessary software to their products (Cisco, 2010; Cisco, 2008). All the leading operating systems such as Microsoft Windows, Mac OS X, and Linux support IPv6. The long term solution for organisations is migrating current network from IPv4 to IPv6 and this migration is impossible to be done overnight due to the large internal and external networks and there are many planning and consultations need to be worked out (Cisco, 2008).

As we can see in near future, every organisation needs to deploy IPv6 in their network if the organisations want to see the Internet continue to operate and to support new applications and users. IPv4 and IPv6 will need to coexist for many years in most organisations for several reasons:

- Most companies adapt IPv6 on their infrastructure gradually rather than all at once.

- If an organisation completely turned off support for IPv4 in their network, then all IPv4 applications, websites, and service would no longer work. By continuing to support IPv4, the organisation can

gradually upgrade applications to IPv6 and test, which is less expensive than upgrading and testing all applications at once.

- It might not be possible to add IPv6 support to older applications for which a company does not own the source code.

- Upgrading or replacing old but stable operating systems, or platforms used for dedicated applications, might not provide ROI. In some cases, it makes better business sense to wait to replace those operating systems until their end of life.

Therefore, organisations need to start planning IPv6 migration strategy. In the process of planning, one of the crucial stages is stakeholders need to figure out all the cost-benefit of migrating to IPv6. For instance, they need to have a product refresh cycle plan to replace old network equipment to new network equipment such as routers, switches, servers, and other incompatible hardware and software to support IPv6.

Hence, there would be a strong motivation to push organisations to deploy IPv6. The author's motivation in this report is to examine and analysis the costs-benefits that will bring to organisations during IPv6 migration. Another author's motivation is to understand the reasons that organisations are not planning migration on IPv6 in their networks.

1.5 Problem Statement

As mentioned in previous section, IPv4 addresses are going to exhaust soon and it will affects every organisation that are providing services either internally or externally. Therefore, every organisation is needed to move on to the new IPv6, but the adoption of IPv6 isn't being done because lack of business case and the unclear cost of migration.

Cost is one of the biggest problems or challenges other than other factor like lack of IPv6 technical expertise and security issues. Without cost, organisations unable to sent staff for training and unable to replace incompatible network equipment.

Besides this, cost is one of the major concerns of IPv6 migration for most of the organisations as they are afraid the migration will overrun from their IT budget. In fact, there are some general costs are needed such as cost for deployment, human resource, upgrading, updating and buying new hardware and software, and long-term maintenance cost of the network. However, there might have some costs are hidden and unexpected during migration. For example, inevitable extra costs when applications do not work as expected. Therefore, one of the purposes of this study is to examine the hidden and unexpected costs during migration.

In addition, benefits of IPv6 migration are important for organisation too. As organisations need to figure out does the benefits are weighed against the invested costs. Otherwise, the decision that results may be less than optimal. For example, cost reduction benefit, cost avoidance benefit, and performance benefit. Another purpose of this study is to examine the benefits of IPv6

migration and how do these benefits increase organisations profits, performance, revenues and competitive advantages.

In short, one of the main issues of IPv6 migration is cost and organisations are afraid the migration will over budget. Besides this, benefits also an importance factor to allow organisations figure out the weight against the costs. Therefore, in this study the author will examine the cost of IPv6 migration, hidden and unexpected costs during migration, and the benefits of IPv6 migration.

1.6 Objectives

The objective of this report is to examine and analysis the costs-benefits on organisational migrate to IPv6. The objectives are divided into several parts:

- To examine the costs needed for organisations on IPv6 migration included upgrading, updating, staff training, and product refresh cycle
- To examine the benefits of IPv6 after migration
- To examine others hidden and unexpected costs during IPv6 migration
- Recommend a general cost effective way for organisations to perform IPv6 migration

1.7 Scope of Work

The scope of this report begins with literature review on several transition mechanisms on IPv6 to further understand on how to deploy IPv6, review on current IPv6 issues, and review on costs needed for organisations on IPv6 migration. The results of literature review improve author's understanding on IPv6 migration and assist author to create more quality interview questions, which will be used during interview session.

Once interview questions are well defined, the author starts to contact interviewees by email and conduct in-depth interview with them. After all required data are collected, the author starts to perform coding and analyse collected data into more meaningful information. Based on the result of the study, a general cost effective way of IPv6 migration will be created as a guideline for organisations to prepare IPv6 migration in future.

1.8 Study Limitations

Many different decisions have factored into the planning of this study. These decisions have influenced the study by, among other things, defining its scope, facilitating data collection, and contextualising the data analysis. However, these decisions have also had a limiting effect on the study's findings. The most significant limitation is limited number of potential study participants. This is because not many organisations are planning to IPv6 migration in the next 24 months. Therefore, these organisations are not qualified as study participants for this study, as they don't have any plan to IPv6 migration yet. Even though qualitative research is aimed for small size study participants, but getting extra studies participants enable researcher to select the most suitable ones to generate study's findings.

CHAPTER 2

LITERATURE REVIEW

In this section, transition mechanisms to deploy IPv6 will be discussed to further understand the transition mechanism for deploying IPv6 and several issues regarding to the deployment. First section will presents transition mechanisms for IPv6 such as dual stack, tunnelling, and translation. Second section will presents issues and impacts of deploying IPv6. The last section will present economical impacts on IPv6 migration.

2.1 Transition Mechanisms

Transition mechanisms generally come in three forms such as dual stack, tunnelling, and translation (Nordmark, 2005). These mechanisms are listed in the order of complexity, with dual stacking being the simplest and translators being the most complex. A sensible approach is to look at the simplest mechanisms first and move to progressively more complex solutions only when the simpler ones do not meet the deployment requirements. The following sub sections will present dual stack, tunnelling, and translation mechanisms in details.

2.1.1 Dual Stack

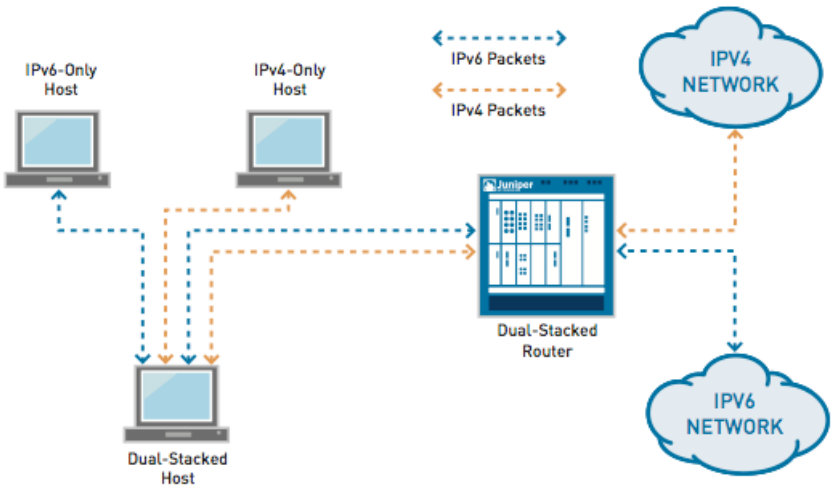


Figure 2.1: A Dual Stacked Device Can Send and Receive Both IPv4 and IPv6 Packets (Juniper Networks, 2009).

The Dual Stack approach is considered the most straightforward approach to transition. It is refer to that a single node support two protocol stacks such as IPv4 and IPv6 stack that operate in parallel and allow the device to operate through either protocol (Waddington & Chang, 2002). Dual stacks can be implemented in both end systems and network devices and it is best suited for core-to-edge implementation strategies. It also can be used internally in IPv6 "islands" (Juniper Networks, 2009). Both IPv4 and IPv6 are network layer protocols with similar functions, both are based on same physical platform and the transport layer protocols loaded on IPv6 and IPv4 respectively. If a host supports both IPv6 and IPv4, the host can communicate with both IPv6 and IPv4 protocol.

During dual stack node receiving and sending data packets, when the link layer receives data segments, it will takes apart and examines packet heads. If the version number of IP packet is “4”, then this data packet is handled by IPv4 stack and if the number is “6” then the data packet will handled by IPv6 stack (Xiong Wei, et al., 2009).

Due to a dual stack host supports both IPv4 and IPv6 protocol, then it is important to determine to use one of the protocol stacks to further communicate in the network. During the communication in the network, destination address is the main parameter of routing selection.

Therefore, there are several scenarios to determine either IPv4 or IPv6 protocol will be chosen to communicate (Xiong Wei, et al., 2009):

- If the destination address is IPv4 address then use IPv4 protocol
- If the destination address is an IPv6 address and it is a local online network then use IPv6 protocol
- If the destination address is an IPv6 address compatible with IPv4 and it is not a local online network, then use IPv4 protocol and at this time, IPv6 will be encapsulated in IPv4.
- If the destination address is an IPv6 address incompatible with IPv4 and it is not a local online network, then use IPv6 protocol
- If the application uses a domain name as destination address, get the corresponding IPv4/IPv6 address from domain name server (DNS) first and then carry out corresponding treatment according to address situation

2.1.2 Tunnelling

Tunnelling, from the perspective of transitioning, it enables incompatible networks to be bridged and it is deployed in a point-to-point manner (Waddington & Chang, 2002). Data is carried through that tunnel using a process called encapsulation, in which the IPv6 packet is carried inside an IPv4 packet, which makes IPv4 appear as a Data Link Layer with respect to IPv6 packet transport. The encapsulating IPv4 header is created at the entry point of the tunnel, and then removed at the exit point of the tunnel. The tunnel endpoint addresses are determined by from configuration information that is stored at the encapsulating endpoint. These tunnels can be defined to go between router-to-router, host-to-router, host-to-host and router-to-host. These technologies are generally categorised as configured or automatic. Configured tunnels are predefined, whereas automatic tunnels are created and torn down "on the fly." The following sub sections discuss several types of manually configured tunnels and automatic configured tunnels in details.

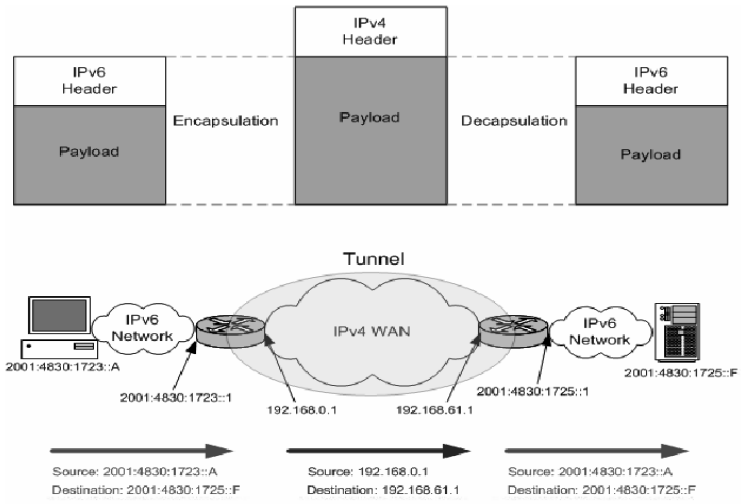


Figure 2.2: IPv6 Tunnelling Diagram Depicts Transport of IPv6 Data Across IPv4 Infrastructure (Robinson, Cesar Ramos, & Jara, 2007)

2.1.2.1 Manually Configured Tunnelling

For manually configured tunnelling, the tunnelling parameters are managed either through manual data entry or through tunnel brokers on the tunnel interface at the tunnel source and at the tunnel destination (Waddington & Chang, 2002). A manual tunnel is set up by statically configuring information at the devices (usually routers) at each end of the tunnel.

Manual tunnels are ideal for interconnecting IPv6 sites over an IPv4 network where the sites do not change. However, as the number of sites grows, the challenge of interconnecting them with a full mesh of tunnels can become an administrative problem. As the number of sites to be interconnected grows, the number of tunnels required to provide direct connections between all sites grows exponentially. Therefore manual tunnels are best used when there are a manageable number of sites to be interconnected, when inter-site communication requires only a partial mesh, or when an alternative topology such as hub-and-spoke can be used (Juniper Networks, 2009). It's usually in router-to-router and host-to-router tunnelling method and IPV6 packets are tunnelled to a router (Govil, et al., 2008).

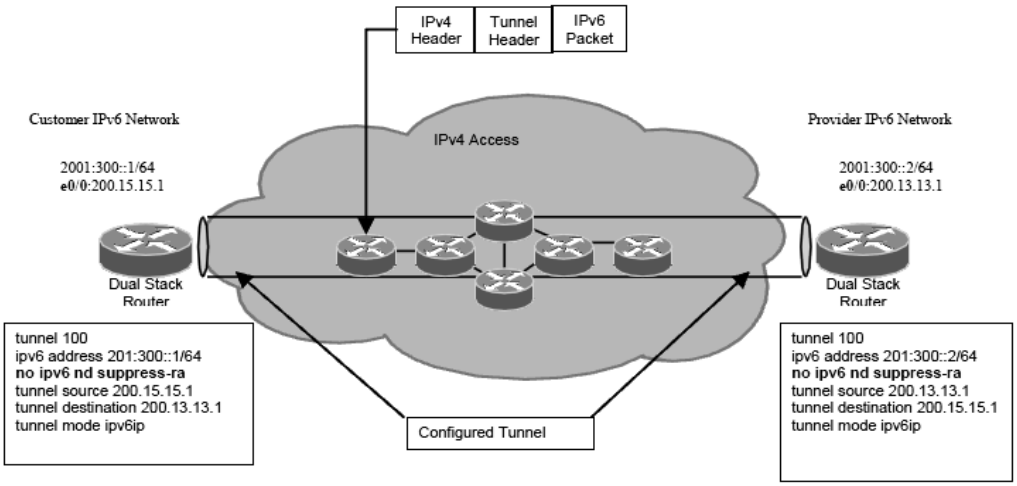


Figure 2.3: Manually Configured Tunnelling (Department of Veterans Affairs, 2006)

2.1.2.2 Generic Routing Encapsulation (GRE) Tunnel

IPv6 traffic can be carried over IPv4 GRE tunnels using the standard tunnelling technique that is designed to provide the services necessary to implement point-to-point encapsulation scheme. As in IPv6 manually configured tunnels, GRE tunnels are links between two points, with a separate tunnel for each link. The tunnels are not tied to a specific passenger or transport protocol, but in this case carry IPv6 as the passenger protocol over GRE as the carrier protocol (Aburas & Mahmod, 2008). As a result of this GRE independence, it is the only tunnel method that can distinguish Integrated IS-IS from other protocols and transport that traffic on the same tunnel. The only configuration difference from the IPv6 manually configured tunnel is the last step, which specifies the tunnel type. Substituting GRE for the tunnel mode will create a GRE tunnel (Brown, 2002).

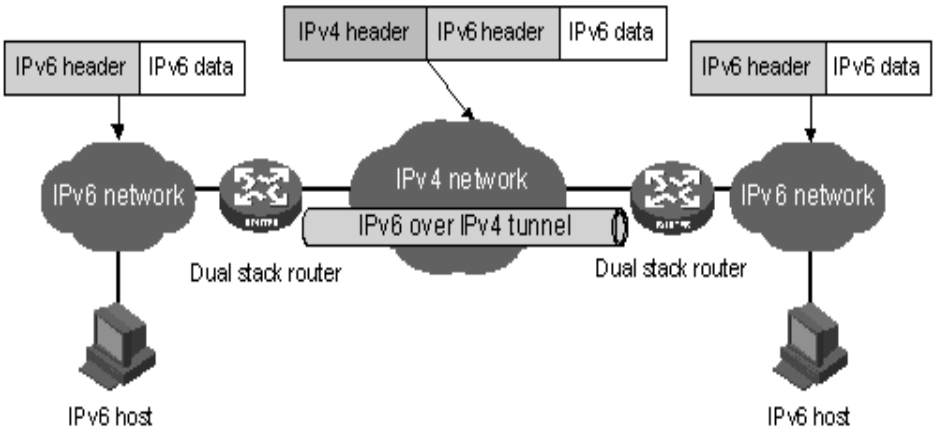


Figure 2.4: Deploying IPv6 over IPv4 Tunnels (Aburas & Mahmod, 2008).

2.1.2.3 Automatic 6to4 Tunnel

An automatic 6to4 tunnel allows isolated IPv6 domains to be connected over an IPv4 network to remote IPv6 networks. The key difference between automatic 6to4 tunnels and manually configured tunnels is that the tunnel is not point-to-point; it is point-to-multipoint. In automatic 6to4 tunnels, routers are not configured in pairs because they treat the IPv4 infrastructure as a virtual non-broadcast multi-access link. The IPv4 address embedded in the IPv6 address is used to find the other end of the automatic tunnel (Aburas & Mahmod, 2008).

An automatic 6to4 tunnel may be configured on a border router in an isolated IPv6 network, which creates a tunnel on a per-packet basis to a border router in another IPv6 network over an IPv4 infrastructure. The tunnel destination is determined by the IPv4 address of the border router extracted from the IPv6 address that starts with the prefix 2002::/16, where the format is 2002:*border-router-IPv4-address*::/48. Following the embedded IPv4 address are 16 bits that can be used to number networks within the site. The border router at each end of a 6to4 tunnel must support both the IPv4 and IPv6 protocol stacks. 6to4 tunnels are configured between border routers or between a border router and a host (Aburas & Mahmod, 2008; Juniper Network, 2009).

The simplest deployment scenario for 6to4 tunnels is to interconnect multiple IPv6 sites, each of which has at least one connection to a shared IPv4 network. This IPv4 network could be the global Internet or a corporate backbone. The key requirement is that each site has a globally unique IPv4 address (Aburas & Mahmod, 2008).

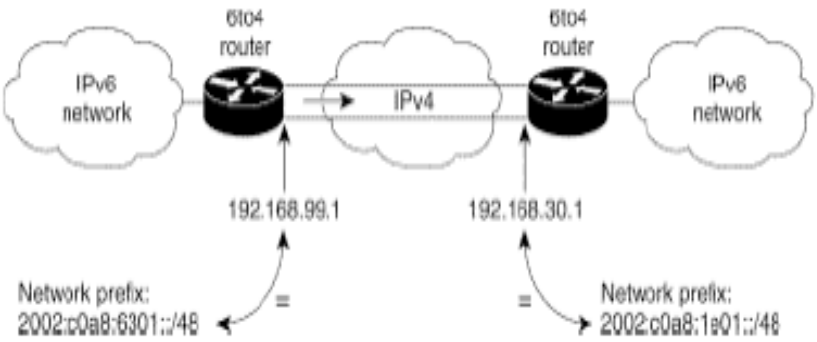


Figure 2.5: Interconnecting 6to4 Domains (Aburas & Mahmod, 2008).

2.1.2.4 Automatic IPv4-Compatible IPv6 Tunnels

Automatic IPv4-compatible tunnels use IPv4-compatible IPv6 addresses. IPv4-compatible IPv6 addresses are IPv6 unicast addresses that have zeros in the high-order 96 bits of the address, and an IPv4 address in the low-order 32 bits. They can be written as 0:0:0:0:0:0:A.B.C.D or ::A.B.C.D, where "A.B.C.D" represents the embedded IPv4 address.

The tunnel destination is automatically determined by the IPv4 address in the low-order 32 bits of IPv4-compatible IPv6 addresses. The host or router at each end of an IPv4-compatible tunnel must support both the IPv4 and IPv6 protocol stacks. IPv4-compatible tunnels can be configured between border-routers or between a border-router and a host. Using IPv4-compatible tunnels is an easy method to create tunnels for IPv6 over IPv4, but the technique does not scale for large networks because each host requires an IPv4 address and an IPv6 address to be able to determine the endpoints of the tunnel (Aburas & Mahmod, 2008).

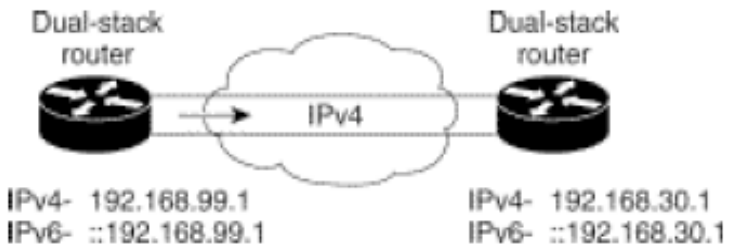


Figure 2.6: Automatic IPv4-compatible Tunnel (Aburas & Mahmod, 2008)

2.1.2.5 ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

It is one of the automatic tunnelling and it primarily used between hosts and routers, whereas manually configured tunnels are used between routers. With ISATAP, a tunnel is created from a host such as PC, to a router. The tunnel is established by using the IPv4 addresses of both the host and the router. The tunnel is automatic in that the host establishes the tunnel only when it needs to; the host is also able to discover the tunnel destination (that is, the router's IPv4 address) dynamically through DNS or a local definition. As a transition strategy, ISATAP is ideal for campus and branch sites because ISATAP allows organisations to make active IPv6 connectivity on the existing IPv4-only network while the infrastructure is gradually migrated to integrate native IPv6 capabilities. Thus, the immediate effect on the IPv4 support infrastructure is reduced to the configuration of one ISATAP router. Additionally, because ISATAP allows native IPv6 connectivity to be activated first in the backbone, other parts of the IPv4 infrastructure can preserve their investment as they naturally evolve to support IPv6 (Govil, et. al., 2008).

2.1.2.6 Tunnel Brokers

Tunnel brokers provide another technique for automatic tunnelling over IPv4 networks. The tunnel broker manages tunnel requests from dual-stack clients and tunnel-broker servers, which connect to the intended IPv6 network. Dual-stack clients attempting to access an IPv6 network can optionally be directed through DNS name resolution to a tunnel broker web server for entry of authentication credentials to authorise use of the broker service. The tunnel broker may also manage certificates for authorisation services. The client provides the IPv4 address for its end of the tunnel as well along with the desired FQDN (Fully-Qualified Domain Name) of the client (Rooney, 2007).

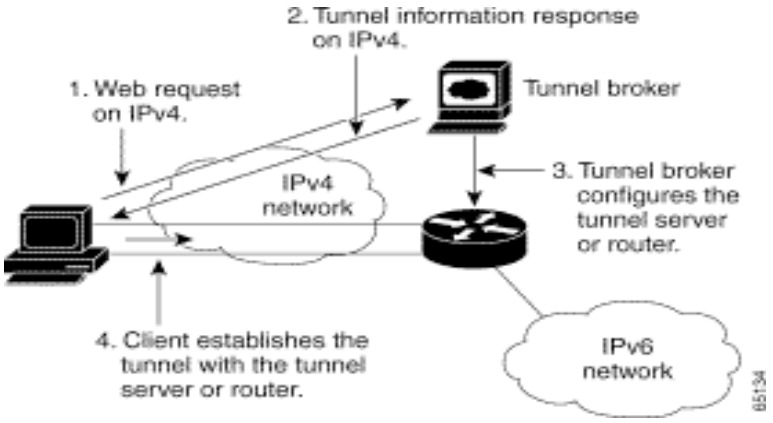


Figure 2.7: Tunnel Broker Interaction (Aburas, Mahmod, 2008)

Once authorised, the tunnel broker performs the following tasks to broker creation of the tunnel:

- Assigns and configures a tunnel server and informs the selected tunnel server of the new client
- Assigns an IPv6 address or prefix to the client based on the requested number of addresses and client type (router or host)
- Registers the client FQDN in DNS
- Informs the client of its assigned tunnel server and associated tunnel and IPv6 parameters including address/prefix and DNS name.

From an end-user perspective, setting up the tunnel connection to the IPv6 network appears similar to setting up a standard VPN connection.

2.1.3 Translation

Translation here means direct conversion of protocol such as between IPv4 and IPv6 (Waddington & Chang, 2002). It is unlike tunnels in which packets of one protocol are encapsulated within packets of another protocol. Translation mechanisms are necessary when an IPv6-Only host wants to communicate with an IPv4 host. The role of translation in IPv4/IPv6 transitioning is the conversion of IP and ICMP packets and the translation algorithm known as Stateless IP/ICMP Translation (SIIT).

SIIT (Nordmark, 2000) specifies a bidirectional translation algorithm between IPv4 and IPv6 packet headers as well as between ICMPv4 and ICMPv6 messages. Translators in the end systems can solve application to network interoperability problems. There are two end system translators such as bump-in-the-stack (BIS) and bump-in-the-API (BIA). Both of these are aimed to allowing IPv4 applications to operate over IPv6 network to meet legacy application requirements.

These techniques work at the lower layers; they have been found to be unreliable in practice due to the wide range of functionality required by common application-layer protocols (Robinson, et al., 2007).

Another way to communicate between IPv6 and IPv4 (-only nodes) is the use of application proxies in the local network (Robinson, et al., 2007). The proxy server will communicate with IPv4 on one interface and on IPv6 on the other interface and its software will perform the translation (Hogg, 2007). For example, an HTTP proxy or SMTP relays dual stack application-layer proxy. These translators really work and are efficient with a minimal intervention. The

proxy or user agent sending the request will perform a DNS search for a certain webpage like www.example.com, and then the dual-stack proxy that supports IPv4 and IPv6 will be able to receive requests from IPv4-only and from IPv6-only hosts. This will relay the request to the user agent using the address provided by the user agent that could be either IPv4 or IPv6 at registration time.

2.2 Issues and Impacts of Deploying IPv6

In this section will discuss several issues regarding to the transition mechanisms and IPv6 security related issues. The following section present related issues with details.

2.2.1 Transition Mechanism Issues

For dual stacks techniques, it can't solve IPv4 and IPv6 interworking problems. It only has the capability to handle both IPv4 and IPv6 in end system and enable like nodes to communicate within each other such as IPv6-to-IPv6 and IPv4-to-IPv4. Much more is required for a complete solution that enables IPv6-IPv4 communications (Waddington & Chang, 2002).

Since, both IPv4 and IPv6 are based on same physical platform; it will increase the CPU and memory utilisation on the system that has to run two routed protocols at the same time. DNS servers that are dual stack may even suffer a larger penalty from having to run both protocols at the same time (Waddington & Chang, 2002). Besides this, there is also the risk of performance issue with hardware.

The administrative overhead also increases with dual stack, as there is a need to operate two networks based on different network layer protocols. In addition, troubleshooting will be more difficult because there will be issue with one or the other protocol and determining where the communication

breakdown occurred will involve checking DNS and multiple stacks on the client and the server.

In addition, there are some constraints for deploying IPv6 in network such as incompatibility, distractions, stepwise transition, IPv6 standards and product evolution that mention by Govil, J. et al. (2008). The IPv6 designers made a fundamental conceptual mistake by designing the IPv6 address space as an alternative to the IPv4 address space, rather than an extension to the IPv4 address space. Therefore, a straightforward transition plan is not working with the current IPv6 specification.

Presently IPv6 address is not useful, as it cannot talk to IPv4 address. It is suppose that system needs to configure every Internet computer becomes automatically enable to talk to IPv6 address as this cannot be done overnight due to the crux of IPv6 transition.

As the IPv6 transition cycle will take years and there is no way to synchronise the process on different site. Therefore, a distributed approach is necessary. IPv6 technology is still evolving while the base set of IPv6 protocols are stable and mature, and product implementations are emerging, many of the standards supporting value-added IPv6 features are still evolving. Hence, organisations to be encouraged to ensure the IPv6 capabilities being procured have a viable upgrade path.

2.2.2 IPv6 Security Related Issues

In this section will discuss several IPv6 security related issues such as security threats similar in IPv4 and IPv6 networks, IPv6 specific security threat, security issues related to transition mechanisms, firewall issues, and intrusion detection in IPv6 networks.

2.2.2.1 Security Threats Similar in IPv4 and IPv6 Networks

IPv6 security mechanisms are much more improved comparing to IPv4, such as by implementing IPSec in IPv6. However, their evasion and misuse is still possible. Considering security issues, especially the transition period of coexistence of both IPv4 and IPv6, due to the new transition mechanism provide new way of Internet and computer systems interoperability. Other than that, some security threats against IPv4 network might also affect IPv6 network as these kinds of attacks has not fundamentally changed from IPv4 to IPv6 such as sniffing attacks, application layer attacks, flooding attacks and man-in-the-middle attacks (Zagar & Grgic, 2006; Durdagi & Buldu, 2010).

2.2.2.2 IPv6 Specific Security Threat

Besides this, there are some security issues specifically for IPv6 due to the protocol brings many difference and new features compare to IPv4. For example, these attacks are reconnaissance attacks, misuse of routing headers, and misuse of ICMPv6 and multicast (Zagar, Grgic, & Rimac-Drlje, 2007; Durdagi & Buldu, 2010). The following sub-section will discuss each type of attack in details.

2.2.2.2.1 Reconnaissance Attacks in IPv6 Network

An intruder uses reconnaissance attacks to gather essential data about the victim network, which use for further attack. To gather this information an intruder uses ping probes and port scan of the accessible system is performed. The port scan procedure for IPv6 is identical with IPv4 and the major difference is in identification of valid address due to the 128-bits of IPv6 address space, so that makes it impossible. Owing to this fact, IPv6 networks are much more resistant to reconnaissance attacks than IPv4 networks. Unfortunately, there are certain types of multicast addresses used in IPv6 networks that can help an intruder to identify and attack some resources in the targeted network (Durdagi & Buldu, 2010).

2.2.2.2.2 Security Threats Related to IPv6 Routing Headers

According to IPv6 protocol specification, all IPv6 nodes must be capable of processing routing headers. Unfortunately, routing headers can be used to avoid access controls based on destination addresses and this can create some security problems. For example, an intruder might uses spoofing packet source addresses to perform a denial-of-service (DoS) attack by using any publicity accessible host for redirecting attack packets (Zagaret et al., 2007; Durdagi & Buldu, 2010).

2.2.2.2.3 Security Threats Related to ICMPv6 and Multicast

In IPv6, there are some important mechanisms such as neighbour discovery and path maximum-transmission-unit (MTU) discovery are dependent on some types of ICMPv6 message. Therefore, it must permit some ICMPv6 message in order to have the IPv6 network properly operate. For example, "packet too big" message is required for the path MTU discovery procedure. ICMPv6 specification also allows an error notification response to be sent to multicast address. In fact, an attacker can misuse this by sending a suitable packet to a multicast address and the attacker can cause multiple response targeted at the victim (Zagar & Grgic, 2006; Durdagi & Buldu, 2010).

2.2.2.3 Security Issues Related to Transition Mechanism

On the other hand, some of the security issues might cause by transition mechanisms such as security of dual stack configuration and tunnelling mechanism. The following sub sections will present security issues related to dual stack and tunnelling in details.

2.2.2.3.1 Dual-stack

On dual-stack, both IPv4 and IPv6 attacks can target configuration host applications. Therefore, firewalls and intrusion detection systems on such hosts must support both IPv4 and IPv6 and must have proper filtering or detection rules for both protocols (Zagar et al., 2007).

Moreover, dual stack requires managing the security configurations of both IPv4 and IPv6 infrastructures. Therefore, configuring packet filter rules and access lists to provide the same level of protection for both will be difficult. A crucial issue is that the two stacks vulnerabilities will compound the attack surface, especially when IPSec is not used. Hence, the firewalls and IDS must support both IPv4 and IPv6 (Caicedo, Joshi, & Tuladhar, 2009).

2.2.2.3.2 Tunnelling

Tunnelling mechanisms may also bring new danger and misuse possibilities. Tunnelling can facilitate an intruder to avoid ingress-filtering checks. If tunnelling methods are in use, all receiving nodes must allow decapsulation of packets that can be sourced from anywhere. For example the use of tunnel broker, it will become an issue to site administrator lot of users on their site and administrator will unaware who use tunnel broker and hence, may introduce security holes which the administrator does not guard against it (Mat Taib & Budiarto, 2007).

Another example of tunnelling mechanism issue is using automatic tunnelling mechanism such as “6to4”. “6to4” connotes encapsulation of the IPv6 packet directly into the IPv4 packet and all receiving nodes must allow decapsulation of packets that can source from anywhere same as tunnel broker case from previously section. This can be a serious security problem and network address within the IPv4 and IPv6 headers may be spoofed, meaning this can mechanism can be used for denial-of-service (DoS) attacks (Zagar et al., 2007).

2.2.2.4 Firewall in IPv6 Network

Firewall is one of the most important network security mechanisms. They act as network traffic filters filtering all traffic that enters or leave the local network. It is usually positioned between a LAN and the Internet. Every received packer is being analysed and results are compared with a predefined set of rules. The firewall will accept, discard packets or sent to an additional check based on predefined rules. For IPv4 networks there are many software firewalls are available on the market included freeware and commercial version for different platform together with friendly user interface, which enable user to define filtering rules easily. However, for IPv6 firewalls are not as much as IPv4. Firewall with IPv6 support is needed to define rules separately as both IPv4 and IPv6 header format is different. Therefore, network administrator must be properly recognised and processed (Zagar et al., 2007).

Another issue is IPv4 firewall cannot be deployed in IPv6 network directly, because there are differences between IPv4 and IPv6 in packet filtering possibilities (Arifin et al., 2006). Firewall does not have capabilities of processing encrypted IPSec packet, attackers can detour the access control of packet filtering system, unless firewall can decrypt IPSec packet. However, deploying Distributed Firewall System can be applicable to the IPv6 network and has capabilities of processing encrypted IPSec packet (Lai, Jiang, Li, & Yang, 2009).

2.2.2.5 Intrusion Detection in IPv6 Network

While for Intrusion Detection System (IDS), the purpose of having IDS is to find potential security problems and to detect an unauthorised intrusion and misuse of network resources. IDS with IPv6 support should also be able to recognise and analyse IPv6 traffic tunnelled in IPv4 as IPv6 protocol defines a new header format as well as IPv6 extension headers. The IDS must implement a proper support for all types of IPv6 extension headers. Otherwise, IDS may discard a legitimate IPv6 packet going through the network (Zagar et al., 2007).

Proper deployment of IDS is also very important. If a node or a network has separate connections for IPv4 and IPv6, it is necessary to deploy proper IDS for every connection. For a dual-stack node with a single connection, deployed IDS must recognise and support both protocols. If IPv6 traffic is tunnelled, a tunnel should be terminated outside the IPv6 firewall and IDS deployed at the ingress point of a network, behind firewall.

2.3 Economical Impacts on IPv6 Migration

After discuss some of the technical and security issues from previous section, this section will discuss about economical impacts of IPv6 migration. It will mainly focus on estimation IPv6 transition costs. It is obvious that the costs of changing from IPv4 to IPv6 are vary depend on case-by-case basic according to network needs and business of the organisation. For example, for existing

organisational network infrastructure, the costs including servers, routers, firewalls, and standard and customized software programs.

Since many current network applications running on IPv4, therefore, IPv4 and IPv6 will coexist for some time before entirely network is IPv6. Even there are some transition mechanism such as dual stack, tunnelling and translation, but still it is not complete even though they are providing transition solution. There are some other issues need to consider in order to make it successful such as economic factor, which is very important to decide whether to go further into deploying IPv6 or not. These factors include the demand for IPv6 by end user, maintaining and supporting current applications, which run on IPv4, and the need of upgrading hardware and software (Arifin, Abdullah, Berhan, & Budiarto, 2006).

The first factor user demand for IPv6 is one of the strongest reasons to motivate organisation to go for IPv6 if they want to growth their business. As one of the IPv6 benefits is unlimited IP addresses and being an early adopter organisation is able to attract more end user, which also mean more business to the organisation.

The second factor maintaining and supporting current IPv4 applications, it is very important to make sure that current existing IPv4 applications are able to support IPv6. There are some old important IPv4 applications are not able to port to IPv6 and this will de-motivate organisation migrates to IPv6. However, keep on supporting old applications to their end user is not an ideal solution for long term, the maintaining and supporting cost will outweigh the benefit in long term.

The last factor the need of upgrading hardware and software, all hardware and software that are not support IPv6 are needed to upgrade. The process of upgrading and purchasing new hardware and software will be part of the product refresh cycle, by doing so will help organisations reduce costs during transition. As hardware and software vendors are increasingly integrating IPv6 as a standard feature in product, allowing organisations to deploy IPv6 as part of routine upgrade cycle (Perset, 2008).

Migration to IPv6 will involve some cost, such as hardware cost, software cost, security mechanism cost, training cost, and unexpected cost. In the following sub sections will discuss about hardware cost, software cost, security mechanism cost, employees training cost, and unexpected cost in details.

2.3.1 Hardware Cost

Hardware is one of the important elements during migration to IPv6; it consists of IPv6 router, network interface card, server switches, and hosts. The cost of hardware is depending on the organisation network how big it is and the level of IPv6 use whether deploy internally or externally or both as well as hardware can be IPv6 capable by way of software upgrades. Besides this, hardware can be classified to essential hardware and non-essential hardware. For essential hardware, it is necessary to make the network to work properly such as routers and switches. While for non-essential network, it makes network work

efficiently such as network monitoring or management system (Arifin et al., 2006).

If old hardware is not able to support IPv6 organisation needs to upgrade them. For example, host computers that are too old in term of hardware specification and not able to support IPv6 even though upgrade its operating system that supports IPv6 then the hardware cost will be high for the organisation to change the entire old host computer to new one. The cost can be reduced if the organisation renews related hardware gradually.

2.3.2 Software Cost

Software cost is another important element; upgrading some software will be required to capable with IPv6. Software upgrades includes server software, which is needed to operate the server computer such as Microsoft server software and Linux server software (Arifin et al., 2006). Desktop operating system such as old operating system that not supports IPv6 is needed to upgrade. The software cost will be high if the organisation currently is using operating system that is not supports IPv6 such as Microsoft Windows 2000 and Microsoft Windows 98 (Microsoft, 2008).

Besides this, organisation that run in-house customised software will experience additional costs to upgrade these programs to IPv6, and enterprises that have test or release processes will see a marginal additional cost for IPv6 configuration tests (Perset, 2008).

However, the main software cost that organisations see related to element management, network management, and operations support systems that are often network specific and will need revised software coding to adjust for IPv6. The cost for these element management based software are large as these software are very crucial during migration to IPv6 (Arifin et al., 2006).

2.3.3 Security Mechanisms Cost

Security mechanism cost plays a very important role besides hardware and software costs. Even though one of the IPv6 features is end-to-end security protection, but intruders and attackers are still able to perform attack toward organisations' network. For example sniffing attack, reconnaissance attacks in IPv6 network, application layer attack, DoS, etc. Security mechanism includes security hardware and security software. Security hardware includes intrusion detection system (IDS), intrusion prevention system (IPS) and firewall while security software includes antivirus, firewall software, IPS software and IDS software.

During migration to IPv6, role of edge network is very important to protect organisation's internally network security. Therefore, IDS, IPS, and firewall devices and software must be able to support IPv6, well-configure and up-to-date (Arifin et al., 2006). The cost of security mechanism can be range from low to high depending organisation's network devices at different level. The cost will be high if the organisation's network is large and many non-IPv6

support security devices need to upgrade. The cost will be low if the organisation's network is small and not many network devices need to upgrade.

2.3.4 Training Cost

Staffs training are very important for organisation that wants to deploy IPv6, as staffs need to have sufficient required knowledge and skill to configure hardware and software during migration. Existing knowledge on IPv6 will vary widely across different level of staffs in the organisation. For those responsible for daily operational upkeep of the network require more hands-on skills and vendor-specific course is more suitable for this group of staffs.

Upgrading hardware can be listed in product refresh cycle so that it helps organisation reduce cost, however, for staffs training organisation need to invest heavily and give their staffs training as soon as possible as understanding and practical experiences on IPv6 require more time to master it (Arifin et al., 2006).

The cost for staffs training is changeable depends on existing staffs knowledge with IPv6. The cost will be low if network administrators have sufficient technical knowledge and skill to configure network hardware and software. The cost will be high if the training required professional level of knowledge and advance hardware equipment as requires hiring professional trainers to train their staffs. For example, configure firewall rule-set that support both IPv4 and IPv6 and Cisco IOS software. As IPv6 is using new

packet header, which is different from IPv4 packet header, therefore, filtering rules must be defined separately for IPv4 and IPv6 traffic and must be properly recognised and processed by the IPv6 firewall.

2.3.5 Unexpected Cost

Lastly, unexpected costs that usually come in during migration as sudden accident might occur and affect the overall cost. Unexpected cost can be in hardware, software or staff. For example, staffs performance diminishing caused by the sudden change of the network system, cost that occurred when want to solve those problems in interoperability and security intrusion if the network affected by intrusion (Arifin et al, 2006). Other than that, inevitable cost when the configuration of software, application and hardware do not work as expected. The cost is varying from small; medium to large cost depends on the case.

CHAPTER 3

METHODOLOGY

This chapter will present the research approach and method that is used in this study. A method is a tool, a way to solve a problem and research new knowledge. This chapter has seven sections. The first section presents the choices of qualitative data collection approaches. The second section presents the rationale of choosing in-depth interviewing approach. The third section presents sampling strategies for selecting participants. The fourth section presents participants selection for the study. The fifth section presents preparation for conducting interview. The sixth section presents development of interviewing guide. The last section presents data analysis method and this chapter concludes with a summary.

3.1 The Choices of Qualitative Data Collection Approaches

This section presents choices of qualitative data collection approaches for study use. There are total three approaches will be discussed such as observation, focus group, and in-depth interviewing in the following sub sections.

3.1.1 Observation

Observation entails the systematic noting and recording of events, behaviours, and artefacts (objects) in the social setting chosen for study (Marshall & Rossman, 2006). The observation records are often referred as field notes, which are detailed, non-judgmental, and concentrate descriptions of what has been observed. Classroom studies are one example of observation, often found in education, in which the researcher documents and describes actions and interactions that are complex: what they mean can only inferred without other sources of information (Marshall & Rossman, 2006). This method assumes that behaviour is purposeful and expressive of deeper values and beliefs.

Observation is a fundamental and highly important method in all-qualitative inquiry (Marshall & Rossman, 2006). It is used to discover complex interactions in natural social settings. Even in studies using in-depth interviews, observation plays an important role as the research notes the interviewee's body language and affects along with his/her words. However, a method requires a great deal of the research. Observer's comments are often a quite fruitful source of analytic insights and clues that focus data collection more tightly. They may also provide important questions for subsequent interviews.

One of the advantages of observation study is it reveal interrelationship among multifaceted dimensions of group interactions. Besides this, it is useful when the subject is feared to provide inaccurate information. It also helps determine questions and types of follow up research based on the group experience.

The disadvantages of observation study are it could cause bias on that study due to bias opinion on the subject. The study group may not be representative of the larger population and it takes time to build trust with subject that facilitates full and honest self-representation.

3.1.2 Focus Groups

The method of interviewing participants in focus groups comes largely from marketing research, but has been widely adapted to include social science and applied research (Marshall & Rossman, 2006). The groups are generally composed of four to twelve people who are unfamiliar with one another and have been selected because they share certain characteristics relevant to the study's questions. The interviewer creates a supportive environment, asking focused questions to encourage discussion and the expression of differing opinions and point of views. These interviews may be conducted several times with different individuals so that the researcher can identify trends in the perceptions and opinions expressed.

The advantages of focus group interviews are that this method is social oriented, studying participants in an atmosphere more natural than artificial experimental circumstances and more relaxed than a one-to-one interview. Besides this, the cost of focus groups is relatively low, they provide quick result, and they can increase the sample size of qualitative studies by permitting more people to be interviewed at one time.

However, certain disadvantages to this method as well, which is the issue of power dynamics in the focus group setting (Marshall & Rossman, 2006). Should the researcher choose to use the method he/she should be aware of power dynamics and be able to facilitate well – these are crucial skills. In addition, the interview often has less control over a group interview than an individual one. Time can be wasted while irrelevant issues are discussed.

3.1.3 In-depth Interviewing

In-depth or unstructured interviews are one of the main methods of data collection used in qualitative research (Ritchie & Lewis, 2003). Qualitative researchers rely quite extensively on in-depth interviewing. They take different forms but a key feature is their ability to provide an undiluted focus on individual. They provide an opportunity for detailed investigation of people's personal perspectives, for in-depth understanding of the personal context within which the research phenomenon are located, and for very detailed subject coverage (Ritchie & Lewis, 2003).

Interviewing can be categorised into three general categories: the informal, conversational interview; the general interview guide approach; and the standardised, open ended interview (Marshall & Rossman, 2006). In-depth interviewing is often described as a form of conversation with a purpose. However, there are some obvious different between normal conversation and in-depth interviews such as their objectives, and the roles of researcher are quite different.

In-depth interviews have particular strength. An interview yields data in quality quickly as researchers can immediately follow-up and clarification respondents. Face-to-face interview combined with observation, it allow researcher to understand the interaction of respondent through body language. Besides this, the respondents themselves can raise and suggest important research issues in an interview.

However, in-depth interviewing has limitation and weakness. It involves personal interaction; cooperation is essential. Interviewees may be unwilling or maybe uncomfortable sharing all that the interviewer hopes to explore (Ritchie & Lewis, 2003). The interviewer may not ask questions that evoke long narratives from participants because of a lack of skill (Marshall & Rossman, 2006). Therefore, the interviewers must be knowledgeable, skilled, and well prepared before entering the field. The interviewer must be adept at building rapport, an interpersonal skill used to develop trust and reduce reticence.

3.2 Rationale for Using In-depth Interviewing

In this study, the benefits of in-depth interviewing outweigh the disadvantages. A primary reason for using interviewing in this study is to allow the researcher to examine phenomenon, in this case the cost-benefit of organisational migration to IPv6, is unknown. Thus, an interview provides the needed flexibility to probe ideas that emerge during the interview dialogue to understand the phenomenon. Interviewing and probing is also a necessity

because the research questions focus on cost-benefits analysis on organisational migration to IPv6 and hidden impacts during migration.

3.3 Sampling Strategies

When sampling strategies are described, a key distinction is made between probability and non-probability samples. Probability sampling is generally held to be the most rigorous approach to sampling for statistical research, but is largely inappropriate for qualitative research.

Qualitative research uses non-probability samples for selecting the population for study. In a non-probability sample, units are deliberately selected to reflect particular features of or groups within the sampled population. The sample is not intended to be statistically representative: the chances of selection for each element are unknown but, instead, the characteristics of the population are used as the basic of selection (Ritchie & Lewis, 2003). These features make them well suited to small-scale, in-depth studies, as we will go on to show. The main sampling approach for qualitative enquiry in this study is summarised below.

3.3.1 Criterion Based or Purposive Sampling

In this approach, the selection of participants, settings or other sampling units is criterion based or purposive. The sample units are chosen because they have particular features or characteristics which will enable detailed exploration and understanding of the central themes and puzzles which the research wishes to study.

Purposive sampling is precisely what the name suggests. Members of a sample are chosen with a purpose to represent a location or type in relation to a key criterion (Ritchie & Lewis, 2003). This has two principle aims. The first is to ensure that all the key constituencies of relevance to the subject matter are covered. The second is to ensure that, within each of the key criteria, some diversity is included so that the impact of the characteristic concerned can be explored. For example in this study, organisational migration to IPv6 is used as selection criterion. This is important both to ensure that all relevant organisational are included and to ensure that any differences in migration perspective between organisational can be explored.

3.3.2 Sample Size

Qualitative samples are usually small in size and there are three main reasons for this. First, the type of information that qualitative studies yield is rich in detail. There will therefore be many hundreds of information from the each unit of data collection.

Second, statements about incidence or prevalence are not the concern of qualitative research. There is therefore no requirement to ensure that the sample is of sufficient scale to provide estimates, or to determine statically significant discriminatory variables. This is sharp contrast to survey samples, which need to have adequately sized cells to draw statistical inference with the required precision (Ritchie & Lewis, 2003).

Third, a small sample size allows for longer, more in-depth interviews. An in-depth interview is necessary because studying cost-benefit analysis in organisational migration to IPv6 involves exploring new questions, something that requires probing, time, and reflection. Besides, this interviewing a small number of organisational is more reasonable in terms of scheduling. Given the expectation that the interviews will last up to an hour and the transcription and analysis will last a great deal more time, it seems necessary to interview only a small number of individuals.

3.4 Participant Selection

The selection of study participants uses a set of specific criteria to identify certain types of industry that were most likely to provide information pertinent to answering the research questions. The criterion for identifying and selecting subjects to interview includes networking service providers, IT software house, and high usage of internal network type of organisations.

The rationale of using these types of organisations because network service provider requires many IP addresses and network infrastructure when help clients to setup their network. For IT software house, the reason is because they might develop IPv6 applications in near future. Therefore, it is one of the industries to consider in participant selection. For the participants' selection, the author will divide organisations into 2 types such as business type and non-profits type or organisation. The rationale of doing this because not only business organisations need to migrate their network to IPv6, but NPOs needs to migrate too. The relationship of selection criterion to the research questions is to determine the costs-benefits of these organisations when their networks migrate to IPv6.

3.4.1 Limitation Regarding Participant Selection

The decision mentioned above had a limiting effect on the study's findings and their generalisation. The most significant limitation arising from the selection of study participants is since the participations are from only certain types of organisations. It is difficult to generalise the study findings to other organisation. It is possible that the different network environment will lead to different migration strategies and impacts.

3.5 Conducting Interviews

The researcher conducted interviews during June 2011 in interviewees' office. The researcher used a semi-structured interview guide as a basic for asking question. The interviews were recorded using digital voice recorder. The following sub section explains the details of the interviews.

3.5.1 Interview Scheduling and Reminders

After identifying prospective participants (see section above), the researcher approached them by sending email and invited them to participate in the study. The researcher described the study to each prospective participant and was told that their identities would remain anonymous if they chose to participate and that the result of the research would be reported in a manner that would not allow someone to deduce their identity. Each participant that was asked to participate agreed to do so. The interview scheduled spanned two-months (June 2011-August 2011).

3.5.2 Interview Location

Each interview occurred within interviewees' office. Conducting interviews in their work place provides convenience and familiar context to them. Interviews occurred in the evening after interviewees are finished work. The reason interviewing took place after they finished work was to avoid potentially distractions during the interview.

3.5.3 Interview Audio Recording, Length, and Field Note

The interview lasted between 20-30 minutes depending on the follow-up questions and probes. All the interviews were recorded on digital voice recorder to ensure that the interview was transcribed accurately. As interviews were being conducted, the researcher took field notes. These notes attempt to describe the latent content of the interviews and record any issues that appeared to re-emerge in each interview.

3.6 Developing the Interviewing Guide

The interviewing guide is semi-structured, which means that it utilises a common set of questions but ultimately relies upon probing and follow-up questions to explore subject areas and obtain deeper understanding. The next sections further explain the semi-structured interview guide including the

standard interview questions, examples of typical probing questions, and pilot testing.

3.6.1 Standard Interview Questions and Probing

This section explains the rationale behind each standard interview question and the types of probes associated with each question. There were a total of eight scheduled questions and the general purpose of each question is to initiate a dialogue within a particular research area so that the researcher can probe the respondent with follow-up questions to discover deeper meaning. Probing includes a series of follow-up questions that occur after asking each major question. Determining the follow-up questions was a constructive process build within the course of the interview dialogue. The researcher made filed notes directly on the interview guide during each interview to help organise and monitor the use of follow-up questions and probing. Thus, the researcher became better at choosing follow-up questions in parallel with becoming more skilled at listening, note-taking, and anticipated responses. Table 3.1 below shows scheduled interview questions, typical probes, and explanation.

Table 3.1: Scheduled Interview Questions and Explanation

Scheduled Questions	Typical Probes	Explanation
Imagine you are now a network		Question 1 is useful as an introductory question

engineer, who is planning to migrate your current company network to support IPv6. Could you please explain how are you going to perform the entire migration?		because it is flexible and non-leading, allowing for a wide-range of ways to being the interview dialogue and build rapport with subjects. However, the likelihood of numerous different responses, many of which may be unanticipated, does require extra caution, by way of field notes, to carefully and thoroughly follow-up all possible leads.
When are you going to implement it? Could you please explain the rationale behind it?	• How long duration needed to complete the migration? • What makes you take so long to complete?	Question 2 provides specificity to the interview questions by focusing on the migration timeline. This is important because organisations' migration timeline affect IPv6 adoption in Malaysia. This question also could answer the reasons IPv6 slow in adoption. Question 2 probes allows for examining how interviewees from different organisations define their migration duration and their reasons of having such duration.
Could you please estimate the costs involved in the migration, in term of: • Human resource / training • Hardware and software cost • Long term maintenance	• How much cost do you plan in employee training? • With your current existing network infrastructure, how many network equipment do you need to upgrade to support IPv6? • What about incompatible software? Do you have in-house development team to upgrade the software or	The purpose of Question 3 is to begin a discussion about costs that are needed in IPv6 migration. Personnel or training costs are needed to give employee training on IPv6 such as setup and configuration on IPv6. Hardware and software costs are needed to upgrade incompatible network equipment, PC, notebooks, and software. Long-term maintenance costs needed to maintain IPv6 network in long run such as solving incompatible issues, servers crashing, etc. Question 3 probes allows for examining how interviewers plan their

	outsource to other software house? • Approximately, how much do you need to upgrade all of them?	budget accordingly in different aspects.
If you were going to get IPv6 in your company network, would you prefer implement internal network first, external network, partial or both networks implement together?	• Why do you choose ____?	Question 4 is examining how interviewees from different organisation plan their migration method. The result of choice examines organisations migration cultures and their way of handling unexpected events occurs. Question 4 probes allows for examining the rationale of organisation for choosing this type of migration plan.
Which transitional mechanism model (i.e. Dual stack, tunnelling, and translation) would you prefer to apply in IPv6 migration?	• Why do you choose ____? • Will it easily to setup or maintain than other model?	The purpose of Question 5 is to understand how interviewees from different organisation decide their transitional mechanism model and their rationale of choosing that particular model. This question probes indirectly answer three costs involved in IPv6 migration (see Question 3).
Could you please describe what would be affected while you upgrade your network to IPv6?	• Why it would be affected? • How it affects? • Who will get affected?	Questions 6 are examining unexpected costs that may occur while organisation upgrade their network to IPv6. This question probes allows for deeper understanding on things that get affected, how the things affect organisation operations, which will be get affected by this, and so on.
Could you please explain how would	• Do you include more manpower to	Question 7 is a follow-up question for Question 6. The

you handle the problems if there were an estimate goes wrong during the migration, which is affecting your company daily operation?	solve the problems? • Does your original migration timeline and costs get affected by this?	purpose of this question is to examining step taken by interviewers' organisation to restore the problems during the migration. Question 7 probes allows for deeper understanding on the way of interviewees handle the problems. The result of this question may directly affects original scheduled timeline and costs, which may imply unexpected costs.
What are the benefits that your company will enjoy after the IPv6 migration is successful?	• How these benefits help your company in daily operation? • With these benefits, how would your company compete with competitors?	The purpose of Question 8 is to understand benefits of IPv6 that interviewees' company will enjoy and the way of IPv6 benefits help them in daily operation. However, probing on this question is depending on situational.

3.6.2 Pilot Interview

Pilot interviews were conducted with several employees in targeted organisations. All employees were asked to participate in the pilot interviews are not part of the final sample. The purpose of the pilot interviewing was to uncover ineffective questions such as confusing questions and poorly sequenced questions. In addition, the pilot interviews allowed the interviewer to practice interviewing procedures including probing, note taking, building rapport, audio recording, and timing.

3.7 Data Analysis

Interviews were analysed using Glaser and Strauss' method of ground theory. Grounded Theory Method (GTM) is defined as a research method that seeks to develop a new theory or to test an already existing theory that is grounded in data. The data are systematically generated and analysed step-by-step to develop a theory. The resulting theory is an explanation of categories, including related concepts their properties, and the relationships among them (Mavetera & Kroeze, 2009).

In grounded theory, variables are referred to as categories or concepts and the researcher attempts to explain in the interrelationships between emergent categories. The development of these categories enables the research to reduce data into more manageable amounts, so that patterns can emerge, thus structuring the theory.

The basic procedure used in a grounded theory approach is to read and reread interview transcripts and field notes, with the purpose of discovering and labelling variables by using a process called open-coding (Mavetera & Kroeze, 2009). By constant comparison of the newly collected data with the initial results, the process gradually advances from coding parts of the data to conceptual categories, and subsequently to conceptual modelling or theory development (Boeije, 2010). The following sections describe the coding and categorising of the interview data.

3.7.1 Grounded Theory Method Coding

Coding means categorising segments of data with a short name that simultaneously summarises and accounts for each piece of data. Coding was developed as a technique in the grounded theory approach, and has been increasingly refined since. At first, the data may appear to be a bulky, diverse collection of accounts, but coding is a tool with which to create order. There are three types of coding that are distinguished, namely open, axial, and selective coding (Boeije, 2010). These three types are expanded on in the following sections.

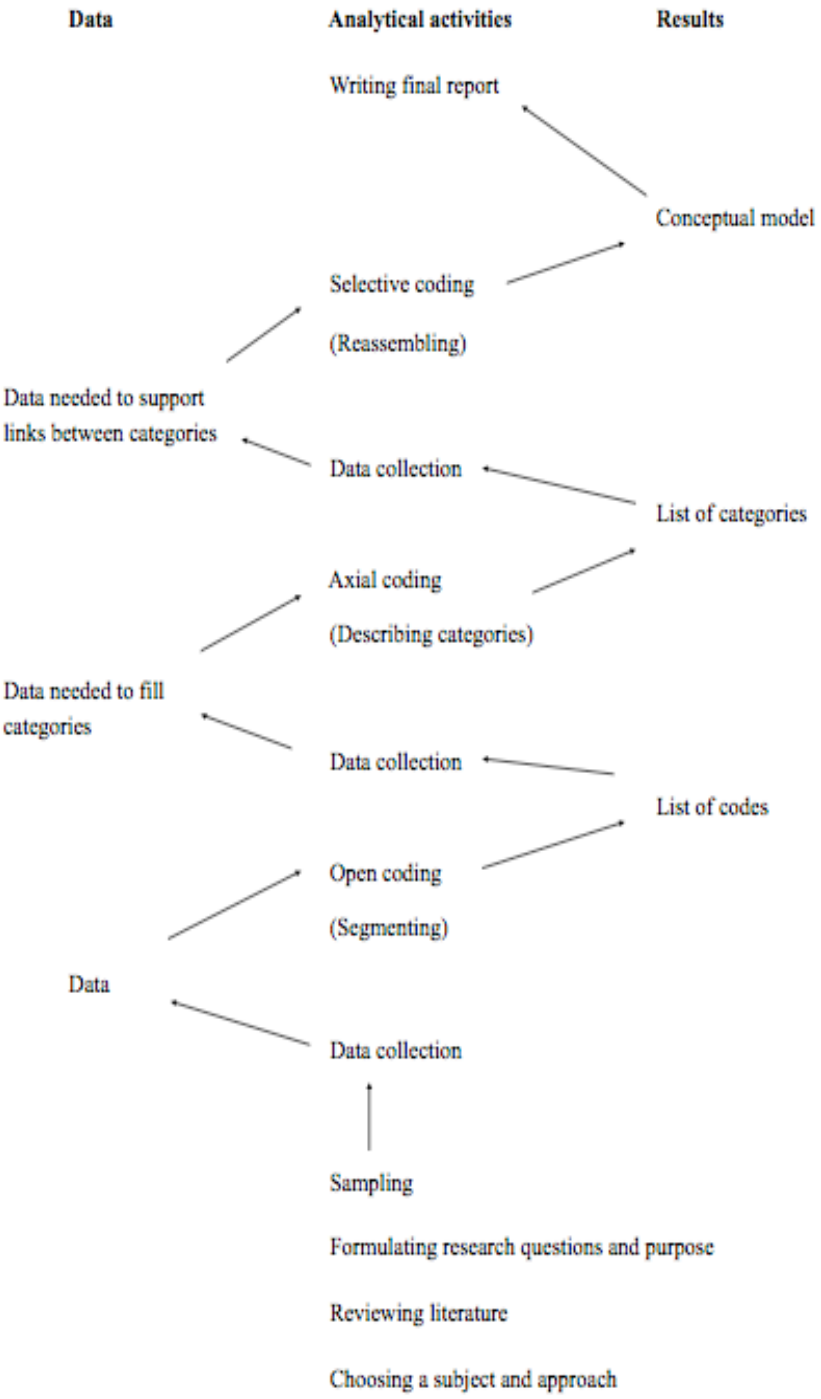


Figure 3.1: Data Analysis Sequencing and Procedures

3.7.2 Open Coding

Open coding is the process of breaking down, examining, comparing, conceptualising and categorising data (Boeije, 2010). This means that all data that have been collected up to that point are read very carefully and divided into fragments. The fragments are compared among each other, grouped into categories dealing with the same object, and labelled with a code.

Open coding usually takes place at the beginning of the research and starts during the collection of first round of data. A code is a summarising phrase for a piece of text, which expresses the meaning of the fragment. A code does not have to be complex or difficult to understand.

The result of open coding is a list of codes, also referred to as a coding scheme. The codes can be sorted by alphabetically or in an order determined by the researcher. The phase of open coding can be ended if no new codes are necessary and this entire process may repeat itself several times until second or third round of data collection. For example, a list of codes may resemble Table 3.2.

Table 3.2: Example of A Code Tree in The Research

Hardware Cost
Hosts • Personal Computer • Notebook
Network Equipment • Router • Firewall • Switch

3.7.3 Axial Coding

Axial coding refers to the formation of categories from the list of codes developed during open coding and then relating the properties of categories to each other, through a combination of inductive and deductive thinking (Boeije, 2010). The primary purpose of axial coding is to determine which elements in the research are the dominant ones and which are the less important ones. As insights into the field increase and ideas about the observed social phenomena develop, confidence grows in making choice among the codes and the connections between them. The second purpose of axial coding is to reduce and reorganise the data set such as synonyms are crossed out, redundant codes are removed and the best representative codes are selected. All activities are employed to gradually focus the research.

In this research study, after identifying, describing, and organising multiple concepts, the next step is to create sets of categories. For example, during this step of coding it become clear that what organisations were talking about in terms of concepts such as hosts, network equipment, and other related concepts should be combined into a single category called hardware costs. For example, the hardware costs category is depicted in Table 3.3.

Table 3.3: Example of Category Formulation

Procurement
Replace incompatible IPv6 devices
Migration timeline
Migration duration
IPv6 compatible software
IPv6 compatible devices
Migration plan
Migration mechanism
System doesn't work
Migrate gradually

3.7.4 Selective Coding

Selective coding refers to looking for connection between the categories to make sense of what happening in the field. Selective coding is aimed at integrating the loose pieces of earlier coding efforts and integrating them to create a single theoretical framework (Boeije, 2010). The initial step in creating the theoretical framework is to select a central category. For example the theoretical framework that emerged in this study consists of a central category consisting of several types of costs needed on IPv6 migration, organisations migration plan and duration, and unexpected impacts on stakeholders. Once selected, the core category becomes the primary character in the development of a single storyline around which all other categories, concepts, and themes are organised. Selecting an appealing, dynamic central character is very important for grounded theorists since the process of building theory is parallels that for writing a story. Thus, selective coding is really about finding the driver that impels the story forward.

The guidelines of deciding core category (Boeije, 2010):

1. Research question and purpose: the most influential factors in determining how the data will be integrated and what the findings will look like.

2. Literature: the result is contrasted with the relevant literature and demonstrates how the sensitising concepts have functioned.

3. Data: the outcome is guided by what stands out in the data in terms of richness and the insights they has yielded.

4. Actuality: the results occasionally grow in value if they fit the actual context of societal and scientific debates or events.

In the final phase of the analysis, the definitive findings are shaped. Instead of the chronological order in which the data were originally collected, the data now stand in the order implied by the data and the research questions.

Conclusion

This study uses interviews to collect data from organisations to find out how these organisations migrate to IPv6 in minimal cost. Finding out how organisations migrate to IPv6 in minimal cost is difficult without actually asking these organisations. Thus, interviewing allows the researcher direct interaction with the organisations' employee; it is the preferred method of data collection for this study.

The interview data was analysed using Glaser and Strauss' method of grounded theory. This method is particularly appropriate for studies with a small number of participants because this form of data analysis offers insight, enhances understanding, and provides a meaningful guide for explaining a new subject. In addition, grounded theory results in a core category that can be used to effectively explain study findings in such a way that it helps to build a new theoretical framework. The core category identified for this study is the deployment costs for organisations migrate to IPv6, a category that ties together hardware costs, software costs, labour costs, and other costs. The following chapters discuss about findings of this study.

CHAPTER 4

RESULTS AND DISCUSSION

This chapter presents the results of analysing the interviews. The first section presents general observations about the study participants. The second section presents study findings related to IPv6 deployment costs on organisational migrate to IPv6 based on Figure 4.1. The third section present benefits of IPv6 after migration. The last section present a general cost-benefit analysis calculation for IPv6 migration based on findings. This chapter concludes with a summary of these findings.

4.1 Interview Analysis Summary

There are total of three participants in the interview process. Participant A is a network administrator from Organisation X; Participant B is a network administrator from Organisation Y; and Participant C is a network engineer from Organisation Z.

The interview data was analysed using a version of Glaser and Strauss open coding technique (see Chapter 8 Methodology). The basic procedure used in open coding involves the researcher reading and re-reading interview

transcripts in order to identify and label emergent, distinguishing features. Then, the researcher combines those features with strong commonalities into a single theme. Upon identifying a theme, the researcher gives it a label or name that is representative of its common features. Finally, the researcher examines relationships within themes and between themes and the study variables in order to generate a set of findings. In this study, the theme is deployment costs needed for organisations to migrate IPv6. Figure 4.1 will be used as interview analysis model throughout this chapter. The next section provides general observations about the study participants.

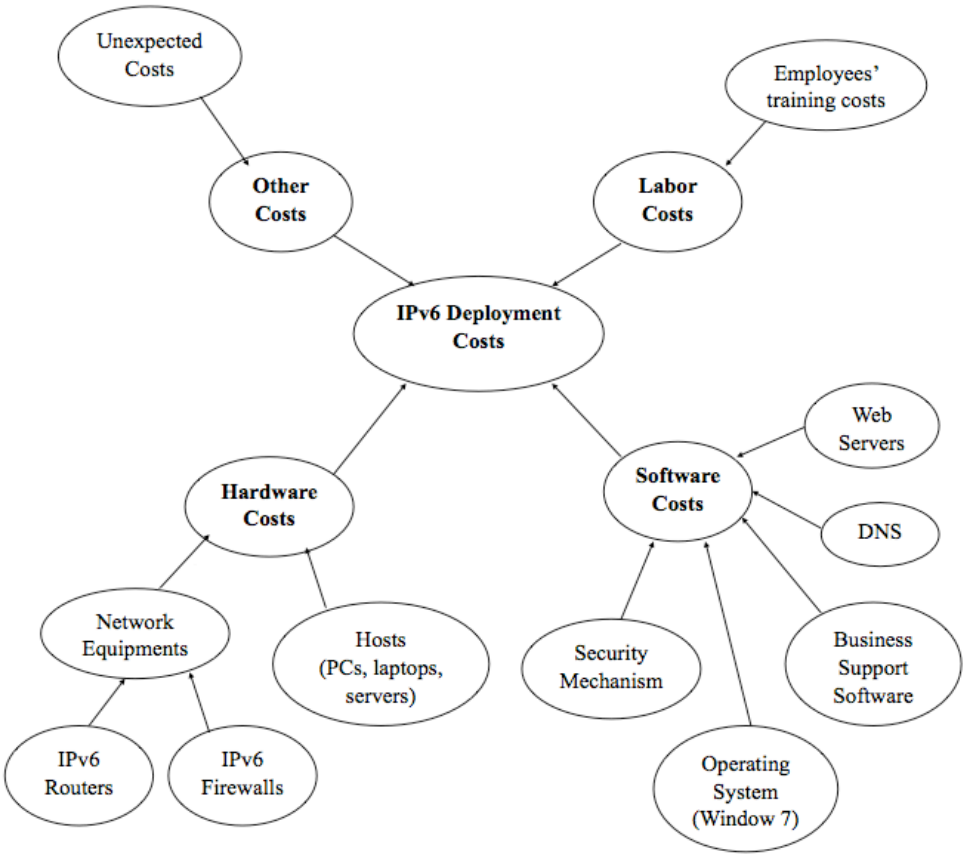


Figure 4.1: Interview Analysis Model

4.2 General Observations Associated with Study Participants

Interview analysis began with a general examination of the interviews in terms of their ideas on IPv6 migration, IPv6 adoption factor, IPv6 migration strategy, migration timeline and duration, IPv6 transitional mechanism, and preferable network to deploy IPv6. Interviews indicated that participants have a wide variety of ideas on how they perform IPv6 migration. Table 4.1 shows the summary of general observations between business organisations and NPO.

Table 4.1: General Observations Associated with Study Participants

General Observations Associated with Study Participants		
General Observation	**Business Organisation**	**Non-profit Organisation (NPO)**
IPv6 adoption factor	Doesn't have any plan at the moment, because vendors do not support IPv6 in a scalable and high performance manner.	It is good to be ready early so that organisation would not face any problem when IPv4 is phased out.
IPv6 migration strategy	Upgrade internal IPv4 configuration, re-configure them to support IPv6 and replace all unsupported IPv6 devices.	Perform the migration gradually to ensure operating system, computers, network equipment, and software are IPv6 support.
Migration timeline and duration	Doesn't define the timeline and duration, but IPv6 migration would start when there are no more global IPv4 addresses.	IPv6 migration will perform by end of the year 2011 and the migration takes about six months to complete.
IPv6 transitional mechanism	Implement dual stack mechanism for internal network and tunnelling mechanism for external network.	Implement dual stack mechanism for internal network and tunnelling mechanism for external network.

Preferable network to deploy IPv6	Implementing internal and external networks concurrently for parts of the organisation to test and work with real environment.	Implementing internal network with dual stack, because external network is connected to ISP and it is not yet ready for IPv6.

When asked about adoption factor to deploy IPv6, one of the participants from business organisation mentioned that adoption factor for his organisation is unknown. This is because many vendors support IPv6 on paper, but do not support it in a scalable, high performance manner or do not support all of the features needed. Therefore, his organisation doesn't have any plan to deploy IPv6 now. However, participant from NPO mentioned that migration to IPv6 would have to happen eventually, it is good to be ready early so that his organisation would not face any problems when IPv4 is phased out in the future and his organisation would not need to rush to implement it.

When asked how they would perform IPv6 migration, one of the participants from business organisation suggests his company will upgrade the entire current internal IPv4 configuration and re-configure them to support IPv6. The reasons they upgrade internal network first, as they don't wish to impact their clients. He mentioned they would create a test lab environment to simulate their internal network with new IPv6 support network equipment to test IPv6 before they setup in their internal network. Besides this, he also suggested to replace all hosts and devices that are not support IPv6 to new IPv6 support devices. He also added that these new IPv6 support devices would be included in the coming product refresh cycle.

On the other hand, participant from non-profit organisation (NPO) suggests that his organisation would perform the migration gradually to ensure operating system; personal computers, notebooks, network equipment, and software are IPv6 support. The reason is that most of their personal computers and notebooks are still using Windows XP. Even there are several patches that enable Windows XP to support IPv6, but it is not support IPv6 by default and his organisation is planning to upgrade their operating system to Windows 7, which is native IPv6 support. Besides this, migrates gradually enable his organisation have sufficient time to sent their staff for IPv6 training. In addition, this approach minimises capital expenses and helps ensure that network equipment is already IPv6-capable when the organisation wants to begin using IPv6-capable applications and computers.

When asking about migration timeline and duration, one of the participants from business organisation not to disclose about the migration timeline as well as the duration of the migration. He just mentioned his organisation would start IPv6 migration when there is no more room for global IPv4 addresses. He also added when all the required infrastructure and software applications are running fine, then the migration will perform. When probes for reason, he mentioned there is no necessary to upgrade IPv6 now if the company runs fine with current IPv4, it is better to stay on IPv4 until the support of it ends.

However, participant from NPO mentioned that his organisation will perform the IPv6 migration by end of the year 2011 and it takes about six months to complete the migration. The reason of taking six months is because they want to ensure their operating system, software used in server and personal computers are ready for IPv6. About three months are used in planning and re-configuring all networks devices and end devices with IPv6 addresses. Another three months are used to re-installing and upgrading all old operating system to the newer one.

When asking about which IPv6 transitional mechanism is preferable to apply in IPv6, participants form both business organisations and NPO suggest dual stack mechanism used in internal network and apply tunnelling mechanism for external network. Participant from NPO stated that by using dual stack in internal network allows his organisation to ensure that in case he overlooked if any system in his network are not IPv6 ready, this will ensure continuity of his organisation daily operations without any disruption.

One of the participants from business organisations mentioned IPv4 and IPv6 would need to co-exist for many years in most organisations. This is because if an organisation completely turned off support for IPv4 in the network, then its IPv4 applications, web sites, and services would no longer work. By continuing to support IPv4, the organisation can gradually upgrade applications to IPv6 and test, which is less expensive than upgrading and testing all applications at once. Besides this, it might not be possible to add IPv6 support to older applications for which a company does not own the source code.

When asking about which networks are preferable to implement first, internal network or external network, participant from NPO suggests implementing internal network with dual stack first. This is because external network is connected to Internet Service Provider (ISP) and external network is not yet ready for IPv6. He also added implement IPv6 to external network when ISP instructs them to do so.

However, another participant from business organisation suggests goes for partial migration, which mean internal and external networks implement concurrently. In addition, he mentioned this partial migration implementation is only for part of his organisations and not entire of the organisation's network. The reason he implements partial migration for parts of his organisation is because to allow his team to test and work with the real environment. He suggests implement internal network with dual stack first instead of implement IPv6 on external network or implement both internal and external networks together for entire organisation's network. This is because affecting their clients is the last choice if they don't have other alternatives option. He said implement both internal and external networks together is like "jump the bridge without a robe".

This section has shows that participants from different organisations and from different industry have different IPv6 migration planning, strategy, transitional mechanisms, timeline, and duration. Some organisations already start planning and implement by end of the year, while some organisations are still waiting for last minute migration due to some reasons mentioned in the

previous section. The following section presents findings related to hardware costs, which is part of the deployment costs for IPv6 migration.

4.3 Study Findings Associated with Hardware Cost

This section examines the interviews in term of how organisations in different industries plan their IT budget on hardware costs so that all required hardware are IPv6 support. The interviews analysis is based on Figure 4.1 and hardware costs can be divided into two categories such as hardware costs for hosts and hardware costs for network equipment. This section begins with findings on business organisations and NPO. Finally, this section concludes with a summary of study findings associate with hardware costs.

Table 4.2: Study Findings Associated with Hardware Cost

Study Findings Associated with Hardware Cost	
Hardware	**Findings**
Hosts	Most of the employees are still using old notebook and personal computer and part of these devices' hardware parts are incompatible with IPv6 due to hardware manufacture no longer support that particular old hardware. Therefore, upgrade costs are varied across organisations and it is depends on amount of hosts that are needed to upgrade.
Network Equipment	Network equipment such as router, switches, and firewalls, which is not IPv6 support are needed to upgrade. Purchasing new network equipment requires careful planning so that new network equipment able to handle organisation daily operation without failure. Upgrade cost for both business organisation and NPO are varied and depend on amount of

	network equipment that is needed to upgrade.

4.3.1 Findings Associated with Hardware Cost

The interviews indicate that most of the hosts such as personal computer, notebooks used by their employee, and servers are needed to upgrade to the newer version. As most of the employees are still using old personal computers, notebooks, and these devices' hardware parts are incompatible with IPv6. This is because manufacture no longer support firmware upgrade for old hardware. Therefore, old hardware parts are incompatible with IPv6 and needed to phase out in the next product refresh cycle. Besides this, some companies are still using old servers, which is not fully IPv6 supports are needed to upgrade to new fully IPv6 support servers. According to one of the participants, he said most of the small-medium enterprise (SME) doesn't have so much resource allocate on IT to upgrade their old hardware compare to large organisations and some SME took more than ten years to refresh their old hardware.

However, for NPO, unit of servers are not as many as business organisations. Unlike business organisations, NPO mainly is about social cause or servicing organisations. Thus, expenses on servers, hardware, and license software for NPO would be much lesser than business organisations.

In addition, old network equipment such as routers, switches, and firewalls, which is not IPv6 support are needed to upgrade. The routers are the

most important systems, because these systems are dealing with routing IPv6 traffic between the different networks. Therefore, decision in buying new equipment is crucial to organisations. There is many planning and meeting on going to ensure the new equipment are able to handle their company daily operations without affecting their clients and their internal employees.

One of the participants from business organisation mentioned that his company just changed most of the routers and firewalls several years ago to support IPv6. He also mentioned that additional cost, which is unnecessary if the company have Cisco devices because most Cisco IOS software is supported with IPv6 feature since 2001. Therefore, rather than replacing foundation devices, his company only needed to help ensure that they had adequate memory and were running a version of the Cisco IOS software that support IPv6 capabilities.

When asking about the preferable brands for their network equipment, all participants mentioned their company prefers Cisco products. The reason is their company is having good experience with Cisco products and having good support from Cisco. Therefore, they plan to continue with Cisco products in future. The next sub-section summarizes findings associated with hardware costs for business organisations and NPO.

Summary Findings Associated with Hardware Cost

Findings indicate that both business organisations and NPO have common infrastructures to upgrade to support IPv6. Infrastructures such as personal computers and notebooks are crucial to support daily operation while network equipment are important to establish connection between Internet and hosts to enable organisations provide services to clients. Besides this, most of the organisations had plan their next product refresh cycle include IPv6 support devices and network equipment to avoid last minute migration.

Findings also shows that different organisations have different amount of hosts and network equipment needed to upgrade as every organisation's network size is different. Thus, IT budget allocated on hardware for each organisation is different as well. The next section presents findings associated with software costs needed for IPv6 deployment.

4.4 Study Findings Associated with Software Cost

This section examines interviews in term of software costs that are needed for business organisations and NPO to upgrade their network to IPv6. The interview analysis begin with analysis different types of software costs such as security mechanism software, operating system, web servers, business support system, and domain name system (DNS) for both business organisations and NPO. Finally, this section concludes with a summary of study findings associated with software costs.

Table 4.3: Study Findings Associated with Software Cost

Study Findings Associated with Software Cost	
Software	**Findings**
Operating system	Both employees in business organisation and NPO are still using Windows XP in their workplace and Windows XP by default is not fully IPv6 support. Therefore, both business organisation and NPO are needed to upgrade their operating system from Windows XP to Windows 7 to support IPv6 by default. Upgrading cost can be range from low to high and it is depends on organisations' size.
Business Support System	Most of the business support system is matured and stable to handle daily business operation, but not many of them are support IPv6 yet. Upgrading business support system is not an easy job; it is very time and resource consuming to ensure new system work perfectly. Upgrading cost is high compared to other software cost.
Web servers	Upgrading web server application enables web server receives IPv6 connection requests from clients. Upgrading cost is varied and it is depends on number of servers operating in organisation and staff knowledge on IPv6. Upgrade cost would be low if their technical staff's are knowledgeable on IPv6 and have less web server applications to upgrade.
Domain Name	Upgrading DNS server is unavoidable and it is important

System (DNS)	for organisations' server to interact with IPv6 requests. The cost of upgrading DNS is considering low compare to cost for upgrading operating systems and business support system.
Security Mechanism	Upgrade security mechanism to support IPv6 is one of the most challenging and time consuming event, because these security mechanism protects organisations' internal network from being attack by external network. Configuration of these security mechanisms takes a lot of time to perform testing to ensure the system work perfectly without failure. Upgrading cost can be range from low to high depending on organisations' network devices at different level.

4.4.1 Findings Associated with Operating System

The interviews indicate that most of the organisations from business organisations and NPO need to upgrade their operating system from Windows XP to Windows 7. This is because Windows XP by default does not support IPv6. Thus, they need to upgrade to Windows 7, which has native support for IPv6. Even though there are several patches that enable Windows XP to support IPv6, but they worried about the complexity of patches and configuration in future.

Another reason is due to Windows XP security issues, as they need to perform update weekly to fix security holes and patches regularly. Besides this, Windows XP is considering an old operating system and it's time to upgrade. When asking about when they will upgrade their operating system, participant from NPO mentioned within 6 months, as it is part of the organisation's planning to migrate by the end of the 2011.

4.4.2 Findings Associated with Business Support System

Other than operating system, another major software costs is upgrading organisations' business support system to work with IPv6. Most of the organisations business support system is matured and stable to handle daily business operation, but only few supports IPv6. In order to work with IPv6, either internal development team includes IPv6 support coding or outsourcing to external software developer house or request assistant from their software vendor. One of the participants mentioned business support system upgrade is not an easy job; it is time consuming to make it perfectly and at the same time to ensure that does not affect their company daily business operation and their clients. It is time consuming because of testing in lab environment and to ensure everything goes smooth before the new software integrate into their live environment. Therefore, the cost of upgrading business support system is high compared to other software cost.

4.4.3 Findings Associated with Web Servers

Aside of upgrading operating system and business support system, upgrade web servers' application also one of the crucial parts as the primary function of web servers is to deliver web pages on the request to clients. This means delivery of HTML documents and any additional content that may be included by a document such as images, style sheets and scripts. Upgrading web server application enables web server receives IPv6 connection requests from clients.

Upgrading web server application cost is varied and it is depends on number of servers operating in organisation and staff knowledge on IPv6. Cost would be low if their technical staffs' are knowledgeable on IPv6 and have less web server applications to upgrade.

4.4.4 Findings Associated with Domain Name System (DNS)

Furthermore, upgrading DNS server is unavoidable and it is one of the important elements when organisations plan to IPv6 migration. DNS is a protocol within the set of standards for how computers exchange data on the Internet and on many private networks, known as the TCP/IP protocol suits. Its job is to turn a user-friendly domain name like "google.com" into an Internet Protocol (IP) address like 74.125.113.99 that computers use to identify each other on the network.

The cost for upgrading DNS server is considering low compare to other software costs discussed above, as it doesn't require much time for testing compare to business support system. However, it is still depends on technical staffs' knowledge on IPv6 network configuration. If their staff is not knowledgeable in IPv6 configuration due to lack of related IPv6 training, then the cost might go higher in term of time and resources taken to complete the web server migration.

4.4.5 Findings Associated with Security Mechanism

Upgrade security mechanism software to work with IPv6 is very challenging and time consuming, according to one of the participants from business organisation. Security mechanism software such as firewall and intrusion detection system are very important to every organisation especially business organisations. As this security mechanism software protect internal network from attacks and block all suspicious incoming connection from external to internal network.

One of the participants mentioned upgrading this security software takes a lot of time to perform testing and to ensure the security mechanism's configuration able to detect and block both IPv4 and IPv6 addresses. This is because if one line of codes is misconfiguring, disaster may happens, which is either block all incoming connection included safe IP addresses or bypass all incoming connection included suspicious IP addresses.

The cost of security mechanism can be range from low to high depending on organisations' network devices at different level. The cost would be high if the organisation's network is huge and many incompatible devices. However, the cost would be low if organisation's network is small and not much incompatible devices need to upgrade. The next sub-section summarizes findings associated with software cost for business organisations and NPO.

Summary Finding Associated with Software Cost

Findings indicate that both business organisations and NPO have common software to upgrade such as upgrading operating system, upgrading web servers, upgrading DNS, and upgrading security mechanism. This software is basis for every organisation that plans to IPv6 migration. The different between both of them are business organisations need to upgrade their business support system to work with IPv6 and more concentrate in security mechanism software. Therefore, business organisations will have slightly higher software cost compare to NPO. However, software cost for IPv6 deployment may vary depends on organisations' network size, amount of incompatible applications needed to upgrade, security mechanism, and operating system licenses. The software cost would be high if there is a lot of software mentioned above is needed to upgrade and vice versa. The next section presents study findings associated with labour cost needed for business organisations and NPO.

4.5 Study Findings Associated with Labour Cost

This section examines interviews in term of labour cost needed for both business organisations and NPO to perform IPv6 migration. The interview analysis begins with findings for both business organisations and NPO. Then, this section concludes with a summary of study findings associated with labour costs.

Table 4.4: Study Findings Associated with Labour Cost

Study Findings Associated with Labour Cost	
Labour Costs	**Findings**
Training	Training cost is one of the most significant costs for organisation, because network administrator, network engineers, and other technical staffs require IPv6 knowledge to configure and setup IPv6 network equipment. There are several types of IPv6 training such as IPv6 deployment, IPv6 security, operating system and application, and software development. The appropriate level of training was provided to each member based on the functions they perform and their responsibilities.
Time	Time is considered as another labour resource, because time will be needed to run testing on new equipment and software, to install and configure new IPv6 hardware and transitional mechanism, and to maintain new IPv6 network. Extra time needed when the new IPv6 system is not work as expected or unexpected events occur during the IPv6 migration.

4.5.1 Findings Associated with Labour Cost

The interview indicates that training cost is one of the most significant costs for business organisations and NPO. Training cost is changeable due to the need of keeping the network administrators up to the standard and to keep the track of the upgraded hardware technology. So keeping such cost depends on existing employee knowledge with the IPv6 routers and servers. However once the employee be skilled enough then any extra improve in IPv6 software will not be a big contribution with the cost and will not need much training since the employee have some understanding of required networks and changes and how they might affect security or interoperability. If non-IT employees need to alter their activities based on IPv6 use, training will be necessary for them.

Participants from business organisation mentioned they had to pay particular attention to training because IPv6 is a new technology and most of engineers are not familiar with its specifics. The success of the IPv6 deployment depended on the ability of the operations staff to manage new protocol. The training efforts employed included academic-style courses, web-based classes, and hands-on experience. The appropriate level of training was provided to each member of the technical staff based on the functions they perform and their responsibilities.

While participant from NPO suggested, several training domains like IPv6 technology, which is the most common form of training available today focuses on describing the protocol operation through a side-by-side comparison with IPv4. Other training domains such as IPv6 deployment, IPv6 security, networking equipment, operating system and applications, software

development, and end users. Each of the training domain focuses on different area of IPv6, targeting for different level of staff, and targeting different level of business function. For example, security analyst staff is suitable for IPv6 security and IPv6 deployment training. On the other hand, software developers and system managers may suitable for operating system and application kind of IPv6 training.

Another labour resource such as time will be needed to run testing, to install and configure new IPv6 hardware, software, and transition mechanism (e.g. dual stack and tunnelling) and to maintain the new dual stack network. As the transition takes place, a more complex network will likely require additional network administrator costs. For example, in a dual stack network, two standards will have to be supported. Thus, it is either have a skilful and knowledgeable network administrator or have several network engineers work together. The following sub-section presents summary of findings associated with labour cost.

Summary Findings Associated with Labour Cost

Findings show that training costs are likely to be one of the most significant upgrade costs. The magnitude of these training costs will depend on existing IT staffs' familiarity and facility with IPv6. Most network staffs will need some understanding of the required network infrastructure changes and how they might affect security or interoperability. Labour cost would be high if existing

IT employees are not familiar to IPv6 and vice versa. The next section presents study findings associated with other cost for business organisations and NPO.

4.6 Study Findings Associated with Other Cost

This section examines interviews in term of other cost such as unexpected costs occurred during IPv6 migration. The interviews analysis begins with findings associated with unexpected cost for business organisations and NPO. Then, this section concludes with a summary of study findings associated with other costs.

Table 4.5: Study Findings Associated with Other Cost

Study Findings Associated with Unexpected Cost	
Unexpected Cost	**Findings**
Unexpected events	Unexpected cost often comes in unforeseen way such as employees performance diminishing caused by the sudden change of the new network system, hardware failure, software failure, etc. The unexpected costs can be range from low to high and it is depends on staff's capability to resolve the issues as soon as possible. The cost would be high, if technical team failed to fix the problem in short period of time.

4.6.1 Findings Associated with Other Cost

The interviews indicates that unexpected cost often comes in unforeseen way such as employees performance diminishing caused by the sudden change of the network system, hardware failure during integration, software failed to upgrade, systems doesn't work as expected, or when the system is affecting clients. Amount of unexpected costs depends on knowledge and skill of IPv6 migration team in the organisation to recover the system and minimise the unexpected costs. For example, if the team able to fix the problem in short period then the unexpected cost would be low. The cost is varying from small; medium to huge cost depends on cases.

In order to further examine unexpected costs occur during IPv6 migration, the interviews indicate significant unexpected costs occur when estimation goes wrong during IPv6 migration. Participants from business organisations mentioned that there would be two cases if estimation goes wrong during migration, which is either the system doesn't work at all or the system only partially working. System doesn't work at all is the least problem while system only partially working is the biggest problem.

When probes for reason, he mentioned when the system is doesn't working at all, prepare for downtime and ready for inspection to figure out the root cause. However, when the system is only partially working, which mean the system is live and their clients are using the system. The system only partially working could be due to misconfiguration on server's end-point or IPv6 network equipment. When the system is only partially working, certain functions might not available like transactional function is not available or mail

system is not functioning. Thus, unexpected cost comes in when the system is affecting their clients' side operation. Cost would be high and keep increasing if network administrator and technical staffs did not solve the problems in short period of time.

On the other hand, unexpected cost for NPO would be lesser compare to business organisations, as NPO is not dealing with commercial clients. Participant from NPO mentioned that if they overlook certain things, some services such as mail server might not function in the new IPv6 network if it does not support. He also added if estimation goes wrong during IPv6 migration, he believes that with dual stack implementation the problem can be resolved quickly as the network still able to work using IPv4 and should not have any big impact. The next sub-section summarizes findings associated with other cost for business organisations and NPO.

Summary Findings Associated with Other Cost

Findings indicate that most of the organisations prefer using dual stack approach for internal network and tunnelling approach for external network. Dual stack somehow could reduce unexpected cost during IPv6 migration, as dual stack allows both IPv4 and IPv6 addresses work together. If either one stack of IP addresses is having problem to connect to the other side, another stack of IP address will automatically changed and connect to the other side.

Besides this, another signification unexpected cost is when the new IPv6 network is affecting clients' side operation such as clients unable to proceed transaction due to certain functions are having problem in server's side, which could cause clients lose sales, lose productivity, resources, and customers. Regarding affecting clients due to unexpected events happen during IPv6 migration, NPO will not have much unexpected cost compare to business organisations, as NPO doesn't deal with business clients.

4.7 Study Findings Associated with Benefits of IPv6 After Migration

This section examines interviews in term of benefits of IPv6 after organisation successful migration such as cost reduction benefit, cost avoidance benefit, and performance benefits. The interviews analysis begins with findings associated with benefits of IPv6 after migration for business organisation and NPO. Then, this section concludes with a summary of study findings associated with benefits of IPv6 after migration.

Table 4.6: Study Findings Associated with Benefits of IPv6 After Migration

Study Findings Associated with Benefits of IPv6 After Migration	
Benefits of IPv6	**Findings**
None	Based on all participants, there is no tangible benefit after their organisation migrates to IPv6, because there is no different at the moment with or without implementing IPv6 in their network as long as their organisation's network run fine with IPv4.

4.7.1 Findings Associated with Benefits of IPv6 After Migration

The interviews indicate that based on all participants, there is no tangible benefit after their organisation migrates to IPv6 at the moment as long as their organisation's network run fine with IPv4. Participant from NPO mentioned that given that migration to IPv6 will eventually happen sooner or later, it is good to be ready early so that his organisation will not face any problems when IPv4 phased out one day and his organisation will not need to rush to implement it.

Participants from business organisation mentioned that there is no point wasting money, if his organisation runs fine with IPv4 now and given that many vendors still don't support IPv6 in scalable and high performance manner. He also added organisations that will gain benefits of IPv6 after migration would be service provider organisations such as Internet Service Provider (ISP) and social networking sites. This is because IPv6 will save the

trouble of doing NAT for these organisations. The next sub-section summarizes findings associated with benefits of IPv6 after migration for business organisation and NPO.

Summary Findings Associated with Benefits of IPv6 After Migration

Findings indicated that based on all participants, there is no tangible benefit if migrate to IPv6 now. This is because there isn't much different for their organisation as long as their organisation runs fine with IPv4 and there is no point wasting money since there is no tangible benefit after migration. Organisations such as service providers and social networking sites are gaining benefits of IPv6, as IPv6 will save the trouble of doing NAT in huge network.

4.8 Cost-Benefit Analysis Calculation

This section shows a general cost model that is needed for IPv6 migration. The calculation gives a basic formula of total costs needed based on Figure 4.1. In the early section, discussed several types of costs that are needed such as hardware, software, labour, and unexpected costs. Besides this, these costs are range from low to high depends on organisation network. In the next subsection, will provide a general cost model for each type of cost.

4.8.1 Hardware Cost Calculation

For the hardware cost, the cost needed is the total number unit of hardware needed, price of the hardware, and total man-day cost needed to install and configure the hardware.

The terms:

X = Total number unit of hardware

Y = Price of the hardware

Z = Total man-day cost (number of staff (man) x cost of 1 man-day)

General formula apply in hardware cost:

$\Sigma_{\text{Hardware cost}} = X_n \times Y_n \times Z_n$

PC / laptop cost, $\Sigma_{PC/laptop} = X_1 \times Y_1 \times Z_1$

Firewall cost, $\Sigma_{Firewall} = X_2 \times Y_2 \times Z_2$

Router cost, $\Sigma_{Router} = X_3 \times Y_3 \times Z_3$

Therefore, $\Sigma_{Hardware\ cost} = \Sigma_{PC/laptop} + \Sigma_{Firewall} + \Sigma_{Router}$

4.8.2 Software Cost Calculation

For the software cost, the calculation is not same with the hardware cost; software cost is based on total man and total man-day needed to complete the software upgrade, develop, testing, install, and configure.

The terms:

X = Total man needed

Y = Total man-day needed

Z = Total copies of Operating System (only apply in Operating System)

General formula apply in software cost:

$\Sigma_{Software\ cost} = X_n \times Y_n$

Web Servers, $\Sigma_{\text{Web Servers}} = X_1 \times Y_1$

DNS, $\Sigma_{\text{DNS}} = X_2 \times Y_2$

Business Support Software, $\Sigma_{\text{BSS}} = X_3 \times Y_3$

Operating System, $\Sigma_{\text{OS}} = X_4 \times Y_4 \times Z_1$

Security Mechanism, $\Sigma_{\text{Sec Mech.}} = X_5 \times Y_5$

Therefore, $\Sigma_{\text{Software cost}} = \Sigma_{\text{Web Servers}} + \Sigma_{\text{DNS}} + \Sigma_{\text{BSS}} + \Sigma_{\text{OS}} + \Sigma_{\text{Sec Mech.}}$

4.8.3 Labour Cost Calculation

For labour cost, the cost needed is total man that needs training, training cost, and total number of training needed. Total number of training needed is based on staff knowledge and job function. For example, network engineers may need more than 1 IPv6 training.

The terms:

X = Total man needed

Y = Training cost

Z = Total number of training

General formula apply in labour cost:

$\Sigma_{\text{Labour cost}} = X_1 \times Y_1 \times Z_1$

4.8.4 Other Cost

For other cost such as unexpected cost, to predict how much it cost is not easy. However, when an unexpected problem comes in, the fundamental problem solver is staffs need to solve the problem as soon as possible. Therefore, the cost needed is total man needed and total man-day needed.

The terms:

X = Total man needed

Y = Total man-day needed

General formula apply in other cost:

$\Sigma_{\text{Other cost}} = X_1 \times Y_1$

4.8.5 Overall IPv6 Migration Cost

In this section will sum up all costs from previous section (4.8.1 – 4.8.4) to show the general cost of IPv6 migration. The formula and total cost are based on research findings and might be inaccurate due to lack of certain criteria doesn't included in the formula. Therefore, the general cost shows below is solely estimation from the research findings.

General IPv6 migration cost:

$$\Sigma_{\text{IPv6 migration cost}} = \Sigma_{\text{Hardware cost}} + \Sigma_{\text{Software cost}} + \Sigma_{\text{Labour cost}} + \Sigma_{\text{Other cost}}$$

Conclusion

This chapter concludes with deployment cost on organisational migrate to IPv6. Organisations include business organisations and non-profit organisations (NPO). IPv6 deployment cost model was build based on data collected during interviews as Figure 4.1 and each type of deployment cost was discussed in details. IPv6 deployment cost model contain four components such as hardware costs, software costs, labour costs, and other unexpected costs.

First, hardware is an important element; it is mainly consists of network equipment and hosts. Network equipment such as IPv6 router is important as it forwarding IPv6 packets and it is main purpose is to allow hosts such as personal computers and notebooks to operate stable IPv6 networks. Firewall hardware, which is also the important security mechanism, and it is functioning as packet filtering. The cost of hardware is depending on the individual networks how big it is and the level of IPv6 capable by way of software upgrades.

Secondly, the software cost. Upgrading some software will be required to work with IPv6, and other software should keep upgrading from time to time. Software upgrades includes server software, which is needed to operate server computers, server, and desktop, operating systems such as Microsoft Windows, firewall software, and intrusion detection system. However, the main software costs that organisations related to their business support software, server software, and security mechanism software that they will need to revised software coding to adjust for IPv6. Software cost has a range of small cost such

as operating system and server application to a large cost such as business support software and security mechanism software.

Thirdly, the labour cost. Training cost is one of the most significant costs. Training cost is changeable due to the need of keeping the network administrator up to the standard and to keep the track of the upgraded hardware technology. So keeping such cost depends on existing employee knowledge with the IPv6 routers and servers. However, once the employee be skilled enough then any extra improve in IPv6 software will not be a big contribution with the cost and will not need much training since the employee have some understanding of required networks and changes and how they might affect security or interoperability.

Next, the other cost. This component is variable cost and it is subjected to the sudden accident occurred and affect the overall cost. For instance, system partially working and affect client's operation, cost that occurred when organisations want to solve some problems in interoperability and security intrusion if the network affected by intrusion. The situation is quite different and it is classified as other cost and its cost is varying from small cost, medium cost to large cost depends on the case.

Last, benefits of IPv6 after migration. Based on all participants, there is no tangible benefit if migrate to IPv6 now. This is because there isn't much different for their organisation as long as their organisation runs fine with IPv4 and there is no point wasting money since there is no tangible benefit after migration. Organisations such as service providers and social networking sites

are gaining benefits of IPv6, as IPv6 will save the trouble of doing NAT in huge network and offer more IP addresses.

Based on the study findings from above, a general cost-benefit analysis calculation for IPv6 migration is formulated. Due to the cost is solely based on study findings and it might lacks of certain criteria in the formula, therefore, the cost is estimated and formulated as

$$\Sigma_{\text{IPv6 migration cost}} = \Sigma_{\text{Hardware cost}} + \Sigma_{\text{Software cost}} + \Sigma_{\text{Labour cost}} + \Sigma_{\text{Other cost}}$$

The next chapter of the thesis presents conclusion and recommendation, which included conclusion for entire thesis, provides suggestions regarding on cost effectively way for organisations to migrate their network to IPv6, limitation of the thesis, and future research.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

This chapter concludes the thesis and provides a recommendation to organisation about using cost effectively way to migrate their network to new IPv6. This chapter has four sections. The first section concludes the study. The second section presents a cost effectively suggestion in IPv6 migration for organisations. The last section provides suggestions on future studies.

5.1 Conclusion

As Internet rapidly becomes the way to communicate, cyberspace is getting crowded. Millions of computers and networks effortlessly exchange vast amount of information using the Internet Protocol (IP). Hence, current IPv4 address space will run out very soon and it will affect everyone who wants to connect to the Internet. Therefore IPv6, which is next generation of IP is needed to allow everyone to continue communicate in the cyberspace.

Due to rapid growth of IPv4, organisations are starting to plan IPv6 migration in their networks. However, IPv6 adoption isn't being done because lack of business case and the unclear of cost migration. In this thesis, the author had conducted a research based on interview with several industry experts to

examine costs and benefits on organisational migrate to IPv6. Therefore, the objective of the research is to examine IPv6 deployment costs, potential IPv6 benefit, and other unexpected costs during migration, so that organisations can use these findings as a basis in future when they are ready to implement IPv6 in their network.

Findings from this study show that several deployment costs are needed such as hardware, software, and labour costs. Among these costs, labour costs is one of the most significant costs because migrating to IPv6 needs many training, installation, and testing on various network equipment, personal computers, and software to ensure all of them run fine with IPv6 in the system. On the other hand, there might have some unexpected costs occur during IPv6 migration like lose of employees' productivity due to system partially working or security intrusions. These unexpected costs are varying and depending on case. However, the findings also show that there are no tangible benefits for organisations that are planned to IPv6 migration now unless organisations like Internet Service Provider (ISP), hardware and software vendors, and web hosting service providers. Otherwise, there is no point wasting money, as long as organisation runs fine with IPv4.

5.2 Recommendation

This section provides a cost effective approach for organisations migrate to IPv6 based on study findings. Generally, implement IPv6 capability over a short time will be more expensive than making the transition as part of an organisation product refresh cycle. Rather than forcing a short-term shift, organisations would focus on replacing as much IPv4-only hardware and software as possible through normal product refresh cycles. Therefore, integrating IPv6 in product refresh cycle for cost reduction.

In addition, one of the most significant costs would be labour-related cost such as employees training, installation, and network testing, but the costs would be mitigated if the labour force were familiar with IPv4 or expert in IPv6. Besides this, cost would be lower in gradual migration scenario where much of the testing and problem resolution can be completed internally over an extended period or through shared initiations. Furthermore, relative programming skills of software engineers at a particular organisation could substantially affect upgrade costs. A company with more skilful programmers might have to hire one additional employee, while another might need three or four, during a transition period.

The suggested recommendation may not fit into all kind of organisations, it is a general suggestion based on study findings in this research study. A detail recommendation is needed and depends on types of organisations.

5.3 Suggestion for Future Studies

In future, the author plans to enhance this study by examines case studies on organisational migrates to IPv6 and provides a customised and more details of cost effective recommendation migrates to IPv6. By doing so, the author able to create a more accurate business case for future use.

Reference

Journal:

Arifin, A. H., Abdullah, D., Berhan, S. M., & Burdiarto, R. (2006). An Economical IPv4-to-IPv6 Transition Model: A Case study for University Network. *IJCSNS International Journal of Computer Science and Network Security, 6*. 170-178.

Caicedo, C. E., Joshi, J. B. D., & Tuladhar, S. R. (2009). IPv6 Security Challenges. *Computer, 42*(2), 36-42.

Cisco (2008). *Global IPv6 Strategies: From Business Analysis to Operating Planning*. Cisco Press.

Durdagi, E., & Buldu, A. (2010). IPV4/IPV6 security and threat comparisons. *Procedia Social and Behavioral Sciences 2*. 5285–5291.

Govil, J., Govil, J., Kaur, N., & Kaur, H. (2008). An Examination of IPv4 and IPv6 Networks: Constraints and Various Transition Mechanisms. *Southeastcon, IEEE*. 178-185

Hanumanthappa, J., & Dr. Manjaiah, D.H. (2009). IPv6 and IPv4 Threat reviews with Automatic Tunnelling and Configuration Tunnelling Configurations Tunnelling Considerations Transitional Model: A Case Study for University of Mysore Network. *International Journal of Computer Science and Information Security: Vol. 3*. Retrieved April 2, 2010, from http://sites.google.com/site/ijcsis/july-2009

Lai, Y., Jiang, G., Li, J., & Yang, Z. (2009). Design and Implementation of Distributed Firewall System for IPv6. *2009 International Conference on Communication Software and Networks.* 428-432.

Mat Taib, A. H., & Budiarto, R. (2007). Security Mechanism for the IPv4 to IPv6 Transition. *The 5th Student Conference on Research and Development (SCOReD).*

Mavetera, N., & Kroeze, J. H. (2009). "Practical Considerations in Grounded Theory Research.". *Sprouts: Working Papers on Information Systems,* 9(32).

http://sprouts.aisnet.org/9-32

Waddington, D. G., & Chang F. (2002). Realizing the Transition to IPv6. *IEEE Communications Magazine*, 138-148.

Xiong Wei, Zhang Jiang-wei, & Zhang Guo-dong. (2009). Application Research on IPv4/IPv6 Dual Stack Technology. *2009 International Con ference on Signal Processing Systems.* 826-828.

Zagar, D., & Grgic, K. (2006). IPv6 Security threats and possible solutions. *World Automation Congress. IEEE.*

Zagar, D., Grgic, K., & Rimac-Drlje, S. (2007). Security aspects in IPv6 networks – implementation and testing. *Computers and Electrical Engineering 33*. 425–437.

Book Chapter:

Boeije, H. (2010). *Analysis in Qualitative Research.* Singapore: SAGE.

Brown, S. (2002). *Configuring IPv6 for Cisco IOS*. Rockland, MA: Syngress.

Marshall, C., & Rossman, G. B. (2006). *Designing Qualitative Research* (4th ed.) USA: Sage Publication, Inc.

Ritchie, J., & Lewis, J. (2003). *Qualitative Research Practice: A Guide for Social Science Students and Researchers.* USA: Sage Publication, Inc.

Webpages:

Aburas, A. A., & Mahmod, Z. S. (2008). IPv4-over-IPv6 Tunnelling. Retrieved July 4, 2010, from http://www.arabrise.org/articles/A040102A.pdf

Aoun, C., & Davies, E. (2007). Reasons to Move the Network Address Translator – Protocol Translator (NAT-PT) to Historic Status. Retrieved April 1, 2010, from ftp://ftp.rfc-editor.org/in-notes/rfc4966.txt

Bakke, M., Cisco, Hafner, J., Huffered, J., Voruganti, K., IBM, Krueger, M., Hewlett-Packard. (2004). Internet Small Computer System Interface (iSCSI) Naming and Discovery. Retrieved April 20, 2012, from http://www.ietf.org/rfc/rfc3721.txt

BGP Report. (2012). IPv4 APNIC Allocation Report. Retrieved April 18, 2012, from http://bgp.potaroo.net/ipv4-stats/allocated-apnic.html

Cisco (2010). IPv6-Cisco Systems. Retrieved April 3, 2010, from http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

Deering, S., & Hinde, R. (1998). Internet Protocol, Version 6 (IPv6) Specification. Retrieved March 1, 2010, from http://www.ietf.org/rfc/rfc2460.txt

Deering, S., & Hinde, R. (2003). Internet Protocol Version 6 (IPv6) Addressing Architecture. Retrieved April 3, 2010, from http://www.ietf.org/rfc/rfc3513.txt

Department of Veterans Affairs. (2006). A discussion of IPv6 Transition Mechanisms. Retrieved October 20, 2010, form http://www.docstoc.com/docs/6650928/IPv6-Migration-Strategy-Document-(Outline)

Hinden, R., Nokia, Deering, S., Cisco Systems. (2006). IP Version 6 Addressing Architecture. Retrieved April 20, 2012, from http://tools.ietf.org/html/rfc4291

Hogg, S. (2007). Internet Protocol version 6: The Next Generation Protocol. Retrieved April 22, 2010, from http://www.gtri.com/docs/IPv6%20-%20The%20Next%20Generation%20Protocol%20v1-1.pdf

Huston, G. (2012). IPv4 Address Report. Retrieved April 17, 2012, from http://www.potaroo.net/tools/ipv4/

IPv6 Forum. (2012). IPv6 Enabled Program. Retrieved April 17, 2012, from http://www.ipv6forum.com/ipv6_enabled/ipv6_enable.php

Johnson, D., & Perkins, C. (2004). Mobility Support in IPv6. Retrieved April 3, 2010, from http://www.ietf.org/rfc/rfc3775.txt

JPNIC. (2007). Study Report on the IPv4 Address Space Exhaustion Issue (Phase I). Retrieved March 30, 2010, from http://www.nic.ad.jp/en/ip/ipv4pool/ipv4exh-report-071207-en.pdf

Juniper Networks & Microsoft Corporation. (2007). Enabling the Next Generation of Networking with End-to-End IPV6. Retrieved March 24, 2010, from http://download.microsoft.com/download/7/d/9/7d9f3a8f-328d-4a42-a5f3-62a1a1e845b9/EndToEndIPv6MSJuniper.pdf

Juniper Networks, Inc (2009). Deploying IPv6: Issues and Strategies. Retrieved June 27, 2010, from http://www.juniper.net/us/en/local/pdf/resource-guides/7100085-en.pdf

KanREN. (2009). Case Study: KanREN Community Experiences Early IPv6 Adoption. Retrieved March 23, 2010, from http://ipv6.internet2.edu/200904-CS-KAN-IPv6.pdf

Kent, S., & Atkinson, R. (1998). Security Architecture for the Internet Protocol. Retrieved April 3, 2010, from http://www.ietf.org/rfc/rfc2401.txt

Marsan, C. D. (2009) Google: IPv6 is easy, not expensive. Retrieved April 1, 2010, from http://www.networkworld.com/news/2009/032509-google-ipv6-easy.html

Microsoft (2008). IPv6 for Microsoft Windows: Frequently Asked Questions. Retrieved August 3, 2010, from http://technet.microsoft.com/en-us/network/cc987595.aspx

Nordmark, E. (2000). Stateless IP/ICMP Translation Algorithm (SIIT). Retreived April 21, 2010, from http://www.ietf.org/rfc/rfc2765.txt

Nordmark, E. (2005). Basic Transition Mechanism for IPv6 Hosts and Routers. Retrieved April 21, 2010, from http://www.ietf.org/rfc/rfc4213.txt

Perset, K. (2008). Internet Address Space: Economic Considerations in the Management of IPv4 and in the Deployment of IPv6. Retrieved August 3, 2010, from http://www.oecd.org/dataoecd/7/1/40605942.pdf

Roberts, P. (2009). Internet Society Organization Member IPv6 Study. Retrieved March 23, 2010, from http://www.isoc.org/pubs/2009-IPv6-OrgMember-Report.pdf

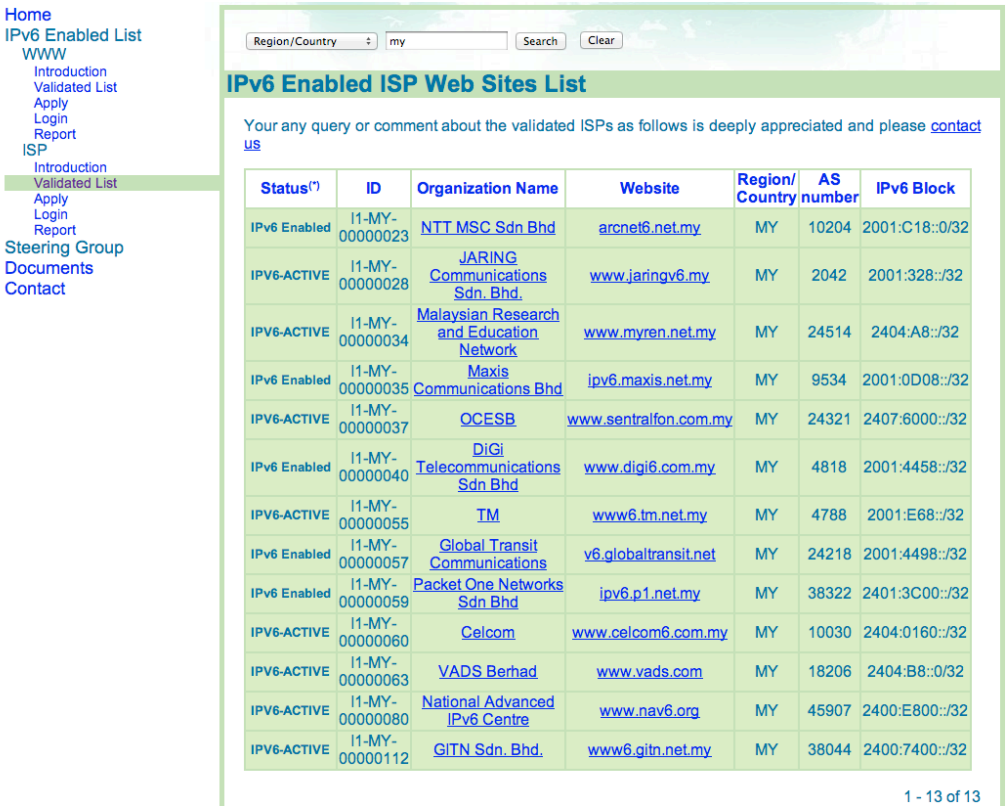
Robinson, N., Cesar Ramos, P.E., & Jara, J. L. (2007). An Enterprise Perspective on IPv6 Transition Mechanisms. Retrieved April 22, 2010, from http://www.esei.com/images/ESEI%20IPV6%20-%20White%20Paper.pdf

Rooney, T. (2007). IPv4-to-IPv6 Transition Strategies. Retrieved July 4, 2010, from http://www.networkworld.com/whitepapers/nww/pdf/bt_wp_IPv6_Transition_Strategies.pdf

Thomson, S., & Narten, T. (2007). IPv6 Stateless Address Auto-configuration. Retrieved April 3, 2010, from http://www.ietf.org/rfc/rfc4862.txt

Appendix A

IPv6 Enabled ISP Web Sites List for Malaysia



Home
IPv6 Enabled List
WWW
Introduction
Validated List
Apply
Login
Report
ISP
Introduction
Validated List
Apply
Login
Report
Steering Group
Documents
Contact

Region/Country | my | Search | Clear

IPv6 Enabled ISP Web Sites List

Your any query or comment about the validated ISPs as follows is deeply appreciated and please contact us

Status(*)	ID	Organization Name	Website	Region/ Country	AS number	IPv6 Block
IPv6 Enabled	I1-MY-00000023	NTT MSC Sdn Bhd	arcnet6.net.my	MY	10204	2001:C18::0/32
IPV6-ACTIVE	I1-MY-00000028	JARING Communications Sdn. Bhd.	www.jaringv6.my	MY	2042	2001:328::/32
IPV6-ACTIVE	I1-MY-00000034	Malaysian Research and Education Network	www.myren.net.my	MY	24514	2404:A8::/32
IPv6 Enabled	I1-MY-00000035	Maxis Communications Bhd	ipv6.maxis.net.my	MY	9534	2001:0D08::/32
IPV6-ACTIVE	I1-MY-00000037	OCESB	www.sentralfon.com.my	MY	24321	2407:6000::/32
IPv6 Enabled	I1-MY-00000040	DiGi Telecommunications Sdn Bhd	www.digi6.com.my	MY	4818	2001:4458::/32
IPV6-ACTIVE	I1-MY-00000055	TM	www6.tm.net.my	MY	4788	2001:E68::/32
IPv6 Enabled	I1-MY-00000057	Global Transit Communications	v6.globaltransit.net	MY	24218	2001:4498::/32
IPv6 Enabled	I1-MY-00000059	Packet One Networks Sdn Bhd	ipv6.p1.net.my	MY	38322	2401:3C00::/32
IPV6-ACTIVE	I1-MY-00000060	Celcom	www.celcom6.com.my	MY	10030	2404:0160::/32
IPV6-ACTIVE	I1-MY-00000063	VADS Berhad	www.vads.com	MY	18206	2404:B8::0/32
IPV6-ACTIVE	I1-MY-00000080	National Advanced IPv6 Centre	www.nav6.org	MY	45907	2400:E800::/32
IPV6-ACTIVE	I1-MY-00000112	GITN Sdn. Bhd.	www6.gitn.net.my	MY	38044	2400:7400::/32

1 - 13 of 13

Source: http://www.ipv6forum.com/ipv6_enabled/isp/approval_list.php?type=loc&content=my

Appendix B

IPv6 Enabled WWW Web Sites List for Malaysia

IPv6 Enabled Program

------New Service

Home
IPv6 Enabled List
WWW
Introduction
Validated List
Apply
Login
Report
ISP
Introduction
Validated List
Apply
Login
Report
Steering Group
Documents
Contact

Region/Country | my | Search | Clear

IPv6 Enabled WWW Web Sites List

Your any query or comment about the validated web sites as follows is deeply appreciated and please contact us

Status(*)	ID	Organization Name	URL	Region/ Country	Tags	Approved Time
IPv6 Enabled	W1-MY-00000255	NTT MSC Sdn Bhd	arcnet6.net.my	MY	Enterprise Site	2009-07-03 06:57:59
IPv6 Enabled	W1-MY-00000347	TM	www6.tm.net.my	MY	Enterprise Site	2009-08-17 08:33:56
IPv6 Enabled	W1-MY-00000383	MLabs Systems Bhd	www.mlabs.com	MY	Enterprise Site	2009-09-17 11:25:34
IPv6 Enabled	W1-MY-00000691	My6 Initiative Berhad	www.my6.my	MY	Enterprise Site	2012-02-23 16:45:14
IPv6 Enabled	W1-MY-00002345	Orbitage	www.orbitage.com	MY	Enterprise Site	2011-11-24 11:44:35
IPv6 Enabled	W1-MY-00000313	.my DOMAIN REGISTRY	rnd.domainregistry.my	MY	Government Site	2009-08-11 05:45:12
IPv6 Enabled	W1-MY-00000377	National Advanced IPv6 Centre	www.nav6.org	MY	Government Site	2009-09-10 11:27:23
IPv6 Enabled	W1-MY-00001080	Jabatan Perkhidmatan Awam	www6.jpa.my	MY	Government Site	2010-11-02 03:20:31
IPv6 Enabled	W1-MY-00001241	Institut Tadbiran Awam Negara	intanv6.intan.my	MY	Government Site	2010-12-22 08:21:10
IPv6 Enabled	W1-MY-00002087	BAHAGIAN PASCA PERKHIDMATAN JPA	www6.jpapencen.gov.my	MY	Government Site	2011-05-31 06:12:56
IPv6 Enabled	W1-MY-00002149	Jabatan Perkhidmatan Awam	www.jpa.gov.my	MY	Government Site	2011-06-07 09:17:05
IPv6 Enabled	W1-MY-00002732	InterNetworks Research Laboratory	www.internetworks.my	MY	Government Site	2012-02-16 04:44:15

Source:
http://www.ipv6forum.com/ipv6_enabled/approval_list.php?type=loc&content=my&start=0&order=asc&orderby=tags

IPv6 Enabled	W1-MY-00000357	OCESB	www6.sentralfon.com.my	MY	IT Site	2009-08-25 11:05:04
SERVICE-IN	W1-MY-00000359	OCESB	www.sentralfon.com.my	MY	IT Site	2009-08-25 11:04:18
IPv6 Enabled	W1-MY-00000505	Packet One Networks Sdn Bhd	ipv6.p1.net.my	MY	IT Site	2009-12-23 08:50:52
IPv6 Enabled	W1-MY-00000625	U Mobile	ipv6.u.net.my	MY	IT Site	2010-03-11 06:15:21
SERVICE-IN	W1-MY-00000343	Malaysian Research and Education Network	www.myren.net.my	MY	Others	2009-08-27 10:37:21
IPv6 Enabled	W1-MY-00000367	Maxis Communications Bhd	ipv6.maxis.net.my	MY	Others	2009-12-22 10:15:35
IPv6 Enabled	W1-MY-00000498	TIME dotCom Berhad	ipv6.time.net.my	MY	Others	2009-12-10 04:06:39
IPv6 Enabled	W1-MY-00000499	global transit communications	v6.globaltransit.net	MY	Others	2009-12-10 07:42:37
IPv6 Enabled	W1-MY-00002150	DiGi Telecommunications Sdn Bhd	www.digi6.com.my	MY	Others	2011-06-06 18:12:57
IPv6 Enabled	W1-MY-00002501	JARING Communications Sdn Bhd	www.jaringv6.my	MY	Others	2011-09-29 05:52:03
IPv6 Enabled	W1-MY-00000250	5 Linux Monsters	www.5lm.net	MY	Personal Site	2009-07-02 08:56:36
IPv6 Enabled	W1-MY-00000278	SimonExploreIT	www.simonexploreit.com	MY	Personal Site	2009-07-10 10:43:35
IPv6 Enabled	W1-MY-00000420	V6.MY	www.v6.my	MY	Personal Site	2009-10-13 05:42:45
IPv6 Enabled	W1-MY-00000622	personal	barricade.mooo.com	MY	Personal Site	2010-03-10 03:56:50
IPv6 Enabled	W1-MY-00001052	personal	bsd.rnh.com.my	MY	Personal Site	2010-10-19 13:52:32
SERVICE-IN	W1-MY-00001406	Relief Goddess Office	imouto.my	MY	Personal Site	2011-02-08 14:31:18
IPv6 Enabled	W1-MY-00001410	Msaifuddin	ipv6.msaifuddin.com	MY	Personal Site	2011-02-08 12:11:44
IPv6 Enabled	W1-MY-00002341	husaini.name.my	husaini.name.my	MY	Personal Site	2011-07-09 05:33:55

1 - 30 of 32 >

Source:
http://www.ipv6forum.com/ipv6_enabled/approval_list.php?type=loc&content=my&start=0&order=asc&orderby=tags

Appendix C

IPv6 Enabled ISP Web Site List for World Wide

Source: http://www.ipv6forum.com/ipv6_enabled/isp/approval_list.php

LUNS Ltd.	www.luns.net.uk	UK	30847	2A01:8900::/3
JT	www.as8681.net	UK	8681	2A02:C28::/32
NetAssist LLC	www.netassist.ua	UA	29632	2A01:D0::/32
Chunghwa Telecom HiNet	www.ipv6.hinet.net	TW	17419	2001:B000::/2
fareastone	ipv6.seed.net.tw	TW	4780	2001:0CD8::/32, 2001:
So-net Entertainment	www.ipv6.so-net.net.tw	TW	18182	2404:0080::/28
ThaiSarn	www.thaisarn.net.th	TH	3836	2001:0F00::/3
Nettree	www.nettree.co.th	TH	45456	2404:8800::/32
CAT TELECOM PUBLIC COMPANY LIMITED	www.cattelecom.com	TH	4651,4652,9931	2001:0C38::/3
UniNet	www.uni.net.th	TH	4621	2001:3C8::/32
TOT Public Company Limited	www.tot.co.th	TH	9737	2001:EC0::/32
Triple T Broadband Public Company Limited	speedtest.3bb.co.th	TH	45758	2403:6200::/32
W802 D.o.o.	www.w802.net	SR	47479	2A00:8100::/3
LGA Telecom	v6.lgatelecom.net	SG	10024	2406:A400::/3
Periquito AB	www.prq.se	SE	33837	2A00:16B0::/3
SpaceDump IT AB	www.spacedump.se	SE	30880	2A01:298::/32
Sahara Net	www.sahara.com	SA	41176	2A02:D70::/32

1 - 30 of 140 > >>

Source: http://www.ipv6forum.com/ipv6_enabled/isp/approval_list.php

Appendix D

IPv6 Enabled WWW Web Sites List for World Wide

Source: http://www.ipv6forum.com/ipv6_enabled/approval_list.php

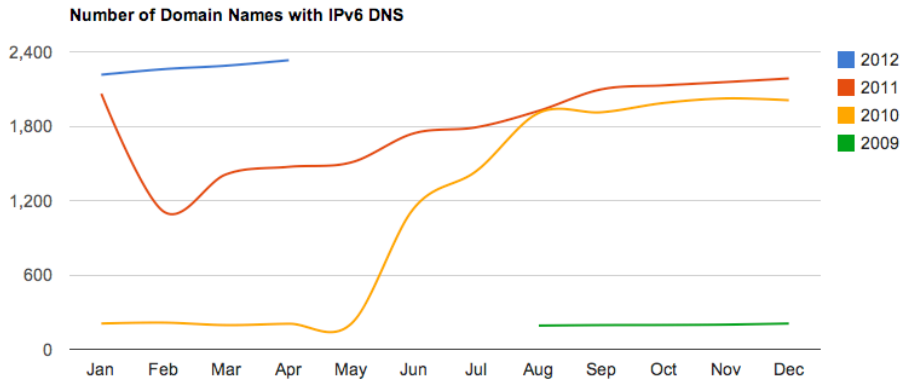
IPv6 Enabled	W1-DE-00000015	WindfluechterNet	www.windfluechter.net	DE	IT Site	2009-05-18 17:14:20
IPv6 Enabled	W1-DE-00000016	WindfluechterNet	blog.windfluechter.net	DE	Personal Site	2009-05-18 09:02:02
IPv6 Enabled	W1-NO-00000017	Mork Namnelag	www.mork.no	NO	Not-for-profit Cooperative Site	2009-05-15 20:10:46
IPv6 Enabled	W1-NO-00000018	Asheim	ashe.im	NO	Personal Site	2009-05-15 21:07:15
IPv6 Enabled	W1-DE-00000023	private	www.kluenter.de	DE	Personal Site	2009-05-18 16:12:11
SERVICE-IN	W1-DE-00000024	The MirOS Project	www.mirbsd.org	DE	IT Site	2009-06-09 21:21:13
IPv6 Enabled	W1-DE-00000026	Das Labor e.v.	www.das-labor.org	DE	Others	2009-05-18 15:00:00
IPv6 Enabled	W1-SE-00000027	LM Jogb	www.jogback.se	SE	Personal Site	2009-06-09 21:21:00
SERVICE-OUT	W1-GB-00000032	Wyrd Dreams Internet Solutions	www.wyrddreams.com	GB	Enterprise Site	2009-05-20 18:29:11
IPv6 Enabled	W1-VE-00000033	ONUVA	www.onuva.com	VE	Enterprise Site	2009-06-17 17:13:08
SERVICE-IN	W1-DE-00000037	Jan Dittberner IT-Consulting & Solutions	www.gnuviech-server.de	DE	IT Site	2009-05-24 17:14:59
SERVICE-IN	W1-DE-00000039	Oliver Niesner	devil_ipv6.strangled.net	DE	Personal Site	2009-05-28 15:53:48
SERVICE-IN	W1-AU-00000040	Shaun Ewing	se.id.au	AU	Personal Site	2009-06-08 03:09:41
IPv6 Enabled	W1-CH-00000041	Sunny Connection AG	www.sunny.ch	CH	IT Site	2009-06-30 03:18:13
IPv6 Enabled	W1-CH-00000042	Internet Society	www.isoc.org	CH	Not-for-profit Cooperative Site	2009-06-08 15:36:06
SERVICE-IN	W1-DE-00000043	Hasso-Plattner-Institut	www.dcl.hpi.uni-potsdam.de	DE	Education Site	2009-06-08 13:06:15
IPv6 Enabled	W1-SI-00000044	Zavod go6	go6.si	SI	Not-for-profit Cooperative Site	2009-06-08 15:54:21

1 - 30 of 1482 > >>

Source: http://www.ipv6forum.com/ipv6_enabled/approval_list.php

Appendix E

Number of Domain Name with IPv6 DNS in Malaysia



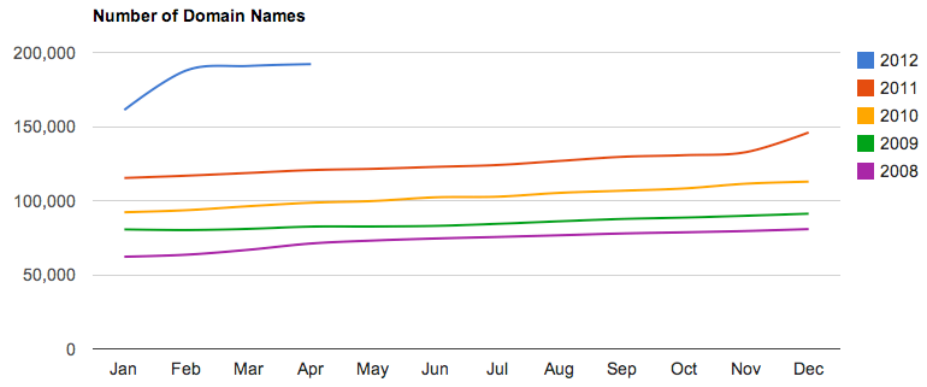
Number of Domain Names with IPv6 DNS:
** As of 17 Apr 2012

Month*		.my	.com.my	.net.my	.org.my	.gov.my	.edu.my	.mil.my	.name.my	Total
2012	Apr **	712	1,212	61	63	260	18	1	5	2,332
	Mar	698	1,184	60	64	258	18	1	5	2,288
	Feb	685	1,165	61	62	261	19	1	6	2,260
	Jan	675	1,137	60	61	257	18	1	6	2,215
2011	Dec	655	1,133	61	58	255	16	1	6	2,185
	Nov	640	1,132	60	52	249	17	1	5	2,156
	Oct	625	1,123	58	53	248	16	1	5	2,129
	Sep	603	1,113	58	57	245	16	1	4	2,097
	Aug	455	1,093	56	56	243	16	1	4	1,924
	Jul	431	997	55	53	236	13	1	5	1,791
	Jun	418	970	52	52	231	13	1	5	1,742

Source: http://www.domainregistry.my/en/statistics.php

Appendix F

Number of Domain Name in Malaysia



Number of Domain Names:
** As of 17 Apr 2012

Month*		.my	.com.my	.net.my	.org.my	.gov.my	.edu.my	.mil.my	.name.my	Total
2012	Apr **	80,959	102,096	2,789	2,724	1,111	2,237	18	165	192,099
	Mar	80,649	101,204	2,774	2,710	1,109	2,239	18	166	190,869
	Feb	79,390	99,611	2,749	2,646	1,103	2,205	18	165	187,887
	Jan	53,238	98,863	2,762	2,632	1,092	2,175	18	402	161,182
2011	Dec	39,050	97,921	2,764	2,613	1,087	2,137	17	401	145,990
	Nov	28,510	95,334	2,713	2,601	1,079	2,120	17	401	132,775
	Oct	27,701	94,020	2,697	2,600	1,112	2,100	16	404	130,650
	Sep	27,083	93,557	2,712	2,593	1,107	2,076	16	413	129,557
	Aug	25,849	92,045	2,692	2,581	1,103	2,091	15	412	126,788
	Jul	25,186	90,258	2,665	2,528	1,099	1,863	14	414	124,027
	Jun	24,978	89,341	2,645	2,492	1,090	1,787	14	424	122,771

Source: http://www.domainregistry.my/en/statistics.php

Appendix G

IPv4 APNIC Allocation Report

IPv4 APNIC Allocation Report

This report was last updated:

08:01 18 Apr 2012 [GMT+10]

Allocation Report for APNIC managed /8 IPv4 Address Blocks

	(/32 addresses)							
/8	%Allocated	RIR	Date	RIR	Allocated	Advertised	%Advertised	%Advertised
	Rsvd	Rsvd	Pool		Allocated			
8-Jan	100.00%	apnic	20100119	0	16777216	15260160	90.96%	90.96%
14/8	99.85%	apnic	20100410	24576	16752640	12080384	72.00%	72.11%
27/8	99.76%	apnic	20100119	39936	16737280	15185152	90.51%	90.73%
36/8	99.22%	apnic	20101018	131072	16646144	7015680	41.82%	42.15%
39/8	100.00%	apnic	20110201	0	16777216	5678080	33.84%	33.84%
42/8	100.00%	apnic	20101018	0	16777216	6240256	37.19%	37.19%
43/8	89.84%	apnic	19890221	1703936	15073280	393216	2.34%	2.61%
49/8	99.99%	apnic	20100806	1024	16776192	13458944	80.22%	80.23%
58/8	99.90%	apnic	20040428	16384	16760832	16249344	96.85%	96.95%
59/8	99.48%	apnic	20040428	88064	16689152	12269824	73.13%	73.52%
60/8	100.00%	apnic	20030401	0	16777216	16348160	97.44%	97.44%
61/8	100.00%	apnic	19970401	0	16777216	16238848	96.79%	96.79%
101/8	100.00%	apnic	20100806	0	16777216	12176640	72.58%	72.58%
103/8	6.39%	apnic	20110204	15704576	1072640	641408	3.82%	59.80%
106/8	99.95%	apnic	20110201	8192	16769024	7599360	45.30%	45.32%
110/8	99.95%	apnic	20081112	8192	16769024	16073216	95.80%	95.85%
111/8	100.00%	apnic	20081112	0	16777216	16109312	96.02%	96.02%
112/8	99.99%	apnic	20080528	1024	16776192	16296192	97.13%	97.14%
113/8	100.00%	apnic	20080528	0	16777216	15349760	91.49%	91.49%
114/8	99.99%	apnic	20071030	2048	16775168	14105856	84.08%	84.09%
115/8	99.95%	apnic	20071030	8192	16769024	14872064	88.64%	88.69%
116/8	99.57%	apnic	20070117	71680	16705536	11126016	66.32%	66.60%
117/8	99.96%	apnic	20070117	6144	16771072	15065600	89.80%	89.83%
118/8	99.94%	apnic	20070117	10240	16766976	15056128	89.74%	89.80%
119/8	99.99%	apnic	20070117	2048	16775168	15288320	91.13%	91.14%
120/8	100.00%	apnic	20070117	0	16777216	13862144	82.62%	82.62%

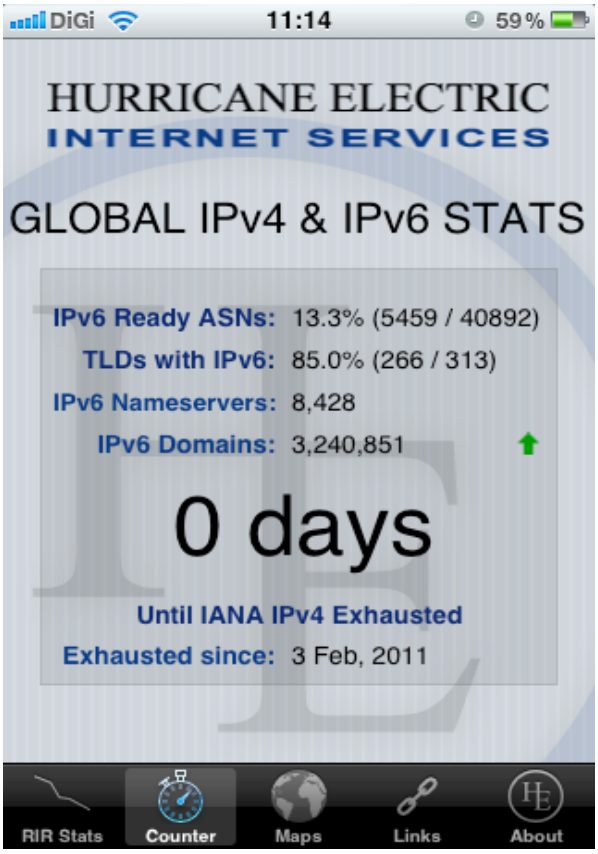
Source: http://bgp.potaroo.net/ipv4-stats/allocated-apnic.html

121/8	99.88%	apnic	20060107	20480	16756736	16300288	97.16%	97.28%
122/8	99.99%	apnic	20060107	2048	16775168	15555072	92.72%	92.73%
123/8	99.99%	apnic	20060107	2048	16775168	15374592	91.64%	91.65%
124/8	99.98%	apnic	20050128	3840	16773376	15559488	92.74%	92.76%
125/8	100.00%	apnic	20050128	0	16777216	16512256	98.42%	98.42%
126/8	100.00%	apnic	20050128	0	16777216	16777216	100.00%	100.00%
133/8	100.00%	apnic	19890405	0	16777216	9829376	58.59%	58.59%
175/8	99.93%	apnic	20090804	11264	16765952	15949568	95.07%	95.13%
180/8	99.93%	apnic	20090430	11264	16765952	16028160	95.54%	95.60%
182/8	99.93%	apnic	20090804	11264	16765952	14899968	88.81%	88.87%
183/8	99.99%	apnic	20090430	2048	16775168	16538880	98.58%	98.59%
202/8	98.92%	apnic	19930101	180992	16596224	13510784	80.53%	81.41%
203/8	99.66%	apnic	19930101	57088	16719872	14016320	83.54%	83.83%
210/8	99.69%	apnic	19960601	51200	16726016	15623168	93.12%	93.41%
211/8	100.00%	apnic	19990601	0	16777216	16016384	95.47%	95.47%
218/8	99.98%	apnic	20001201	2560	16774656	16380160	97.63%	97.65%
219/8	99.98%	apnic	20010901	4096	16773120	16541440	98.59%	98.62%
220/8	99.80%	apnic	20011201	33792	16743424	15404544	91.82%	92.00%
221/8	100.00%	apnic	20020701	0	16777216	16644096	99.21%	99.21%
222/8	100.00%	apnic	20030201	0	16777216	16605440	98.98%	98.98%
223/8	99.98%	apnic	20100410	4096	16773120	13505792	80.50%	80.52%
47 /8s	97.69%		20120418	1.09 /8	45.91 /8	38.36 /8	81.62%	83.55%
Totals: 47.00 /8s Assigned, 45.91 /8s Allocated, 1.09 /8s in RIR Pool, 38.36 /8s Advertised								

Source: http://bgp.potaroo.net/ipv4-stats/allocated-apnic.html

Appendix H

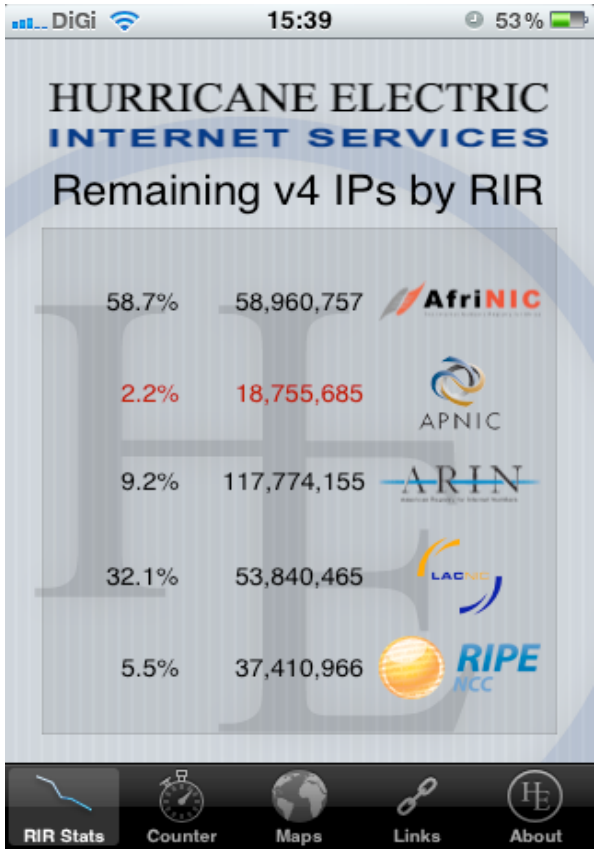
IANA Unallocated Address Pool Exhaustion Date



Source: Screen shot taken on March 31, 2012 from author's iPhone.

Appendix I

Remaining IPv4 addresses by RIR



Source: Screen shot taken on March 31, 2012 from author's iPhone.