An Economical IPv4-to-IPv6 Transition Model: -A Case study for University Network-

A. Hadi Arifin†, Dahlan Abdullah†, Sami Mohamed Berhan††, and Rahmat Budiarto††

†Faculty of Economics, Malikussalah University, Acheh, Indonesia
††National Advanced IPv6 (NAv6) Center, Universiti Sains Malaysia, Penang, Malaysia

Summary
The new internet protocol version 6 has promising with shining future. The Universities as a high learning organization should be the first mover to cope with this technology. This paper discusses and highlights the cost of migration from IPv4 to IPv6 in Universiti Sains Malaysia (USM), this cost includes two aspects, first aspect is the economical cost which is real cost of hardware, software, training and other cost which the sudden cost that take place in the system. The second aspect is the technological assessment which will discuss some components of the economical cost but from technical point of view.
We propose a cost model that could be followed by the Universiti Sains Malaysia to estimate the cost of migration to IPv6. The objective of this report is to be a model or a useful guide for IPv6 migration in USM network as well as for other universities' network.
Key words:
IPv6, Transition Cost

1. Introduction

There was an effort to develop a protocol that can solve problems in the current Internet Protocol which is Internet Protocol version 4 (IPv4). The Internet Engineering Task Force (IETF) was started to develop a new protocol in 1990s, and it launched IPng in 1993 which is stand for Internet protocol New Generation. The person in charge of IPng area of the IETF recommended the idea of IPv6 in 1994 at Toronto IETF gathering [1].

IPv6 has some transition methods or techniques that permit end user to put into operation IPv6 slowly but surely and provides a high level of interoperation between both protocols IPv4 and IPv6. IPv6 is a new promising technology which keeps upgrade in the history. It will slowly grow into existing IPv4 infrastructure and positively impact our network [9].
IPv6 product development and implementation efforts are already in progress all over the world. IPv6 is designed as an evolutionary step from IPv4. It can be considered as extra development to IPv4, because it can be installed as network software which upgrade in most Internet machines, and it can work smoothly with the current IPv4 data.
Since there are no transitional networks (ISPs) IPv6-ready yet in Malaysia, therefore, to get going deploying IPv6 we need transition methods, since there is no complete wide world IPv6 network infrastructure. The contributors of IPv6 understand that the transition from IPv4 to IPv6 will quite long time. Because it is possible that there will be some portion of ISP, people, and organization still use IPv4. As a result, we should know that changing the Internet Protocol from IPv4 to IPv6 will takes extensive period [7].
We should look at this stage as strategic vision, and we should look at the existing of IPv4 and IPv6 network infrastructure as necessary situation before the complete migration to IPv6.

It is quite obvious that changing directly from IPv4 to IPv6 is very costly, since many current network applications running on IPv4. Hence, IPv4 and IPv6 will coexist for some time.
The scarcity of information on the subject of IPv6 migration costs, merged with the reality that many organizations are not sold on the supposed benefits offered by the Internet Protocol version 6, is making the case for upgrading difficult to argue [2].

2. Theoretical Consideration

One of the main transition techniques is Dual-Stack method where the end communication point has provided by both protocols IPv4 and IPv6. In this case, if the node communicates with another node that run IPv6, the dual stack node will work as only IPv6 protocol, at the same time if the end host communicate with another host which runs IPv4, the dual stack node will operate as only IPv4.

The dual-stack transition mechanism can work in three different styles, first one is when the IPv4 stack is switched on and the IPv6 stack is switched off, so in this case the stack behaves like an IPv4-only node. When the

Manuscript received November 16, 2006.
Manuscript revised November 22 , 2006.

IPv6 stack is switched on and the IPv4 stack switched off, it behaves like an IPv6-only node (see Fig.1).
When both the IPv4 and IPv6 stacks are active, the node can use both protocols to ensure effective transition. For each IPv4/IPv6 node it has at least one address for each protocol version. The configuration part of dual-stack, it uses IPv4 configuration styles which are static configuration or DHCP to configure IPv4 node, and it uses IPv6 configuration methods which are static configuration or auto configuration to configure IPv6 node.
Domain Name Server should be able to resolve both IPv4 and IPv6 which has specific requirement for resolution. Other transition techniques are tunneling and translating [5,6,7,8].

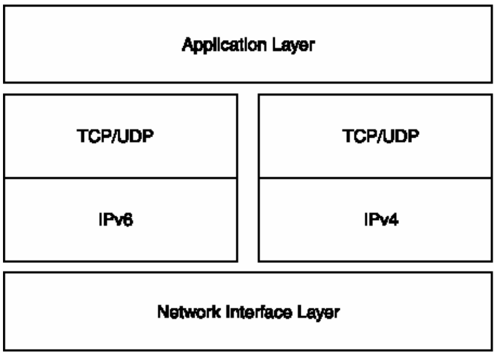

Fig1 Dual-Stack structure [7]

2.1 IPv6 transition Cost and Economic Factors Consideration

Implementation of IPv6 will involve some cost, since it is new technology and it will run using the current network infrastructure which is IPv4. However, the key features that IPv6 offered will enable us to save cost especially in the long run.

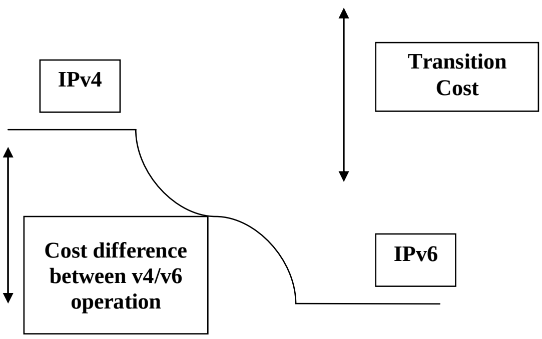

Fig.2 Cost difference between IPv4 and IPv6 [10]

In Fig.2 is a study that has been conducted by North America IPv6 task force. It shows that operation cost of IPv4 is very expensive comparing with IPv6 where the line of cost start form bottom, nevertheless, co-existence of IPv4 and IPv6 during migration process will incur cost, since we will use transition mechanism to deploy IPv6 in this period. The cost includes hardware, software, staff training and transition.

Although dual-stack, Tunneling, and translation are providing us with transition solution, but still it is not complete, there are still some other issues we should consider to get complete solution for transitioning. One of the issues is economic factors which are 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, the need of upgrading hardware, and availability of IPv6 products in the market. The first factor user demand for IPv6 is one of the strongest reasons to go for IPv6, since it has many features and it has bigger address space. It also has enhanced quality of service, error handling, security and authentication which attract the end user for demand IPv6, but at the same time increasing in the demand, will increase the number of network administrator needed, and also specialist end user [3].

From the global view of point IPv4 addresses are limited, because theoretically IPv4 allows only four billion nodes to be connected to the internet, since the internet users are increased gradually year by year it seems that IPv4 will have shortage of internet addresses. In the other hand, IPv6 is very big and theoretically it can allow (340 undecillion) nodes to be connected to internet. These internet addresses are unique which can support real end to end communication without the need for NAT which make the overall network messy with unreal internet addresses.

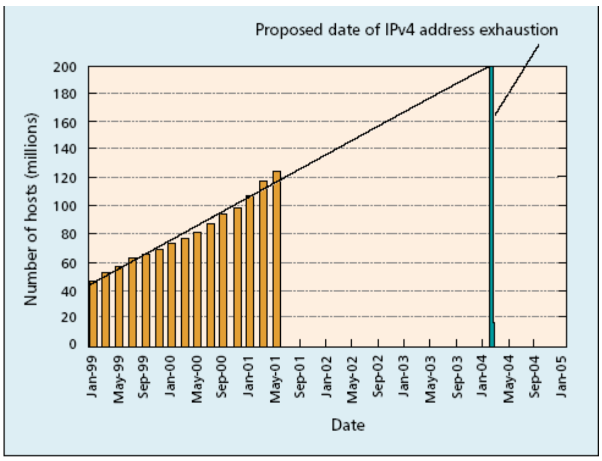

Fig.3. IPv4 addresses exhaustion [4].

Fig.3 shows the exhausting of IPv4 addresses, with the increasing number of hosts that connect the Internet. Huitema (IETF RFC 1715 Proposed the H-Ratio which defines a logarithmic ratio of end systems to available address bits). From this, the H-Ratio expects that only 200 million end systems are possible to consume the rest of the address space. Having this investigation, with the observed increase of the Internet technology and users, it would seem that IPv4 address collapse could become a serious problem by 2004 [4].

Another economic factor is marinating IPv4 application, which is also a technical issue. It is very important that current applications which run on IPv4 can also run on IPv6. Most probably it will be some applications cannot be ported to IPv6 and end user will not be motivated to implement IPv6, since the interested applications cannot work on IPv6 network but the need for IPv6 features may affect the legacy of marinating IPv4 application.

The last factor that we touch on is upgrading network infrastructure. Generally, the current IPv4 infrastructure cannot handle IPv6; therefore many transition mechanisms exist to solve this problem partially. Upgrading will include both network hardware and software to support IPv6-compatible protocols. Majority of network hardware working on IPv4 based, and it tries to enhance its packet processing performance by application-specific integrated circuit (ASIC) hardware, and such hardware is not easy to upgrade. The other component of upgrading which is network software, there are a number of routing software that IPv6-capable, and it is commercially available.

2.2 Approaches to Estimate IPv6 Transition Cost

Basically to come out with a transition cost model, we need to follow a specific approach that helps us in organizing the raw data, and designing a good model.
There are two types of approaches that we could follow which are:

- Statistical approach.
- Economic Assessment approach.

Concerning statistical approach it is well known method but due to the shortage of information regarding IPv6 migration cost, and the range of this method which work more efficiently on a wider range such as ISP transition cost whereby we need to collect statistical data about the internet users and the ISP itself.

The second approach, Economic Assessment approach, which we will follow in this paper. It is concerning about the direct cost that incurred from IPv6 transition and deployment. It works fine with either IT or non-IT organization. For example this approach has been followed by U.S. department of commerce's National Telecommunications and Information Administration for IPv6 cost in USA.

2.3 Economical Assessment Cost Approach

As normal big project which is deploying IPv6 the cost obviously will be high in the beginning but we can expect the cost to get lower and lower because of two reasons:
First, the wide benefits that we will benefit from it that IPv6 offers.
Second, the cost of hardware and software predictable to be cheaper since many organizations in IT business industry are moving towards IPv6.
Economic cost approach is straight forward to the cash cost of the elements of the cost model. It is applicable for our case building IPv6 transition cost model for the universiti Sains Malaysia.

In order to build an IPv6 model for non- profit organization such as Universities, by following economical assessment approach. We will need to highlight both cost and benefits since we are looking at it from economical point of view.

Our cost model will contain four components which are:

1- Network Hardware costs.
2- Network Software and operating system costs.
3- Training costs.
4- Unpredictable costs.

Now we will discuss each components of the model in terms of economic cost.
First, hardware is an important element, it is mainly consists of IPv6 router which is forwarding IPv6 packets and it is main purpose is to allow computer nodes to operate stable IPv6 networks ,firewall hardware which is also the important security mechanism, and it is functioning as packet filtering. Other network hardware such as interface cards, name server switches, and hosts. The cost of this hardware is depending on the individual networks how big it is and the level of IPv6 use as well as some of the hardware can be IPv6 capable by way of software upgrades. So the range of hardware cost here is low to medium according to NIST.

Secondly, the software cost. Upgrading some software will be required to work with IPv6, and other software we should keep upgrading from time to time. Software upgrades includes server software which is needed to operate the server computer, server and desktop operating systems such software is available by many vendors such as Microsoft, Sun Microsystems also it is available by open source providers such Linux operating system, network administration and monitoring this type of software is usually is necessary to the firewall system or the intrusion detection system, however the main software costs that organizations 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. So the software cost also has a range of small cost such as cost of operating system and server application to large cost such as network monitoring software, and huge application like enterprise resource planning software.

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

Furthermore, the extra costs that come after the IPv6 implementation may possibly be more obvious since the level of the technical staff who are in charge of the network are vary from one staff to another. Likewise, training costs should be smallest for organization such as universities because it usually have already some networking professionals and consultants. As long as the migration is going on, more and more network hardware and software will to be required which will come with the result of extra network administration costs.
Lastly, other cost. This last component is a variable cost and it is subjected to the sudden accident occurred and affect the overall cost. For instance, employees performance diminishing caused by the sudden change of the network system, cost that occurred when we want to fix some problems in interoperability and security intrusion if the network affected by intrusion. The situation are quite different , as result it classified as other cost and its cost is vary from small cost, medium cost to large cost depends on the case.

The Asian Pacific network information centre come with suggestion according this issue, they suggest that a courses in the members who are allocated for IPv6 from APNIC such as Japan, Korea, Australia, Singapore, and the rest of the members.
Second suggestion is conducting courses about IPv6 in a form of opening seminars, and lastly conducting courses through website since it is very useful way of conducting training. The IPv6 Cost Model Diagram is shown in Fig. 4.

3. Prototype

In order to build a prototype IPv6 transition cost model for USM, we need firstly to be sure that the design of the model fit the non-profit organization such as universities.

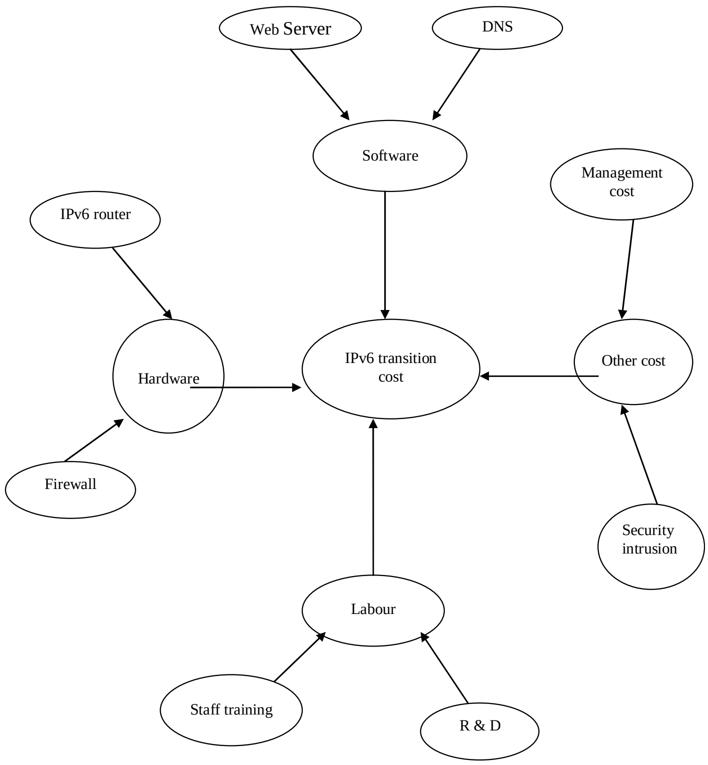

Fig.4 IPv6 cost model diagram

Determining the cost to be high or low is vary from one organization to another. For example, long run investment such as building IPv6 network might be significant to one organization and it is not for others, as well budget allocate for the project is also vary from one organization to another. Table 1 shows the prototype of the cost we proposed. Since it is a prototype model the cost we obtained is not fixed. It depends on the university capabilities', we have tried to put the weight either Low, Medium or High cost, by comparing the university's situation with other public available data about IPv6 vendors, enterprise and ISPs. We also add some kind of data such as management cost, because it is well known that any decision coming out from university need to go through many management processes. Another thing that might be added is trying to weight each of IPv6 benefits to be complete cost analysis report, since the magnitude of potential benefit is significant.

Table 1: IPv4 to IPv6 Transition Cost for USM

Item	University's cost
Hardware	
Replace router	**Medium**
Replace firewall	**Medium**
Replace interface cards	**Medium**
Software	
Upgrading network monitoring/ management	**High**
Operating system	**Low**
Upgrading DNS server and web server	**Low**
Upgrading databases software e.g. oracle, SAP	**High**
Labor	
Train networking staff	**Medium**
R & D	**Medium**
Other	
Unexpected threat e.g. security intrusion	**High**

4. Implementation and Result

In this section, we are going to discuss the estimated cost of migrating from IPv4 to IPv6 in the Universiti Sains Malaysia. We will highlight firstly, the IPv4 infrastructure cost for USM, since IPv4 is the only internet protocol used in USM.
Then we can emphasize on the cost will occurred by migrating to IPv6. Lastly we will come out with possible solutions to migrate to IPv6 with less cost.

Usually the cost of the internet infrastructure includes many factors that potential organization must take it into consideration in order to maintain the internet service of the organization. These factors usually include the hardware technology that enables the organization to have connection to the Internet and connect the organization's department with each other. The hardware technology can be classified to essential hardware, which necessary to make the network to work properly such as routers and switches and non-essential hardware which makes network work efficiently such as network monitoring/ management system.

Another factor is the software which is the same as hardware necessary to enable the network to work properly such as the operating system, and server software, also other software to keep the network performance efficient like intrusion detection and prevention software.

An important factor might be the labor cost. Labor cost mainly focuses on the training cost. This training cost can be high or low cost, depends on the training subject, in other words, if the training subject is very advance or professional level, it might be expensive since it required advance trainers and hardware. In the contrast, if the training subject not that advance it might not be expensive. The last factor we will highlight here is the unexpected cost, which we labeled under other cost.

Before we come to the estimation of the cost for IPv6, we need to have close look on the current IPv4 cost and then give our estimation in the case of migrating to IPv6.

According to USM computer center which is in charge of maintaining the Internet technologies in USM, we have the information about overall IPv4 infrastructure's cost. We can organize this information as in Table 2.

Fig. 5 shows the Estimated transition time for USM to migrate from IPv4 to IPv6 (Dual stack configuration)

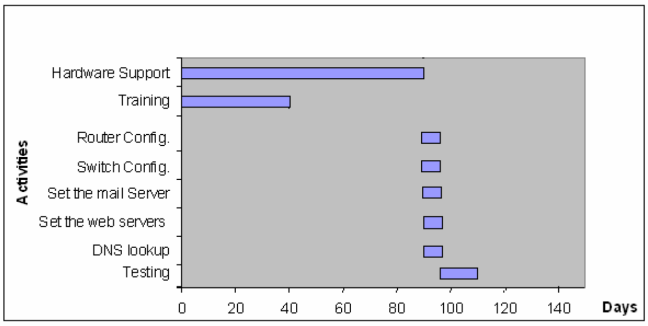

Fig. 5: Estimated Transition Time for USM

Table 2. Current IPv4 Infrastructure Cost at USM

Item	University's cost	Cost Range
Hardware		
Router (WAN)	**RM 10,000 – 20,000 per router**	**Medium**
Firewall (**Intrusion Detection/Prevention)**	**Few hundreds thousands**	**High**
Core switches	**RM 400,000 per switch**	**High**
Normal switches	**RM 2000 – 5000 per switch Multiply by 500 units switch**	**High**
Cabling	**RM 200 multiply by 50,000 fiber optic and 55K UTP**	**High**
Software		
Upgrading network monitoring/management	**IDP software**	**High**
Operating system	**Linux**	**Low**
Upgrading DNS server and web server	**Linux**	**Low**
Upgrading databases software	**Sybase System**	**High**
Labor		
Networking staff training	**RM 5000 per person**	**High**
Normal user training	**Handled internally**	**Low**
Other cost		
Unexpected threat e.g. security intrusion	**Affect students and university reputation**	**High**
Management Cost	**Descision of upgrading takes around 6 months**	**High**

4.1 Technological Cost Assessment

4.1.1 Network Hardware Issues

Nowadays the new existing firewall support both IPv4 and IPv6, however these firewall operate quite differently since we have to separate rule-sets for IPv6 and IPv4. These rule-sets should be handled very carefully. Because any mistake in this stage will cause security exposure.
Although Internet protocol version 6 has many criteria that make it quite preferable from security point of view. It is easy to configure and it has the option of auto configuration. It is secure or hard to be lied to malicious scan from intruders. It also has the criteria of make scanning and initiate self propagation against security threats. However, IPv6 still is facing some security challenges. Some of these challenges are concerning the firewall filtering, other is concerning servers problems in the other ends. As well as Application challenges that causes security exposures.

IPv6 firewall challenges

There are some challenges facing IPv6, and these challenges differ from one migration technique to another. For example, in the tunneling migration technique this has SIT and Teredo which address assignment and automatic tunneling for unicast IPv6 transition, protocols. Currently it has some challenging for the firewall, because tunneling techniques encapsulate the IPv4 packet and the firewall is not designed to apply the set – rules of packet filtering on the payload of IPv6 rather than rules applied directly to the IPv4.
Another challenge is the firewall of 6to4 and SIT does not exist yet. For an IPv4 firewall rule-set, SIT and 6to4 are nothing more than IP protocol 41 on IPv4. As for an IPv6 firewall rule-set, SIT and 6to4 do not exist in the market. No rule set applies straight away to such type of tunnels beyond switching the current protocol 4 on or off. In the other tunneling type which is Teredo, it is considered and functioning just as User Datagram Protocol on IPv4, and it is not handled by the IPv6 stack and rule-set.
So since the firewall may do not have the rules that applied straight away against the tunneled payload traffic, such tunneling protocols seems to cause a security exposure.

In common, we might categorize the security issue in IPv6 into: Challenges that appear once we want to apply same IPv4 set-rules to IPv6. We mentioned about this example above.

The second category is IPv6 security for small network or for home network. For example, what kind of security policy should be followed, since there is no security policy standard for the small network?

Other challenges as we mentioned above is concerning the server in the other end. If the server in the other end is not configured properly it can easily cause a security and IPv6 can not protect us against such security threats.

As same as server mis-configuration threat, the design of the application if it is poor it could create a security hole that might be exploited by intruders.

4.1.2 Network Software and operating system issues

Sybase database

According to Sybase official website the IPv6 is not supported yet. The Sybase is a complete database system but It works with EAServer which basically run on internet network. Currently it is still running on IPv4 Internet Protocol.
Why does not support IPv6? Because the Sybase system is using Eclips for their java development, and currently they are using JDK 1.4 which is not supported IPv6 protocols

Operating system

The operating system used in most of the IPv6 network is Unix or Unix-like operating system. Currently, IPv6 is a default set in many operating systems such MacOs, windows and Linux operating systems.

Linux is preferable to many organizations since it is open source, and it offer many of its services free of charge such Domain Name server, and the operating system itself.

Also in Unix – like operating system can be done manually or otherwise from the option in the Network preferences panel , but usually it is a default setting in all Unix-like operating system.

4.1.3 Training issue

Since the IPv6 considered as new and promising standard for Internet protocol, there is need to educate people specially who are in charge of the network administration. In the case of the Universiti Sains Malaysia, it should train its network administrators and other computer professional staff to cope with this new technology.

At present the computer center in the Universiti Sains Malaysia trains the network staff to keep their skill up to the standard. Such training is holding in outside computer training institutes which engage the computer center in a prohibitive cost.

The IPv6 training is quite different form the network routing training that is available right now in the network training centers. We can observe that there are some few IPv6 relative topics training such as Cisco IOS and so on. However, there is no a complete IPv6 course offered yet that discuss and train the users about IPv6 transition methods.

In the case of the Universiti Sains Malaysia, it can take the advantage of the Computer Science School and the National Advanced IPv6 center conduct IPv6 training in-house. While we have mentioned previously that the cost of labor should be less in the education organization such as universities because there are available experts in such organization which help us to cut the cost dramatically.

4.1.4 Unpredictable other cost

This type of cost must be around all the ways, because the network system is dynamic and not fixed. Then, the cost of sudden case happen to the system can be recorded under this component of our cost model. Here we will discuss the IPv6 transition cost from the technological point of view.

Unexpected cost can be in Hardware, software, or in staff performance. In the case of software unexpected cost we know that not all applications run on IPv6, and there are a heavy progress to make IPv6 available as an option in the software network connection.

Unexpected cost of training staff, this case might happen and it is very usual for staff to have short training due to sudden development progress. This type of training could be expensive if it is conducted outside the university.

Other than that as we have mentioned earlier, an example of unexpected cost can be in form of cost of the damage that happen because of virus attack. This damage can be physical damage or as a university can be damage in the reputation especially if the university system is not accessible or not reachable. The graph in Fig.5 summarizes the IPv6 technological cost for USM based on the current Ipv4 Network infrastructure.

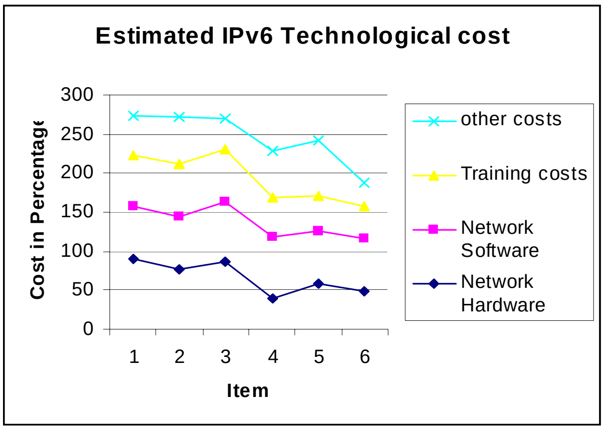

Fig. 5: Estimated IPv6 Technological Cost

4.2 The estimated IPv6 cost model for USM

Table 3 shows the cost model we obtained from the assessment we conducted that took time about 2 months.

5. Conclusion

The implementation of IPv6 is getting wider and wider acceptance between nations and countries. The universities as high education organization should be the first mover to adopt the new technology. Cost estimation of IPv6 transition can help IPv6 migration faster. As for USM case, the overall transition cost is relatively low. The highest costs occur for labor, unpredictable and management costs. The cost for hardware is low, since USM just upgrade their core switches and routers.

Table 3. Cost Model for USM

Item	Description	University's cost
Hardware		
Router (WAN)	**Fixed cost**	**Low**
Firewall (**Intrusion Detection/Prevention)**	**Few hundreds thousands**	**Medium**
Core switches	**Fixed Cost**	**Low**
Normal switches	**Fixed Cost**	**Low**
Cabling	**Fixed Cost**	**Low**
Software		
Upgrading network monitoring/management	**IDP software**	**Medium**
Operating system (Linux)	**Open Source**	**Low**
Upgrading DNS server and web server (Linux)	**Open Source**	**Low**
Upgrading databases software	**Sybase System**	**High**
Labor		
Networking staff training	**RM 5000 per person**	**High**
Normal user training	**Handled internally**	**Low**
Other cost		
Unexpected threat e.g. security intrusion	**Affect students and university reputation**	**High**
Management Cost	**Decision of upgrading takes around 6 months**	**High**

References

[1] Arano, Takashi. June 2003. "IPv6 Market Opportunities—Real Business Challenges in Japan." Presented at the U.S. IPv6 Summit

[2] Cara Garretson 2005, unclear costs dampen IPv6 migration. Network World, August 8.

[3] Cisco Systems. 2003a. "SAFE: A Security Blueprint for Enterprise Networks." <http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm>. Posted Wednesday, October 22, 2003.

[4] Daniel G., Fangzhe C. 2002.Realizing the Transition to IPv6. IEEE communication magazine, June, vol. 6, issue 3: 138-148.

[5] Hossam A., Laurent T. 1999. Methods for IPv4-IPv6 Transition. The Fourth IEEE Symposium on Computers and Communications, France, 478-484.

[6] Ioan R., Sherali Z. 2003. Evaluating IPv4 to IPv6 Transition Mechanism. IEEE, West Lafayette, USA, v (1):1091-1098.

[7] Joseph Davies. 2003. Understanding IPv6. Washington: Microsoft Press.

[8] Kai W., Ann-Kian Y.A.L.Ananda. 2001. DTTS: A Transparent and Scalable Solution for IPv4 to IPv6 Transition. IEEE .Singapore, 248 – 253.

[9] Silvia Hagen. 2002. IPv6 essential. New York: O'Reilly.

[10] Yanick P. 2005. Providing an IPv6End-2-End Environment IPv4 IPv6 Interoperation. NAv6TF/ARIN XV IPv6 Conference

Hadi Arifin received Bachelor degree from Syiah Kuala University and Magister Economics degree from Padjadjaran University in 1985 and 1991, respectively. Currently, he is a Ph.D candidate at School of Social Science, Universiti Sains Malaysia (USM). He is also Rector of Malikussaleh University in Lhokseumawe, North Acheh. His research interest includes economical asssesment cost.

Dahlan Abdullah received Bachelor degree in Informatics Engineering from Universitas Islam Indonesia (UII) in 1999. He is currently doing his master of science program at school of computer sciences, Universiti Sains Malaysia (USM). His research interest includes IPv6 and network management.

Sami Mohamed Berhan received his B.Sc. in Computer Science from International Islamic University and Master in Computer Science from Universiti Sains Malaysia (USM) in year 2004 and year 2006, respectively. His research interest includes IPv6 and network security

Rahmat Budiarto received B.Sc. degree from Bandung Institute of Technology in 1986, M.Eng, and Dr.Eng in Computer Science from Nagoya Institute of Technology in 1995 and 1998 respectively. Currently, he is an associate professor at School of Computer Sciences, USM. He is the deputy director of National Advanced IPv6 (NAv6) Center, USM. His research interest includes IPv6, network security, Ethnomathematics and Intelligent Systems. He is chairman of Security Working Group of APAN.