IPv6 MIGRATION FRAMEWORK FOR GOVERNMENT AGENCIES IN MALAYSIA

by

AWINDER KAUR A/P MOHINDER SINGH

Thesis submitted in fulfillment of the requirements
for the degree of
Masters of Computer Science

July 2009

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to all those who have made it possible for me to complete my thesis. First and foremost, I would like to thank my supervisors Pn Rosnah Idrus and Prof Sureswaran Ramadass for their personal guidance and encouragement throughout my research. They have always been there when I needed assistance in my thesis as well as stimulating suggestions for my research. Most importantly, they believed in me and consistently motivated me all through my journey in the completion of my thesis. I would also like to express my appreciation to Assoc Prof Dr Rahmat Budiarto for his ideas contributions, valuable advice and friendly help. I would like to thank my close friends and colleagues who have encouraged me a lot. I would like to acknowledge my colleague Adil Hidayat who has shared his resources pertaining to IPv6 and gave a helping hand whenever I required assistance. I am also extremely grateful to my family on their constant encouragement and love that has kept me motivated and never give up. Finally, I would like to thank God whom I turn to for the courage, strength, persistence, enthusiasm and determination in writing my thesis.

TABLE OF CONTENTS

CHAPTER 1 – INTRODUCTION

CHAPTER 2 – LITERATURE STUDIES

CHAPTER 3 – RESEARCH METHODOLOGY

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MAMPU	Malaysian Administrative Modernization and Management Planning Unit
MEWC	Ministry of Energy, Water and Communications
NAT	Network Address Translation

RANGKA KERJA MIGRASI IPv6 UNTUK AGENSI-AGENSI KERAJAAN DI MALAYSIA

ABSTRAK

Malaysia adalah sebahagian daripada negara-negara dunia yang berusaha untuk berhijrah ke protokol Internet Versi 6 (IPv6) disebabkan oleh alamat IPv4 yang hampir lupus dan keterbatasan protokol Internet Versi 4 (IPv4). Salah satu daripada usaha yang diperlukan adalah untuk membolehkan pelaksanaan IPv6 di agensi-agensi kerajaan Malaysia di mana agensi-agensi tersebut akan menerajui migrasi IPv6 di Malaysia. Pembangunan rangka kerja migrasi IPv6 akan dapat membantu agensi-agensi kerajaan mengenalpastikan komponen-komponen serta langkah-langkah proses migrasi IPv6 yang perlu diambil. Penyelidikan dijalankan tentang migrasi IPv6 dengan objektif untuk mencipta rangka kerja bagi agensi-agensi kerajaan di Malaysia. Data diperolehi daripada kakitangan agensi-agensi kerajaan di Malaysia melalui soal selidik dan temubual. Dapatan dari penyelidikan tersebut telah digabung dan digolongkan ke dalam lima kategori iaitu kesedaran IPv6, kemajuan, cabaran, keperluan implementasi dan cadangan pelaksanaan IPv6. Penemuan kaji selidik digabungkan dengan rangka kerja awal migrasi IPv6 untuk membentuk rangka kerja migrasi IPv6 bagi agensi-agensi kerajaan di Malaysia yang mengandungi komponen-komponen penting untuk migrasi IPv6 yang perlu dipertimbangkan. Teknik "triangulation" yang mengabungkan dua kaedah kajian iaitu soal selidik dan temubual telah digunakan untuk meningkatkan kredibiliti dan kesahan kajian ini. Tesis ini mengemukakan rangka kerja yang boleh digunakan sebagai panduan bagi agensi-agensi kerajaan di dalam proses migrasi IPv6, terutamanya diperingkat perancangan. Rangka kerja ini dibentuk berdasarkan sumber-sumber maklumat IPv6 yang disatukan dengan keperluan, permintaan dan cabaran-cabaran yang dihadapi oleh agensi-agensi kerajaan Malaysia. Pelan migrasi IPv6 ini juga mengandungi komponen-komponen migrasi yang menunjukkan aspek migrasi IPv6 yang berlainan dan penting untuk perancangan IPv6 agensi-agensi kerajaan

IPv6 MIGRATION FRAMEWORK FOR GOVERNMENT AGENCIES IN MALAYSIA

ABSTRACT

Malaysia is involved in the worldwide effort to migrate to IPv6 due to the global IPv4 address depletion and other IPv4 limitations as well as to derive IPv6 benefits. One of the required efforts is the Malaysian government agencies' IPv6 enablement in which the government agencies will spearhead all IPv6 migration in Malaysia. The creation of an IPv6 migration framework will assist the agencies in identifying the components and steps of the IPv6 migration process. A study is conducted on the IPv6 migration with the objective of creating an IPv6 migration framework for the Malaysian government agencies. Inputs were obtained from the government agencies staff in Malaysia through survey questionnaires and interviews. The findings were combined and categorized into five categories which are IPv6 awareness, IPv6 implementation progress, challenges, requirements and IPv6 implementation recommendations. The survey findings were combined with the initial migration framework to develop an IPv6 migration framework for the Malaysian government agencies which consists of the necessary components of the IPv6 migration that need to be considered. Triangulation technique which is a combination of two research methods which are questionnaires and interview has been used in this thesis to increase credibility and validity of the result. This thesis provides the framework that can be used to guide the government agencies in their IPv6 migration process, especially in the planning stages. The development of the proposed migration framework is based on resources from other countries that have migrated from IPv4 to IPv6 coupled with Malaysian government agencies specific IPv6 requirements, demands and challenges. The proposed IPv6 migration framework consists of several IPv6 migration components looking at different aspects of IPv6 migration essential for the agencies IPv6 planning.

CHAPTER 1 - INTRODUCTION

1.1 Overview

Today, Internet plays a vital role in the conduct of the businesses as well as everyday communication process. Internet Protocol version 4 (IPv4) is currently the most widely used internet protocol which was initially designed to facilitate communications between research laboratories, universities and government labs. However, the 30 years old IPv4 protocol was never designed for the rising numbers of mobile phones, PDA, RFID tags and other IP communication devices today. The limited 32-bit IPv4 address space is now a setback for the addition of new internet accessible devices and applications. IPv4 address space is theoretically limited to only 4.3 billion addresses, lesser than the world's population. It did not consider the increasing population and internet growth. Current solution for the depletion of IP addresses is the usage of Network Address Translation (NAT) which allows a large number of hosts to share a single IPv4 address. However, a number of issues arise with the usage of NAT. It does not support standard-based network layer security and higher level protocols mapping, and it is a bigger issue when both parties are connected through private addresses. Other disadvantage of IPv4 is it does not include authentication and encryption which is essential in private communications over public networks to secure data from third party view or modification. IPSec which addresses these issues are optional in IPv4 and proprietary solutions are required. Also, IPv4 is not able to accommodate the needs for greater mobility, integrated security, enhanced connectivity, faster speed and easier management. Realizing the benefits of IPv6, Malaysia has taken steps in adopting IPv6. One of the steps is the government agencies in Malaysia are mandated to migrate to IPv6. Planning is an important step in the IPv6 migration and thus, an IPv6 migration guideline is vital.

1.2 Background

IPv4's limited 32-bit address space; extensive growth of the Internet; the increase of Internet accessible devices and applications; the need for built-in authentication and encryption mechanism integrated with greater mobility, enhanced connectivity, faster speed and easier management; as well as other IPv4 limitations promotes the need for a new next-generation internet protocol known as Internet Protocol version 6 (IPv6) (WWT, 2006). Deployment of IPv6 globally is crucial for the advancement of the internet and moving towards the next-generation networks. Realizing the importance of IPv6 deployment, countries around the world are undertaking efforts to migrate to the protocol.

Japan, the pioneer of IPv6, has determined its IPv6 direction a long time ago. Its IPv6 transition goals and timelines have been identified through the e-Japan initiative (Esaki, 2007). At the same time, highly populated Asian countries, such as China and India, have more reasons to deploy IPv6 where factors such as the increasing devices, services and applications as well as the depletion of IP addresses plays an important role. Researchers, academicians and entrepreneurs from China hope to be one of the first, apart from Japan and Korea, to develop services and applications fully utilizing IPv6 features and capabilities (Worthen, 2006). For countries with more IP address allocation such as the United States, the main motivation for IPv6 deployment is the increasing population which requires more IP addresses and the need to exploit the IPv6 features and benefits (Ladid, 2007). Meanwhile, the European Commission has showcased its leadership in IPv6 through the fully funded IPv6 projects as well as awareness program efforts (Martinez et al., 2003). Nevertheless, Malaysia is also not left behind in the adoption of IPv6.

Recognizing the necessity and importance of IPv6, Malaysia is taking appropriate actions to deploy the technology. The Government of Malaysia has established a National IPv6 Council to provide leadership and strategic planning for the implementation and adoption of IPv6 in the country. Thereafter, National Advanced IPv6 (Nav6) Centre was setup by the Ministry of Energy, Water and Communications (MEWC) to coordinate and assist the National IPv6 Council in the deployment of IPv6 (MEWC, 2007). The IPv6 timeline is mandated by the Government whereby all ISPs in Malaysia must be able to provide IPv6 connectivity by end of 2006, federal government to adopt IPv6 by 2008 and the entire nation to be IPv6 enabled by 2010.

MYICMS886 (Malaysian Information, Communications and Multimedia Services 886) Strategy, government's blueprint to further develop the information and communications (ICT) technology, includes IPv6 as one of the eight key infrastructure projects. The adoption and deployment of IPv6 will complement the rest of the services and infrastructures in MyICMS886. With its features such as large address space, quality of service (QoS) support and advanced security, IPv6 will enhance and support the six focus growth areas identified in MyICMS886 which are (i) Content Development, (ii) ICT Education Hub, (iii) Digital Multimedia Receivers, (iv) Communications Devices such as VoIP, Embedded Components & Devices, and Foreign Ventures (MEWC, 2005). IPv6 is also identified as one of the key infrastructure to be implemented under the Ninth Malaysian Plan (9MP) from year 2006 until year 2010. Apart from sensor technologies and broadband, 9MP also states that the anticipated migration from IPv4 to IPv6 will spur R&D activities in the areas of IPv6 compatible applications, quality and security, which are new features available in IPv6 (EPU, 2006).

In line with the IPv6 timeline set by the Government, all major ISPs in Malaysia are Phase 1 IPv6 compliant according to the IPv6 compliance test done on 27th March 2007 (MEWC, 2007). The other important step is the federal government IPv6 deployment where efforts are taken to ensure that they meet the 2008 deadline. Among the efforts undertaken are the pilot projects in two ministries which are the Ministry of Energy, Water and Communications (MEWC) and Malaysian Administrative Modernization and Management Planning Unit (MAMPU).

However, most federal government agencies have not been able to achieve their 2008 IPv6 timeline due to many factors such as the IPv6 migration uncertainty, budget constraints and other factors. Only two government agencies (MAMPU and MEWC) have completed their IPv6 pilot project. There are several issues that should be identified and addressed while deploying IPv6 in government agencies. It is of utmost importance that the migration to IPv6 is non-disruptive to the agency's network and daily operations. Security is also a key importance in the communications of the government networks whereby network security should be well-protected during the migration process. Other concerns of the migration process are the cost involved, the needs, security impact and risk involved. To address these concerns and to provide necessary information on the migration to IPv6 process, a migration framework is necessary which the focus of this research.

1.3 Problem Statement and Objectives

Planning plays an extremely important role in the migration to IPv6 (Cisco, 2006). Most government agencies need to budget their projects much earlier. By planning the migration process early, agencies will have their budget on time. Determining the most suitable transition technique and mechanism is also a part of proper planning. The selection of the most appropriate transition technique from IPv4 to IPv6 is important as the migration period is long in which IPv4 and IPv6 nodes will exist in parallel. Various transition techniques and mechanisms can be used at different stages of the migration process or in combination at the same time (Huang and Ma, 2000). This can be identified in a migration framework.

In order to assist government agencies in Malaysia, the migration framework must be well-studied. Lack of guidelines on the migration from IPv4 to IPv6 in government agencies raises uncertainty to government agencies on the entire migration process. Based on the survey conducted (Chapter 4), agencies are unsure of the interoperability between the IPv4 and IPv6 systems, the IPv6 inventory assessments of devices, applications and services, the protection of network security during migration, and the measured cost of the entire migration. The migration from IPv4 to IPv6 requires more effort than the previous Y2K bug as Y2K is only said to affect a subset of systems but IPv6 will affect almost all of the current systems. Clear IPv6 migration guidelines will address the various IPv6 migration concerns and issues. Without proper planning, the transition to IPv6 could entail unwanted cost and complexity during migration. Thus, there is a strong need to create a well-engineered, sufficiently resourced migration framework which will minimize risks and ensure a more coordinated as well as risk managed migration to IPv6.

The main aim of this thesis is to propose a migration framework for the government agencies' IPv6 migration. The IPv6 migration framework will include the guide for IPv6 compatibility for devices, applications and services; benefits, limitations and comparisons between the various deployment techniques, security implications, costs involved and migration to IPv6 approach. The researcher also applies her experience and knowledge on IPv6 obtained from working in the National Advanced IPv6 (NAv6) Centre, Universiti Sains Malaysia. The methods used by the researcher to study and collect appropriate information and data to create a migration framework are literature studies, interview and questionnaires.

The benefits and advantages that IPv6 will bring to government agencies in Malaysia are deemed great but the transition process will not be an easy task without the assistance of a well-resourced migration framework. The migration framework specifically for government agencies networks with details on the transition process such as costs, equipments and applications requirements, transition techniques, security implications and others components must be created. The IPv6 migration framework will be able to identify steps and requirements of the migration process as well as to address the agencies' issues and concerns.

The objectives of the migration framework for the government agencies are stated below:

1. To propose a resourceful IPv6 migration framework for Malaysia's government agencies' IPv6 migration,
2. To create a migration framework equipped with necessary guidelines and information to assist government agencies in undergoing a well-coordinated transition,
3. To prepare a guideline on the costs of the transition,
4. To identify the potential security risks during migration,
5. To identify the applications and equipments to be upgraded or replaced.

1.4 Research Questions

This research will attempt to solve the following main research question:

"What is the approach that the government agencies should undertake in migrating to IPv6?"

Among the details that will be developed (sub-questions) through the main research question are:

1. What are the cost planning and assessments for the IPv6 migration?
2. What are the security planning and assessments for the IPv6 migration?
3. How do the agencies go about their IPv6 migration?
4. What is the deployment technique used for the transition?
5. Are there any other migration framework available / currently being developed for the transition to IPv6?
6. What are the government agencies staff perspectives, concerns, problems, progress and awareness of the IPv6 migration?

Figure 1.1 in the next page (Rich Diagram) shows the research problem in this study. Soft systems methodology (SSM) developed by Peter Checkland is designed to shape interventions in the problematic situations encountered in management, organizational and policy contexts, where there are often no straightforward 'problems' or easy 'solutions.' Though informed by systems engineering approaches, it breaks with them by recognizing the central importance of perspective or world-view in social situations. A variety of methods can be used to gather information ranging from formal research techniques to unstructured and serendipitous approaches; the advantages of the 'rich picture' according to Checkland is that it draws together information and perspectives from the widest possible range of sources (Lester, 2008).

It can be seen that the limitations and problems in IPv4 leads to the IPv6 adoption of the Malaysian government agencies and planning plays an important part in the migration process. However, the main concern is what is the migration approach? There is need for a migration framework with components such as cost concerns, security concerns, migration steps required, and the addressing of the agencies problems and concerns regarding IPv6 migration.

Below is the rich diagram showing the research problem:

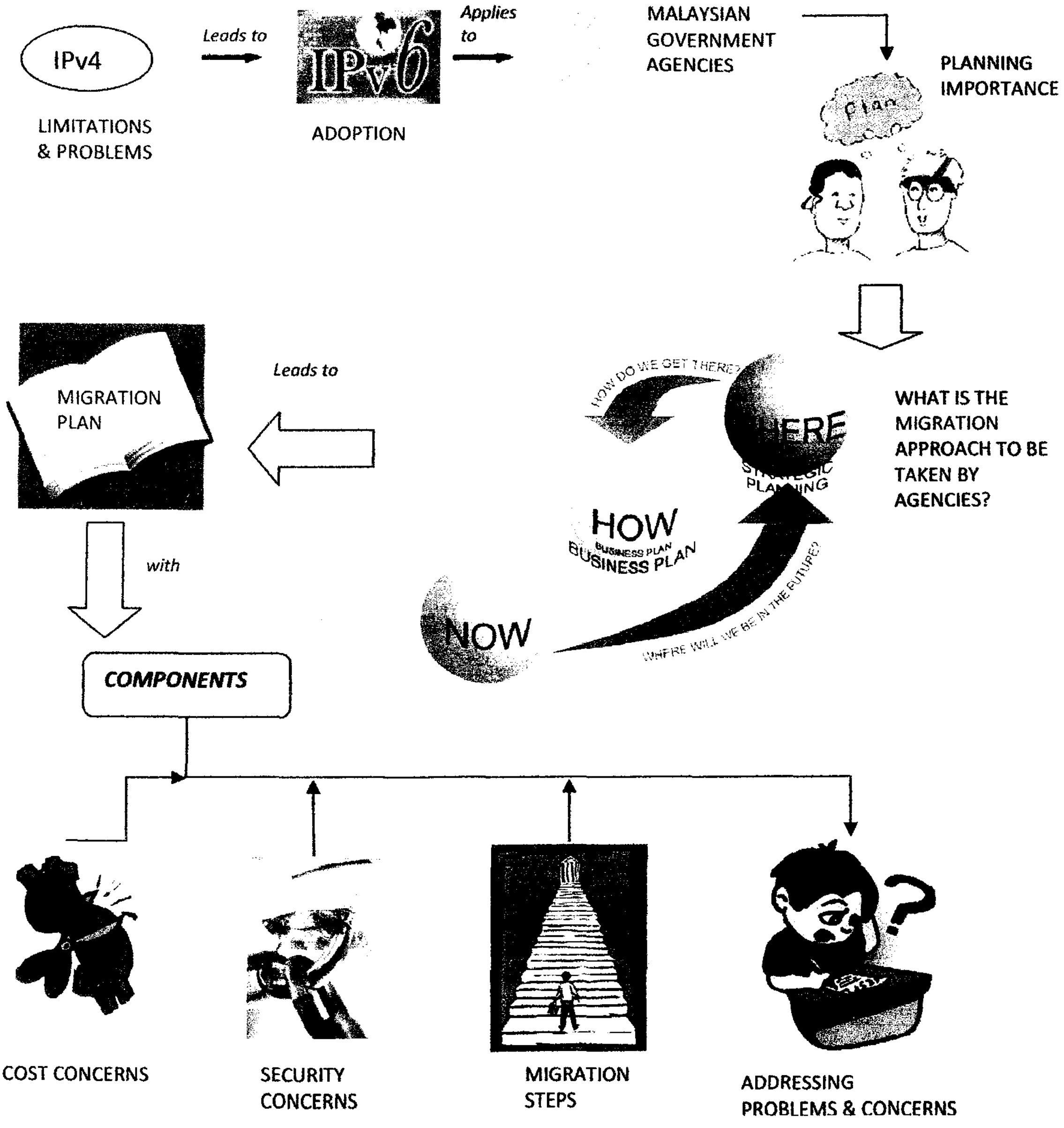

Figure 1.1 Research Problem Rich Diagram

1.5 Proposed Solutions

Malaysia realizes IPv6 adoption is necessary as IPv6 adoption contributes to Malaysia's vision to be positioned as a global ICT and multimedia hub. Most importantly, Malaysia will not be left behind when the entire world's network infrastructure is IPv6 enabled. IPv6 is identified in MYICMS886 blueprint and the 9MP as well as the mandated IPv6 timeline. One of the focuses right now, apart from the ISP's providing full IPv6 connectivity according to the IPv6 timeline, is the adoption of IPv6 by federal government agencies. The federal government agencies were supposed to have adopted IPv6 by end of 2008. However, only two Malaysia's federal government agencies have completed their IPv6 pilot projects by year 2008 which are MAMPU and MEWC.

Not only the government's timeline contributes to the need for the government's IPv6 migration, but there are many benefits in terms of technical and commercial that could be attained through the IPv6 adoption. For instance, through IPv6, government agencies are able to benefit technologically and improve their daily operations as well as overall business process. The integrated encryption and authentication features of IPv6 are vital in the government networks in providing data security and protection. Agencies will be able to fully utilize benefits of IPv6 such as Quality of Service (QoS), mobility, auto-configurations and other IPv6 features, for example, Department of Defense (DoD) United States utilizes IPv6's features for their net-centric warfare (Patterson, 2006). Since there are limitations in IPv4 and inevitable benefits and features in IPv6 government agencies have no reason for not adopting the technology. However, in-depth planning is extremely critical for the success of the migration process

The reason to which federal government agencies were chosen to spearhead the migration to IPv6 process in Malaysia as federal government agencies plays an important role in setting an example for state government agencies, private and semi-public organizations in Malaysia. Federal government agencies being the key element of the country that will lead the migration to IPv6 process as well as address the various concerns of other organizations which are to migrate by year 2010.

Although a lot of efforts are taken by various stakeholders in the adoption of IPv6 by federal government agencies, it is inefficient without the aid of a proper migration guideline or framework. An IPv6 migration framework will be able to guide the agencies on the issues and concerns that they have such as indicated cost; requirements of the migration; security impact; risk involved; deployment technique; and other issues. In a nutshell, a well-defined IPv6 migration framework will reduce possible errors and delays during the migration and provide more information on the overall migration process.

1.6 Importance of Thesis

Being a key element of the nation, government agencies must ensure that the migration process is technologically feasible and non disruptive to its daily operations. The main importance of this thesis is to create an IPv6 migration framework with guidelines on IPv6 migration to government agencies. Although needs and expectations vary greatly by agencies, the guidelines that can be applied and implemented in government agencies IPv6 migration.

This thesis aims to contribute in the following areas:

1. An IPv6 migration framework for the Malaysia's government agencies will prepare, plan and determine the necessary details and information as well as steps in the migration process.
2. The IPv6 migration framework will allow agencies to plan their IPv6 migration in terms of the migration approach, cost planning and assessments, inventory assessments, human resource training, and security planning and assessments.
3. Agencies are aware of and able to understand the challenges and risks of the migration process so that precautions are taken throughout the migration process.

With the aid of a migration framework, government agencies will be able to lead and spearhead the migration to IPv6 process smoothly in Malaysia and therefore, set an example for the other organizations (private and semi-public) in adopting IPv6 by 2010. It pays to plan ahead as planning will ensure the migration process is well-structured and organized, time is not wasted on unimportant matters, cost is controlled and complexity does not arise during transition process. With the migration framework, agencies are able to plan the purchasing and/or customize the creation of new products, application and services in which IPv6 compatibility is compulsory. Tenders for new equipments and applications that are sent out by the agencies must also include IPv6 as part of its specifications. Agencies are also able to plan the replacement and upgrading of equipments, applications and services to meet the IPv6 requirement. Government agencies will not waste unnecessary time and cost as well as to risk its migration which it might have without proper planning. As most of the government agencies are still at the planning stage of their migration process, the migration framework will boost the agencies' migration to IPv6 as well as to address the concerns that they might have with regards to the IPv6 migration. Agencies are able to move towards the next-generation network which offers tremendous opportunities, thus providing these agencies with the competitive edge needed.

Most importantly, this migration framework will assist government agencies to achieve Malaysia's vision to be IPv6 enabled by year end 2010.

1.7 Structure of Thesis

The thesis is organized into six related chapters.

Chapter 1 provides a background on the IPv4 and IPv6; features, benefits and advantages of IPv6 over IPv4; existing problem and the need to have an IPv6 migration framework; the methods used to obtain the needed / right information; and the contribution of the thesis in general.

Chapter 2 presents the literature studies done on IPv6 and about the studies in the context of IS research.

Chapter 3 discusses about the interview and questionnaires survey methods used to obtain information and relevant data to develop the IPv6 migration framework.

Chapter 4 includes the reports and analysis from the questionnaires and interview survey methods and finally, the research analysis.

Chapter 5 presents an IPv6 migration framework for Government agencies' migration from IPv4 to IPv6.

Chapter 6 concludes the research; lessons learned throughout the research process; contribution of the research; proposes way forward and future steps to further develop the migration framework.

CHAPTER 2 - LITERATURE STUDIES

2.1 Introduction

Today's networking requirements goes beyond just the support for web pages and email. IPv4, being an integral component of the Internet Revolution, is not able to accommodate the wide growth of network devices diversity, mobile communications and worldwide deployment of networking technologies.

Next-generation internet protocol (IPv6) was created to accommodate these needs. IPv6 is equipped with superior scalability, reliability and security compared to IPv4; and it is able to accommodate the addition of more devices, better mobility, upgraded connectivity, easier management, advanced security and better speed (Microsoft, 2004). This thesis is driven by the fact that there is no concrete migration framework available especially to assist the Malaysia Government agencies' IPv6 migration (Bradner and Mankin, 1995). This chapter discusses on various literatures that have been researched by the researcher in regards to the migration to IPv6. The researcher chose the appropriate literatures and data for the researcher's studies/migration plan from the many technical literatures on IPv6 available by looking at the ones with a strategic point of view. This chapter includes the Malaysia's Government agencies IPv6 readiness, infrastructure migration from IPv4 to IPv6, transition Techniques, guide on IPv6 support for applications and devices, security implications, cost implications, examples of IPv6 migration frameworks, and MEWC and MAMPU IPv6 pilot project.

2.2 Malaysia's Government Agencies IPv6 Readiness Status

Malaysia is not far behind in the adoption of IPv6. The National IPv6 Council was established to provide leadership and strategic planning for the deployment of IPv6 in Malaysia. Then, National Advanced IPv6 (NAv6) Centre was setup in 2005 by the Ministry of Energy, Water and Communications (MEWC) to assist the council and coordinate IPv6 deployment in Malaysia. IPv6 is identified as one of the eight key infrastructure areas under MyICMS 886 strategy. Under the 9th Malaysian Plan (9MP), IPv6 is highlighted as one of three technologies focused by the Ministry of Energy, Water and Communications. MYREN, a national research education network has an IPv6 dual-stack deployed linking 12 Universities and Research Centers (MEWC, 2007).

Malaysia has its IPv6 timeline set whereby all Internet Service Providers (ISPs) is to provide IPv6 infrastructure by year 2006, federal government agencies to adopt IPv6 by year end 2008 and the entire nation to be IPv6 enabled by year 2010. As for the ISPs, all major ISPs in Malaysia are Phase 1 IPv6 compliant according to the IPv6 compliance test done on 27th March 2007. One of the main focuses now is the federal government agencies IPv6 migration. Efforts are taken to ensure federal government agencies in Malaysia are able to meet their 2008 IPv6 deadline. One of the major steps taken to meet the federal government agencies IPv6 timeline is the IPv6 pilot project in two ministries. The two ministries are the Ministry of Energy, Water and Communications (MEWC) and Malaysian Administrative Modernization and Management Planning Unit (MAMPU). Both pilot projects which have been completed serve as a guide for other government agencies (MEWC, 2007).

2.3 Infrastructure Migration from IPv4 to IPv6

The huge Internet size and the large number of IPv4 users today makes it difficult to migrate straight from IPv4-only to IPv6-only. As individuals and organizations are getting more and more dependant on the Internet to perform their daily tasks, the downtime to replace the protocol will not be tolerated (Patterson, 2006). Thus, the best alternative is the co-existence of the both protocols and IPv6 should be implemented node by node based on the auto-configuration procedures which makes is unnecessary to configure IPv6 hosts manually. This will be the best way for users to derive the IPv6 advantages while still being able to communicate with IPv4 devices (Loshin, 2004).

There are five requirements identified by Chown (2005) to introduce IPv6 services in a network. The five requirements in introducing IPv6 services are as following (Chown, 2005):

1. The current IPv4 services should not be disrupted in any way during the router loading process of encapsulating IPv6 in IPv4 in tunnels;

2. IPv6 services must perform as well as the current IPv4 services or even better than the current IPv4 services (For instance, at the IPv4 line rate and with similar network characteristics);
3. Both IPv4 and IPv6 services should be easily managed and monitored as mechanisms must be available for both the protocols to be managed and monitored;
4. Network security must not be at stake in any way during the introduction of the new protocol (IPv6) or the loophole of the transition mechanisms used (if any); and
5. A plan for IPv6 address allocation should be created.

It is recommended that IPv6 migration follows a phased approach (Cisco, 2008). Cisco, 2008 has recommended the following phases to be followed in migrating to IPv6:

1. Testing IPv6 in a lab environment:

   The first phase of the IPv6 migration is IPv6 testing in the lab environment. This enables the agencies IT personnel to perform tests that could be disruptive or introduce a security risk if IPv6 was fully deployed in the agency's operation network. The test environment should be setup to resemble the actual environment. The lab environment should have network hardware and software features as well as the applications to operate over IPv6. The test lab should not be connected to the agency's operation network. Only when the testing is successful, the test lab can be connected to the agency's operation network. Through this test phase, IT personnel will obtain valuable experience by integrating IPv6 into the agency's network and finally determine its IPv6 migration framework.
2. IPv6 pilot deployment:

   The next phase is the IPv6 pilot deployment phase where IPv6 is deployed in a few locations of the agency's network. IPv6 is enabled in the infrastructure during the pilot phase. Routers and switches are setup to process IPv6 traffic.

In this phase, the agency's Local Area Network (LAN) is configured to transport the agency's IPv6 prefixes to the agency's host computers, printers and other devices. The agencies should also ensure that the network security architecture is configured to handle both IPv4 and IPv6 as well as to setup the DNS and DHCP servers to handle the IPv6 queries. The Network Management System (NMS) should also be configured to monitor the IPv6 network. One or more applications in the agency should be configured to run over IPv6 to experience IPv6 advantages.

3. Broad deployment of IPv6 in operations LAN/WAN environments:

   The next phase is the broad deployment of IPv6 in the agency's operations Local Area Network (LAN) / Wide Area Network (WAN) environments. The pilot network should be connected to the agency's WAN network while applying the lessons learned from the pilot deployment. The tested IPv6 enabled applications should also be available throughout the agency.

4. IPv6 and connectivity to the Internet:

   The next phase is the agency's IPv6 connectivity to the Internet where the agency will be using dual-stack connectivity to connect to the Internet. The agency's existing network infrastructure such as the intranet, DMZ, extranet and internet should be configured to block or allow IPv6 traffic as required. Security should be tested before the agency allows IPv6 connection with external sites.

5. Advanced Features:

   In the last phase of the IPv6 migration, the agency should identify how IPv6 features can improve the design and delivery of the agency's existing and planned applications and services using IPv6 features such as mobility, security, quality of services (QoS) and multicast.

Through this section on the infrastructure migration from IPv4 to IPv6, the researcher has identified the requirements and phases of introducing IPv6 in a network through the literature studies.

2.4 IPv6 Transition Techniques

Migration to IPv6 requires an appropriate transition technique (Hagen, 2006). There are several transition techniques that can assist the migration to IPv6. This section discusses on the IPv6 transition techniques available to assist in the IPv6 migration. There are three transition techniques (dual-stack, translation and tunneling) available and these transition techniques are differentiated through the connectivity of each system to the IPv6 Internet and the methods that the network and hosts achieves IPv6 capability.

The three IPv6 transition techniques are listed below and these techniques can be used in combination (Huitema, 1996):

1. Translation technique (IPv6-only networks) – This technique allows IPv6-only devices to communicate with IPv4-only devices
2. Tunneling / Encapsulation technique (additional IPv6 infrastructure) – This technique allows IPv6 devices at the edge to communicate via an IPv6 backbone, it avoids order dependencies when upgrading hosts, routers or regions
3. Dual-Stack technique – This technique allows IPv4 and IPv6 to co-exist in similar devices and networks

These transition techniques will be elaborated further in section 2.4.1, 2.4.2 and 2.4.3. The combination of two or three IPv6 transition techniques at the same time is known as a hybrid deployment technique. The migration from IPv4 to IPv6 will be done one step at a time, initiating from a single host or subnet (Huitema, 1996). Deployment of IPv6 in a large scale network will require more than just one technique based on the various demands and requirements of the network.

According to Shepherd (2002), factors that will decide the most appropriate transition techniques (if one or more techniques are used in combination) to be used during the transition are the number of registered IPv4 addresses, support for applications, service providers' offerings and the most desired transition timeframe (Shepherd, 2002).

2.4.1 Dual-Stack Transition Technique

Dual stack technique is one of the simplest methods of introducing IPv6 to a network and is also the best way for IPv4 and IPv6 to co-exist in the same time before the complete transformation to the IPv6-only network in the future (Gilligan and Nordmark, 2000). With the dual-stack technique, a host or router has both IPv4 and IPv6 protocol stacks in the operating system. IPv4 and IPv6 addresses are configured in each IPv4/IPv6 node. These IPv4 and IPv6 nodes can send and receive datagram and communicate with other nodes in the IPv4 combined with IPv6 network.

The issue of deploying an IPv4/IPv6 dual stack network is the need for the configuration of internal and external routing for IPv4 and IPv6 protocols. The IPv4 and IPv6 protocols interaction is also a challenge because the management of the interaction should be overseen. This is because dual-stack IPv4 / IPv6 networks will be mostly interacting with external IPv4-only networks in the beginning stage of IPv6 deployment (Schild et al., 2004).

According to Schild, Strauf et al. (2004), a network or backbone becomes dual-stack if the routers and switches in the network routes both IPv4 and IPv6. The implementation of the dual-stack technique will require the routers to support both IPv4 and IPv6 addresses. In a dual-stack technique implementation, it is necessary to have access to IPv6 Domain Name System (DNS) and adequate memory for both IPv4 and` IPv6. Challenges that might arise during dual-stack technique implementation are memory and CPU exhaustion as well as the need to introduce additional security requirement. Thus, the researcher suggests the steps should be taken to ensure that these issues and challenges does not arise, and a more smooth and cost-effective solution is created (Cisco, 2007a).

2.4.2 Tunneling / Encapsulation Transition Technique

Tunneling or encapsulation technique used in the migration from IPv4 to IPv6 is when IPv6 is used on top of the existing IPv4 infrastructure with no changes made to the routers or IPv4 routings (Gilligan and Nordmark, 2000). Tunnels encapsulate the IPv6 packets in IPv4 packets and carry it to the network parts that are not IPv6 enabled. Tunneling technique is used only when the network is not able to offer native IPv6 functionality. In other words, the tunneling technique is used when the network is not at all or partly offering native IPv6 functionality. The three steps involved in the tunneling process are encapsulation, decapsulation and tunnel management. The tunneling technique involves two tunnel endpoints. These tunnel endpoints are IPv4/IPv6 dual-stack nodes which most of the time are the routers (Carrera and Fernández, 2003).

Tunneling is considered a practical approach to the transition from the current IPv4 networks to adopt the IPv6 technology. As there are quite a number of existing tunneling mechanisms, it is not easy to choose the right tunneling mechanisms. There are a variety of tunneling mechanisms available (either manually or automatically configured tunneling mechanisms) to carry IPv6 over the existing IPv4 networks. The tunneling mechanisms available are configured tunnel; tunnel broker; automatic tunnels; 6to4; 6over4; ISATAP; Teredo; Tunnel Setup Protocol (TSP); DSTM; and Open VPN-based tunneling solution (Schild et al., 2004).

2.4.3 Translation Transition Technique

Translation technique is used when an IPv4-only device wants to communicate with an IPv6-only device, or vice-versa. IP header must be translated in this technique. The translation process will be more complex if the application processes IP addresses because most of the problems of IPv4 Network Address Translators will be inherited. The translation mechanisms available are Stateless IP/ICMP Translation Algorithm (SIIT), Network Address Translation with Protocol Translation (NAT-PT) and Network Address Port Translation with Packet Translation (NAPT-PT); Bump-in-the-Stack (BIS); Bump-in-the-

API (BIA); Transport Relay; SOCKS; Application Layer Gateway (ALG). ALGs are used to translate embedded IP addresses, recomputed checksums and others. SIIT and NAT-PT are associated translation techniques. DSTM which is a blend of translation and dual-stack model is used when insufficient IPv4 addresses are available. Similar to tunneling technique, translation technique can be implemented in border routers and hosts (Dunmore, 2005)

The diagram below shows the IPv6 Transition Techniques (Dual-Stack, Translation and Tunneling) for the migration to IPv6 as explained in section 2.4.1, 2.4.2 and 2.4.3:

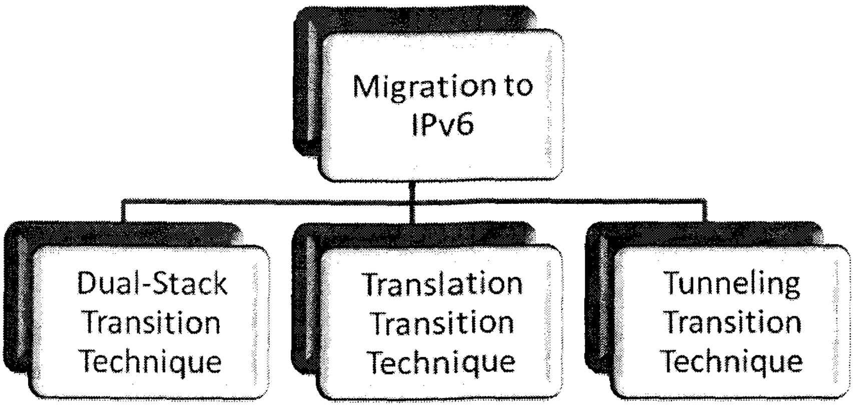
Migration to IPv6
Dual-Stack Transition Technique
Translation Transition Technique
Tunneling Transition Technique

Figure 2.1 IPv6 Transition Techniques Diagram

2.4.4 Integration and Coexistence in IPv6 Deployment

According to Cisco (2007b), the key strategy of deploying IPv6 in a network is to be able to integrate into and coexist with the current IPv4 networks. As IPv4 and IPv6 will most likely coexist for a long period of time, the transition technique chosen is part of the IPv6 designs basis. The choice of an appropriate deployment technique or the combination of various techniques are dependent on the agencies network infrastructure and the influence of other factors such as IPv6 traffic forecast and the availability of IPv6 support on end system (Cisco, 2007b).

2.4.5 Factors Influencing IPv6 Transition Technique Choice

There are several factors identified by Shepherd (2002) as the factors that influence the most suitable transition technique. The factors that influence the most suitable transition technique that should be used for organizations IPv6 migration are (Shepherd, 2002):

1. The amount of IPv4 addresses space available in the organization. Organizations with larger public IPv4 addresses should use dual-stack while organizations with smaller number of public IPv6 addresses should use an IPv6-only internal infrastructure such as NAT-PT or ISATAP. It is also possible to run parallel networks with IPv6 and IPv4 + NAT.
2. The speed of deployment also influences the choice of the transition mechanisms. The most suitable mechanism for organizations that conduct testing and the gradual migration to IPv6 is ISATAP or an internal tunnel broker.
3. The ISP service offerings also influence the choice of the transition mechanisms. Organizations which has access to an ISP offering native-IPv6 connectivity are able to use quite a number of mechanisms available while organizations without native-IPv6 connection access needs a 6to4 tunnel or built IPv6-to-IPv4 tunnels to other IPv6 locations.
4. Support for applications. Interoperation can be achieved through translators and relays such as NAT-PT, BIS, SIIT, TRT and SOCKS as well as dual-stack mechanisms such as DSTM and ALGs.

In choosing the appropriate transition mechanism, considerations should also be given to address space, existing infrastructure, cost and specific application domains (Shepherd, 2002). Based on the transition mechanisms and techniques discussed, the most appropriate transition technique or techniques (if a combination of two or three techniques is used in the same infrastructure) will be selected based on the criteria that need to be met.

2.4.6 Preferred Transition Technique

According to Cisco (2005), dual-stack technique should be considered as the way to deploy IPv6 in consideration of performance, security, quality of service (QoS) and multicasting. The dual-stack IPv4/IPv6 technique requires the switching or routing platforms. The simple reason to why dual-stack seems to be the most convenient technique right now is because most of our networks are running on IPv4 and right now, dual-stack IPv4/IPv6 network seems to be the best option (Cisco, 2005).

The advantage of dual-stack technique overall is that the network for both IPv4 and IPv6 are almost similar and there might not be a need for new IPv6-only routers and also does not need the maintenance of a potential complex network. However, this can also be a disadvantage. When the network is similar, the problems, particularly software bugs, might affect IPv4 services which would not occur if it was a separate network. The other issue is the performance consideration caused by running IPv6 in the IPv4 services particularly if the dual-stack implementation is not included in the hardware and IPv6 is encapsulated in the IPv4 routers in software (Cisco, 2005).

Cisco's campus IPv6 deployment options also suggest that hybrid deployment technique which is a combination of dual-stack and tunnels technique to be used in the enterprise IPv6 deployment (Cisco, 2005). The hybrid model states that dual-stack is used where possible and tunnels are used for the rest of the areas but all leverages on the existing IPv6 network design (Velde, 2005).

As dual-stack seems to be the suggested IPv6 transition technique, the steps in deploying a dual-stack IPv4/IPv6 network on common infrastructure as identified by (CIO, 2006) are as below:

1. The creation and operation of a test network with the tunneling of IPv4 (or maybe MPLS or ATM) connections to obtain the perspective on the IPv6 operations.

2. Evaluation of the router software versions in the test environment to know whether it is stable and robust to be used in the main network with IPv4 and IPv6 together and the ways IPv6 will affect IPv4 performance.

3. If the both protocols are stable, production routers can be upgraded to IPv4/IPv6 and IPv6 enabled on the links that are used and normally the network topology is the same as IPv4.

4. If problems such as severe bugs effecting production services come up, the problems should either be fixed or avoided or dropped back to an IPv4-only operation

2.4.7 Summary of Transition Techniques

Based on the literature on IPv6 transition techniques, the researcher understands that the selection of proper transition technique is necessary for the migration from IPv4 to IPv6. The three IPv6 transition techniques available as identified by the literature are dual-stack; translation; and tunneling that are differentiated by the connectivity of each system to the IPv6 Internet and the method that the network and hosts achieves IPv6 capability. The transition techniques can be used solely or in combination (hybrid deployment technique) depending on the size and deployment requirements of the network. Dual-stack technique and translation technique are interoperation transition approach which is the ability to convert from one format to another format (conversion of IPv4 and IPv6 packets) through protocol translation or dual-stack approach while the tunneling approach encapsulates data at one layer of the OSI model into the header of the same layer whereby IPv6 data is allowed to travel from one site to another via IPv4 in the internet.

Integrating and coexisting with the current IPv4 networks during IPv6 deployment is essential. As IPv4 and IPv6 will most likely coexist for a long period of time, the transition technique chosen is part of the IPv6 designs basis. The choice of an appropriate deployment technique or the combination of various techniques depends on the organization's network infrastructure and the influence of other factors such as IPv6 traffic forecast and the availability of IPv6 support on end system.

2.5 Guide on IPv6 Support in various Operating Systems

The researcher identified the need for agencies to have guidance in IPv6 support in various host, network devices and applications. This section discusses and identifies a guide on IPv6 support for host, network devices and applications that is essential for inventory assessment.

To understand the necessary equipments and applications that must be upgraded and/or replaced to enable IPv6 support, it is important to understand the IT environment elements first. The three categories of IT environment elements are as following:

1. Hosts

   For the host, Operating System (OS) must include a dual-stack IPv4/IPv6. The hardware configuration for a given host must be able to comply with the OS release requirements. Hosts include the following:

   a. Computers (mainframe, workstation, desktop, laptop and others)

   b. Mobile devices (PDA, smartphone, UPMC and others)

   c. VoIP devices (IP phone, conference bridge and others)

   d. Video over IP devices (IP camera, video server and others)

   e. IP-enabled industrial devices (sensors, readers and others)

2. Network Devices

   Network devices must support an IPv6 feature set that matches the deployment requirements. The different network devices are as following:

   a. Routers (software forwarding and hardware forwarding based platforms).

   b. Layer 2 switches (support for device management and other L3-related features such as Multicast Listener Discovery snooping).

   c. Layer 3 switches (hardware forwarding and service line cards).

d. Security appliances (firewall, IDS, VPN, concentrator, hardware encryptor).

e. Data centre networking (storage networking, load balancer and others)

f. Network management appliances (Network Analyzer Module, testers, probes and others).

g. Wireless infrastructure devices (Wi-fi access point, GGSN, Packet Data Serving Node (PSDN) and others).

3. Applications

The applications portfolio inventory should be able to deliver a matrix that provides the upgrade options. The various applications available are as follow:

a. Mandatory services (DNS server, NTP server, network management and others). IPv6 support in mandatory services is a must because these services are crucial elements to any deployment.

b. Off-the-shelf applications that depend on the software vendors to integrate IPv6 in their roadmap.

c. Homemade applications (applications that have been developed internally that would have to be upgraded for future use).

d. New applications (easiest to deploy IPv6 on).

e. Old applications (which will never be upgraded to IPv6 and eventually be replaced with newer applications).

The migration to IPv6 requires the upgrading and replacement of three major network component categories as following (Hexago, 2006):

1. Operating Systems (OS)

The OS must be dual-stacked. For example, IPv6 support in Solaris 7, Windows 2000, FreeBSD 4.0 (KAME), Linux (Usagi) in 2000, Mac OS X 10.2 and others.