UNIVERSITY OF MAURITIUS RESEARCH JOURNAL – Volume 16 – 2010
University of Mauritius, Réduit, Mauritius

Research Week 2009/2010

IPV6 Deployment - Mauritius to benefit from Opportunities and World-wide Experiences

O Moonian
Faculty of Engineering,
University of Mauritius
Email: ovn@uom.ac.mu

Anwar Chutoo
Faculty of Engineering,
University of Mauritius

Begum Durgahee
Faculty of Engineering,
University of Mauritius

Sameerchand Pudaruth
Faculty of Engineering,
University of Mauritius

Paper Accepted on 17 March 2010

Abstract

The current standard protocol, IPV4, has reached its limit in terms of addressing possibilities, being limited by the 32-bits addressing scheme. Its successor, IPV6, had been devised since the mid 1990's. In addition to handling the address limitations, IPV6 also includes a number of improved features, making it superior to IPV4 in several aspects. However, its deployment has taken much longer than expected. This paper presents how the design IPV6 improved over IPV4, the additional benefits of the new design, and challenges faced for the deployment of IPV6. It then outlines the deployment strategies adopted by different countries. It finally discusses how Mauritius can benefit from the IPV6 deployment and what lessons it can draw from deployment experiences obtained elsewhere.

1.0 Introduction

IPV4 has been the standard protocol over the Internet for more than two decades. It has proven to be robust, easily implemented and interoperable and had stood the test of scaling an internetwork to a global utility of the size of today's internet [Davies, 2008]. However, in spite of this, IPV4 has serious addressing, routing and security limitations, that had been identified since the mid 90's [Melford, 1997]. Its use of 32-bits addresses is a major limitations in the number of devices that can have an IP address and is a major hurdle for end-to-end communication in ubiquitous computing and the exponential growth of devices that can connect to the Internet. Additionally, the classes A,B and C address allocation is inherently inefficient and besides addresses have been distributed in an inequitable way, resulting in a bias with more than 70% of the global IPV4 addresses belonging to organizations in the US from the early days [Hagen, 2004].

The next IP generation, IPV6, has been proposed since the mid 90's [Hiden, 1996] and has been quite widely deployed since. It has major technical advantages, such as a virtually inexhaustible number of IP address (5 x1028 for each of the 6 billion persons in the world today). However, the deployment of has a price tag and the need and merit of its deployment has continuously been debated, resulting in a large number of organizations showing reluctance to completely change to IPV6. This explains why the globe is not fully IPV6 yet. There is the large base of IPV4 infrastructure that already exists and the large base of IPV4 applications that may need to be IPV6-enabled [Bouras, 2005]. Thus researchers have tried to address the limitations in number of addresses through alternative solutions such as CISR and NAT. While the alternative solutions fill the gap in the short term, IPV6 provides a more durable solution and the protocol goes beyond the addressing issue. It improves on a number of existing features while also including additional features resulting in an improved efficiency and quality of communication.

With the many advantages, it provides IPV6 will open up opportunities that would either not be possible or would be inefficient under IPV4. Mauritius will need to seriously consider the shift to IPV6 in the near future, so as to be able to benefit of the multiple advantages and opportunities presented by IPV6. This paper presents the different advantages of IPV6, the price tag for its deployment and discusses the opportunities and challenges that its deployment presents for Mauritius. The rest of the paper is structured as follows: section 2 discusses how the design of IPV6 addresses the limitations inherent in IPv4, section 3 presents the challenges faced for IPV6 deployment while section 4 discusses different migration technologies. Section 5 presents the deployment strategies adopted in different developed countries. Section 6 discusses the deployment strategies for Africa, section 7 then presents the challenges and opportunities for Mauritius while section 8 concludes the discussions.

2.0 Addressing the limitations of IPV4

IPV6 has been designed to overcome shortcomings of IPV4 in a number of features. This has been achieved by changes in the header, where fields have been changed in their sizes, purposes and processing needs, while new fields have been included to enhance support for some of the features. This section discusses these changes.

2.1 Larger Address space

To overcome the limitations of IPV4, IPV6 uses 128 bits for addresses. With its large address space, IPV6 will not only connect more people to the Internet, it will also enable the use of all sorts of always-on devices like mobile phones, sensor devices, tv-sets, digital radios, refrigerators, air conditioning devices, cars, and many more to imagine, that will each need a permanent IP address [Hagen, 2004]. The very large number of available addresses also allow for a more organized address assignment and more efficient routing. With IPV4, the maximum number of bits allowed to a site for subnetting and addressing hosts is 24 bits, with 8 bits being used to identify the organization. Since this allows for only 256 organizations and a number of such 8 bits combinations have already been used for the same complexly-organized group, this leaves rather limited scoping for addresses allocated to ISPs. Thus most sites around the world can only be allowed 4-8 bits for subnetting and 4-8 bits for hosts [Eddy, 2006]. With the much larger address space of IPV6, the Internet Assigned Numbers Authority (IANA) provides addresses to Regional Internet Registries and the latter to Local Internet Registries in such a way that at least 16 bits are available for subnetting only, in addition to the 64 bits available for host addressing. The available address space further allows for well-defined scoping which enables IPV6 to have additional features such as all-routers addresses and prefix-delegation extension.

2.2 Higher Security

IPV4 provides for security of transmitted data through the use of the IPSec, a framework of open standards developed by the Internet Engineering Task Force (IETF) that provide security for transmission of sensitive information over unprotected networks [Dunmore, 2005]. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (peers), such as Cisco routers. IPSec provides the following (optional) network security services and local security policies dictate the use of one or more of these services:

- Data confidentiality—The IPSec sender can encrypt packets before sending them across a network.

- Data integrity—The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.
- Data origin authentication—The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.
- Anti-replay—The IPSec receiver can detect and reject replayed packets.

With IPSec, data can be sent across a public network without observation, modification or spoofing.

IPSec functionality is essentially identical in both IPv6 and IPv4; however, IPSec in IPv6 can be deployed from end-to-end - data may be encrypted along the entire path between a source node and destination node. (Typically, IPSec in IPv4 is deployed between border routers of separate networks.)

In IPv6, IPSec is implemented using the authentication extension header and the ESP extension header. The authentication header provides integrity and authentication of the source. It also provides optional protection against replayed packets. The authentication header protects the integrity of most of the IP header fields and authenticates the source through a signature-based algorithm. The ESP header provides confidentiality, authentication of the source, connectionless integrity of the inner packet, anti-replay and limited traffic flow confidentiality.

2.3 Quality of Service

Network transmission plays an important role in supporting real-time applications, which are generally QoS-based. Thus it is important for network protocols to have some form of QoS support. IPV4 had the Differentiated Service Code Point (DSCP) field which formed part of the

Type of Service field that was used to develop the Diffserve architecture [Bouras et al, 2004]. Although this field did provide for traffics of different types, it had only four possible classes of traffic and thus was limited in the classification of traffics. In IPV6 the DSCP field still exits, but it forms part of the Traffic Class field. However, IPV6 also contains a Flow Label field. The use of the field was standardized in 2004 [Rajahalme et al, 2004]. This field allows individual flows from a source to be labelled.

The presence of the flow label field has interesting potentials to support QoS. Routers and other intermediate nodes can be informed of the kind of treatment to be given for each flow. Information about processing parameters, such as maximum delay can be sent to the intermediate nodes. In his master's thesis, B. Prakash [Prakash, 2004] even proposes the subdividing of the flow-label field in such a way that the different sets of bits can represent different processing parameters.

2.4 Mobility

Mobility allows a node to change its location on a network and still maintain all its existing connections. Mobility support existed in IPV4. Mobile IPV6 has built up on the already existing support but includes a number of improved features.

In IPV4, mobility support is dependent on the transport protocol, since it uses UDP for signalling. Mobile IPv6 uses IPv6 extension headers. This allows for a cleaner implementation, since the code can fully integrated with the IP-processing where it belongs, and no transport protocol port numbers need to be bound for special use [Eddy et al, 2006]. Additionally, Mobile IPv4 uses triangle routing and bi-directional tunnelling, whereas Mobile IPv6 supports a more efficient optional route optimization technique.

Furthermore, although Mobile routers (and correspondingly, the mobile networks behind them) are supported in Mobile IPv4, their operation is not particularly well specified. In contrast, Mobile IPv6 mobile routers, called NEMO routers, have been specified very clearly in their own standards documents [RFC3963].

Thus, IPV6 has superior mobility features than IPV4 since, in IPV6, mobility is based on cleaner design, support for route optimization, and NEMO extensions.

2.5 Higher Packet Processing Efficiency

IPV6 has improved efficiency for packet processing. IPV4 packets included checksums that were processed at each node. Although efficient means of computing IPV4 checksums were developed, the checksum has been removed from in IPV6 since the most data-link layer protocols have their own checksums and transport protocols also have their own checksums (Eddy, 2006). The checksums in the lower and higher layers were actually more powerful than the IPV4 checksums.

Fragmentation of datagrams, when required, can be a performance bottleneck in IPV4 routers. It loads the routers and limits the throughput. This facility, however, is only exploitable by users, at any point in the network, sending packets larger than a particular link's MTU. In IPV6, routers do not fragment packets. Packets larger than an outgoing link's MTU are dropped. Source nodes have responsibility of packet fragmentation.

The IPV6 header is also simpler to process (Davies, 2008). The number of fields has dropped from 12 in IPV4 to 6 in IPV6, while the number of fields that must be processed by an intermediate router has dropped from 6 to 4. Seldom-used fields supporting fragmentations and options have moved to the extension header.

Another improvement in IPV6 is that it uses neighbour discovery (ND) instead of the older address resolution protocol (ARP) to resolve a subnet into link layer protocol addresses. The IPV6 ND provides extensibility that has been used for various purposes including security, automatic prefix and interface identifier configuration and advertisement of the MTU, features not available in IPV4.

3.0 Challenges for IPV6 deployment

In his paper IP Next Generation overview (Hinden, 1996), R Hinden argued that IPng or IPv6 would be a necessity with the proliferation of nomadic personal computing devices. He argued that the nature of nomadic computing requires an Internet protocol with built in authentication and confidentiality, thus being a major catalyst for IPv6. He also proposed that the different TV channels and Video on Demand would be another major driving force for IPv6. Another idea put forward by him is device control, where different everyday life devices will be controlled via the Internet. He also predicted that there would need to be a major shift towards the new IP in the 1999's to 2003's. However, as per information available at the arstechnica website [Iljitsch, 2008], the adoption of IPv6 as at 2007 appeared to be only 0.0026 percent out of 90 ISPs and other organizations, although the author argued that a lot of IPv6 traffic has been missed due to equipment used in the study. The same report reveals that only 0.12 % of IPV6 native traffic flowed in the Amsterdam Internet Exchange. These numbers seem very small. However, the IPV4 address space is expected to be exhausted in 2012 (CXOtoday, 2009; Eustace, 2009) and the need for IPv6 will become imminent. In the following sections, we discuss some of the reasons why IPv6 has had such a slow start and adoption given the initial predictions and also the challenges involved for the deployment of IPv6. Then the costs involved for deploying IPv6 and solutions are also discussed.

IPv4 will be used for years even after IPv6 has been deployed. IPv6 and IPv4 are two different protocols, where resources available over IPv6 are not reachable from an IPv4 node and vice versa. But, the layers in the Internet Architecture are independent of each other, thus enabling both IPv4 and IPv6 transmission to run in parallel, on the same network. Therefore, the transition mechanism requires that IPv4 and IPv6 hosts are able to interoperate. The IPv6 deployment between hosts and routers need to done incrementally, with few interdependencies and low start-up cost. Finally, it should be easy for system users, network operators and administrators to address [Bradner & Mankin, 1995]. Moreover, the IPv6 has been present for many years, but there has been a poor growth in its deployment across the Internet [Eustace, 2009]. The objective of IPv6 was to have most computers and networks working on a dual-stack by this time, until IPv6 gradually takes over. Dual-stack enables both IPv4 and IPv6 to coexist, where servers and clients will speak both protocols and application or service can use either protocol to communicate.

During the transition, the organisation should expect that most systems software will need to be upgraded. Hardware which have only IPv4 implementations should be considered for replacement and before buying any new hardware, the organization should ensure that the new hardware provides for IPv6 support. There are different strategies to transition to IPv6. The easiest migration process can be through an upgrade of the whole network, Operating Systems and Application. This will provide all the good features of IPv6, but it is expensive. The next choice is to have an incremental deployment, which in addition to the good features of IPv6, it allows lower cost and risk management. Finally, one can wait for the last minute to deploy, and not benefit from the IPv6 features. The consequence will be loss of market shares and lagging behind the market trend.

IPv6 deployment encounters many challenges. One of the biggest hurdle to move to IPv6 is the business need [Botterman, 2009]. The issue is that if customers do not require IPv6, there is no ability for providers to charge for IPv6. Consequently, there is no extra money for investing in new hardware and software. For an organization to build a short term IPv6 business case does not make sense. Nevertheless, not having any customer demand is not a fundamental problem, since deployment of IPv6 will happen anyway. The customer needs are more towards contents and services, such as Google, Skype and many more, and they are not interested in the protocol being used and IPv6 do not provide such new services. Developing countries which are now deploying IPv6 will have an advantage since new IPv6 capable hardware will be used instead of investing in any hardware upgrade.

Routers, servers and client products which support dual IP layer (v4 and v6) and programming application interfaces have been in the market since quite some time [Bound, 2001]. These equipments can be used for infrastructure deployment and to interoperate with IPv4 networks. Once again, the issue is cost, as vendors are charging extra for IPv6. But, the deployment of cable-tv modems, residential gateways, DSL equipment, home network cable and routers and many more still need to support encapsulation of IPv6 within IPv4 or to be replaced and eventually move to native IPV6 [Bound, 2007].

The next IPv6 deployment gap is that considerations for porting software applications and services are not expanding fast enough. The alternative is to centralize the applications and use IPv6 tunnelling to connect with IPv6 hosts and routers over existing IPv4 Internet. The applications do not provide IPv6 support in software Infrastructure, for example, the 3G IP Multimedia Subsystems (IMS) are limited in deploying IPv6 on Fixed Mobile Convergence between Wireless and Broadband. Enterprise Resource Applications (e.g SAP, Oracle, DB2, Finite Element Analysis) and Media Entertainment Applications, such as Gaming, Virtual Life, Content

Distribution, Peer-to-peer File Sharing are also taking a long time to be ported on IPv6 [Bound, 2007]. Another important requirement while deploying IPv6 is the Security Infrastructure and many organizations are already using IPv4 security software infrastructure for Intrusion Detection, Network Edge Packet Filters and Custom Firewalls. These security software still requires to be adapted to IPv6. Even full featured Network Management platforms that are used to manage IPV4 network elements and processes need to be upgraded to support IPv6.

The core network can already handle IPv6. But, according to IDG News Service [Kirk, 2009], only 17 percent of 610 Europeans, Middle East and Central Asia organizations has transitioned to IPv6. This is due to the breach in the IPv6 transition process, in the form of missing operational IPv6 knowledge and experience, 'debugging' of hardware and software, testing verification, budgets for training and IPv6 transition planning.

The internet is facing a transition situation where IPv6 is coexisting with the traditional IPv4 and the bridging between the two technology will be needed for a long time. The challenge, here, lies in IPv6-only or IPv4-only systems or networks. Even though IPv6 is already operable in the core network, IPv4-only customers will require various gateways, in order to allow the translation between IPv6 hosts and IPv4-only servers, for example, Windows 7 Direct Access. The IETF is currently working in finding translation solutions for enabling a unilateral IPv6 deployment [Baker, 2009].

Many organizations are also not interested in transitioning to IPv6 because their customers and employees cannot use IPv6. The compelling immediate action within the IPv6 deployment process is to have IPv6 supported 'small gateways' for private homes. Thus, allowing larger IPv6 deployment possibilities.

According to the IPv6 Deployment Survey commissioned by the European Commission, cost is one of the major barrier to deploy IPv6 [Botterman, 2009]. Normally, when deploying a network Infrastructure, network, security, Human Resource Training, Contents Management and Administrative cost are considered. But, in general when considering deploying an IPv6 Infrastructure mainly the 'cost' of Training, Network Upgrade and Dual Stack operation is being foreseen.

Training cost, is probably the highest among the costs. Even though, IPv6 is not 'so different' compared with IPv4, the hurdle is that staffs do not have enough knowledge and experience with IPv6. Thus, training in IPv6 is perceived to be expensive. However, many organizations have recurrent training for many other new technologies and protocols and, if well-planned, the cost for providing IPv6 training should not be considered as high.

IPv6 deployment happens as part of the normal upgrade cycle, and it is impossible to separate the costs of IPv6 from upgrade costs. Typically new network equipments or upgrades are planned ahead the time for reasons like more bandwidth capacity, intrinsic network growth, procurement of new services and applications for customers, etc. Therefore both hardware and Operation and Maintenance tools become IPv6 enabled in a natural update process. The problem arises for home users, as the upgrade cycle is slower, since sometimes hardware is never changed and thus translation technologies become a necessity.

As discussed above, the IPv4 and IPv6 is currently facing a coexistence period and this is likely to remain for quite some time. Obviously, deploying IPv6 using a Dual stack Infrastructure is considered to be costly. This is because it involves managing two networks, as both protocols (IPv4 and IPv6) have to be maintained. The perception that the operational cost is higher on a Dual Stack Infrastructure can be argued, since there are

Management tools that facilitate the integration process. Moreover, in the long term, IPv6 traffic will become dominant and more IPv6 only networks will be operating, thus decreasing operational costs, as Network Address Translation (NAT) gateways will not be necessary.

The cost of IPv6 deployment depend on many factors. In order to minimize costs while moving to IPv6, organizations have to carefully choose when to start IPv6 deployment [6DISS, 2007]. The size of the network, current hardware and software being used and how soon the network should be IPv6 ready are other components that need considerations while deploying IPv6. But, the key for transitioning for a new protocol, technology and services or IPv6 is planning ahead and that helps to minimize costs.

Organizations often do not consider the cost for not deploying IPv6 and those cost are hidden and difficult to realise. Many studies already demonstrated that operating a network with NAT means extra complexity and cost [Christman, 2005; The TCP Guide, 2005; Huston, 2009; IEEE-USA, 2009]. VoIP, triple play, end-to-end security, peer-to-peer, on-line gaming, and many other new applications cost even higher to be deployed on IPv4, since they do not operate easily through NAT and require coorperation of NAT vendors [IEEE-USA, 2009]. It is also more expensive for developing applications to traverse NAT and work across different network scenarios [Huston, 2009]. Moreover, most security precautions were ignored in IPv4 and NAT complicates deployment for secure applications [Christman, 2005].

Many transition technologies are now available, even though native IPv6 support is not feasible for now. Tunnel brokers, 6to4 and Teredo, are examples of smaller and inexpensive approaches for IPv6 deployment. The transition is not only occurring in ISPs and enterprise networks, but also more operating systems are available with IPv6 enabled by default and more applications are using IPv6 automatically even though it is not available in the ISP or enterprise network. Thus, not deploying IPv6 now can be costly, since with time customers are having a global adoption, when upgrading to new operating systems, by using new services and applications.

Last, but not least, customers might not know much about IPv6, but soon they will end up knowing the value of IPv6, since some applications and services will 'run-only' or 'run-better' with ISPs offering IPv6 services. Therefore the way forward, is to deploy IPv6 on our networks in order to mitigate the effects of the imminent depletion of the IPv4 address space and as usual to keep up with the competition and innovation cycle.

4.0 Migration Technologies

Broadly speaking, there are three transition mechanisms that have been designed to make the migration from IPv4 to IPv6. This section looks briefly at each of these.

4.1 Dual-Stack Approach

This is usually considered to be the simplest way of adding IPv6 capability to an existing IPv4 network. In this method, both hosts and networking devices such as routers are equipped with the IPv4 and IPv6 protocol stacks. IPv4 applications thus use the IPv4 stack while IPv6 applications use the IPv6 stack [Bound, 2002]. Thus, both hosts and routers can easily handle both IPv4 and IPv6 packets by reading the version number in the header field of the datagram. This is the most deployed strategy for moving from IPv4 to IPv6. However, where a host with dual-stack capability has to communicate with a host running only IPv4, this method fails as it cannot use its IPv6 capability. Another drawback to dual-stack protocols is that the routers require dual administration of the two routing protocols and must be provisioned with enough storage space to keep both routing tables.

4.2 Tunneling Mechanisms

Tunneling is an approach whereby two hosts running a similar protocol has to communicate over a network which do not support this protocol. This strategy can be adapted to allow IPv6 hosts to communicate over an IPv4 network. This is done by encapsulating the IPv6 packets inside IPv4 packets. The packets are then transmitted to its endpoint which will de-encapsulate the packet by stripping off the IPv4 header to get the IPv6 packet. The resulting packet will then be forwarded to its final destination. For this method to work, it is important that both the hosts and network devices support both protocol stacks (dual-stacks). Tunnels can be configured manually on both endpoints, in a semi-automatic way (the sender only) or fully automatic. ISATAP and Teredo are two popular automatic tunneling mechanisms. For a complete discussion of tunneling methods, the reader is referred to [6Net, 2005].

4.3 Translation Mechanisms

Translation comes into play when an IPv6-only host has to communicate with a remote IPv4 node. The most common translation mechanism is address translation. To map IPv6 onto IPv4, the translator reads the least significant thirty-two bits of an IPv6 address to obtain the IPv4 address. To map IPv4 onto IPv6, the translator sets the least significant thirty-two bits of the IPv6 address to the IPv4 address. However, translation can occur at different layers in the protocol stack, not only in the network layer [Doyle, 2003]. Examples of translation mechanisms are the stateless IP/ICMP Translation algorithm (SIIT), Network Address Translation Protocol Translation (NAT-PT), Bump-In-The-Stack (BIS), Bump-In-The-API (BIA), SOCKS-based IPv6/IPv4 Gateway and SOCKS64 [Tantayakul et al, 2008].

5.0 Deployment Strategies World-wide

According to the survey results published by Google at the RIPE meeting in Dubai (Google, 2008), the top five countries that generate significant IPv6 traffic are: Russia (0.76%), France (0.65%), Ukraine (0.64), Norway (0.49) and the United States (0.45%). Although China showed 0.24%, it surpasses US in terms of the number of users. Japan with 0.15% is also very highly ranked.

The European Union and Japan are leading the transition to IPv6. This is inevitable since they rely on the Internet as much as the Americans, yet they own significantly fewer IPv4 addresses [Childress et al, 2003].

The United States owns 70% of the available IPv4 addresses, so it is no surprise that the United States is not pushing for a quick transition to the new technology [Childress et al, 2003]. However, the US government has issued a mandate, since 2007, to make the switch to IPv6 as early as possible [Das, 2008b].

IPv6 Canada is a sub-chapter of the North American IPv6 Task Force. Their mission is to stimulate, promote and support the successful integration of IPv6 into Canadian economy accelerating the global transition to IPv6 [IPv6Canada, 2006]. The firm Viagenie in Canada has developed a tunnel server (freenet6.net) to allow any IPv4 node to be connected to the 6Bone [Das, 2008b]. International connectivity of IPv6 has been achieved through native IPv6 and tunnelling.

China is the leading country in terms of Internet traffic, both for IPv4 and IPv6. The Chinese government has initiated the China's Next Generation Internet Project (CNPI) which is a five-year plan to propulse China as the world leader in IPv6 integration. As in 2006, 20 major cities of China were already connected through IPV6 [Worthen, 2006]. It is a pure IPv6 backbone. China has officially displayed its expertise in the IPv6 world during the 2008 Olympics in Beijing where everything from security cameras to vehicles were connected to an IPv6 network. The Olympics events were also streamed on the Internet using IPv6 hosts and networks devices only [Das, 2008a].

The IPv6 Task Force was created in France in 2002. The active involvement of France Telecom, the leading telecom operator in the country, has placed France amongst the leaders in the new technology [European IPv6TF, 2004a]. France is ranked second in the world in IPv6 traffic [Google, 2008].

However, this position is criticised on the fact that 95% of this traffic comes from only one website (free.fr).

IPv6 deployment in Japan enjoys strong government support [Das, 2008b]. In terms of number of applications deployed using the IPv6 protocol, Japan is by far the world leader. Most current home appliances being produced in Japan support IPv6. These include but are not limited to home routers, network cameras, digital TVs, IP-phone, electricity meters, etc. Japan has implemented a nationwide earthquake warning system using IPv6. Residents have a special equipment (e.g. a phone) at home on which the status of any warning is displayed [MW, 2008].

In Malaysia, the National Advanced IPv6 Centre (NAv6) was established by the Ministry of Energy, Water and Communication (MEWC) in March 2005. It serves as the National Centre for IPv6 research, human resource development and monitoring of IPv6 development for Malaysia [Nav6, 2008]. MYREN which is a national research education network in Malaysia has an IPv6 dual-stack deployed linking 12 Universities and Research Centres [Nav6, 2008].

The Government of India considers IPv6 deployment to be one of the top priorities for the country [IPv6 Forum India, 2009]. An Indian IPv6 Task Force was established in 2004 soon after the 1st South Asian IPv6 Summit. The contribution Sify Technologies Limited has been very significant in the deployment of IPv6 in India. An Indian IPv6 summit was held on the 15-16 December 2009 to further promote the deployment of IPv6 amongst ISPs, governmental departments and users.

In Spain, the Ministry of Science and Technology is supporting its IPv6 Task Force fully in the deployment of IPv6 across the country. Telefonica, a major telecommunication provider in Spain, had launched the first IPv6 service during the IPv6 Global Launch Event in Madrid, 2004, paving the way for Spain to be among European leaders in IPv6 technology [Jordi, 2004].

The mission of the German IPv6 Task Force is to promote the timely deployment and adoption of IPv6 in Germany. The ministry of defense wishes to deploy IPv6 in the armed forces. 25% of ISPs have native IP connectivity. The 6WIN backbone network offers full native support for their participants [Wikipedia, 2009].

United Kingdom is the second country in Europe in terms of IPv6 address allocation. UK has the largest number of active LIRs in Europe [European IPv6TF, 2004b]. Many universities have set up IPv6 academic networks. JANET, UK's education and research network, has supported IPv6 trials since 1998. JANET has interconnections with GÉANT and the pan-European backbone network interconnecting the European NRENs (National Research and Education Networks). JANET was also a partner in the 6Net project [JANET, 2009]. However, UK is not a leader in IPv6 deployment in Europe.

The government of Korea plans to achieve complete IPv6 transition in the public sector and 10 millions IPv6 users by the end of 2010. It also plans to achieve total IPv6 transition in backbone networks by 2010 and ISP access networks by 2013 [Das, 2008b]. Thus, Korea has clearly seen the need to invest into the deployment of IPv6 for both the public and private sectors.

The IPv6 Steering Committee and IPv6 Forum in Taiwan were founded in 2002. Since then, IPv6 has been deployed aggressively by the government in key areas like education, e-government, transportation, etc [IPv6 Forum Taiwan]. The academic IPv6 network, Sinica, is connected to 8 other local IPv6 networks and has links to 19 international IPv6 networks. Taiwan is leaving no stone unturned in moving into the future of the Internet.

Netherlands is one of the leaders in Europe in IPv6 deployment. SixXs (sixxt.net) is a dutch organisation whose mission is to help IPv6 users from all over the world. It also provides various services and software which has contributed significantly to IPv6 adoption globally [Wikipedia, 2009]. XS4All, Signet and Business ISP Introweb are Dutch ISPs which provides IPv6 connectivity to all broadband users. Netherlands has significant expertise in deploying IPv6 [Wikipedia, 2009].

Some network operators, hardware and device manufacturers, and others are in the process of taking up IPv6, through deploying it in their networks or building it into their products. However, many players are sitting on the sidelines, adopting a wait and see approach [Internet Society, 2009].

The political and social issues are being addressed by the European IPv6 Task Force (IPv6TF), by National IPv6 Task Forces and by the IPv6 Forum. While deployment is underway, it is not progressing fast enough [Internet Society, 2009]. IPv6 is necessary for the continuity, stability and evolution of the Internet.

6.0 Deployment strategies for Africa

One of the main reasons why IPV6 deployment has been and is being held back is the use of extensive NAT. Another reason as mentioned above is that existing ISPs and companies may not be willing to move towards IPv6 since they already have the infrastructure for IPv4 and their equipments may not be compatible with IPv6 or they may simply not have the need to move to IPv6. However, the situation for many African countries may be different. Most African countries are new to the IT sector and may not have yet invested massively in hardware. This leaves a unique opportunity for African countries. They can do it right from the first time itself, i.e. invest in an IPv6 Infrastructure right from the start. However, a number of problems might arise for the African IPv6 adoption:

- A lot of industrialized countries might want to dump their older technology to African countries. Technology evolves a lot nowadays and new technology is mostly adopted in industrialized countries. As a result, these countries might have a surplus of obsolete technology that they might want to 'dump' onto African countries. So one of the major challenges for these countries will be to resist going for cheap, IPv6 incompatible hardware.
- A lot of technology transfer and training will have to take place for the African countries. African countries may not have the number of qualified personnel to adopt IT related technology, even IPv6.
- African countries have a lot of issues to resolve like civil wars and famine

AfriNIC is the Regional Internet Registry (RIR) for the African continent [AfriNIC, 2001]. AfriNIC has been assigned the IPV6 blocks of 2c00::/12 and 2001:4200::/2 [Wiki, 2001] . AfriNIC strives to make the adoption of IPv6 easy for African countries and undertakes a number of measures in this endeavor.

In its attempt to encourage the adoption of IPv6, in 2004 and 2005, AfriNIC waived the initial fee and the first year's annual fees for any qualified organization adopting IPv6 [Akplogan, 2004]. In 2007 and 2008, the new billing policy stipulated that there will be no additional costs for any established Local Internet Registries (LIRs) with existing IPv4 allocations. New LIRs would be allowed a 50% discount on the initial setup fee and 100% discount on the first year's membership fee for a LIR with IPv6 only allocation. These LIRs would be allowed 75%, 50%, 25% discount on the respective membership fee for the three subsequent years [Akplogan, 2007].

One of the problems suffered by IPv6 deployment is the few number of IPv6 applications available on the market. In this respect, AfriNIC provides on a temporary basis a free IPv6 address range to organizations who want to test their applications over IPv6 [Aina, 2005]. Any organization that wishes to test or experiment with IPv6 can request for a range of IPv6 addresses for a period of one month and the lease can be extended if needed.

AfriNIC also provides access to its virtual IPv6 lab [AfriNIC, 2002]. The virtual lab can be used for testing and educational purposes. This testbed is managed by AfriNIC and is setup with the support of the 6Deploy consortium and mainly Cisco System to increase hands-on experience with IPv6. The testbed consists of the CISCO 2811 and Cisco 12404 routers.

AfriNIC provides a yearly LIR Training Program to help the Africa Internet Community [AfriNIC, 2003]. One of the key topics in the training is IPv6 Basics, where the trainees are exposed to the different issues in IPv6 like transition mechanisms (including tunnelling), activating IPv6 on PCs and Installing IPv6 on different platforms (XP/W2003, Linux, BSD), Basic stateless/stateful configuration, (including privacy setup), Transition mechanisms (Including Tunneling) and Basic configuration of routers.

7.0 Opportunities and challenges for Mauritius

As other countries in the world are planning their IPV6 deployment, Mauritius will need to do the same so as to overcome the exhaustion of IPV4 addresses and also to benefit of the many advantages of IPV6. The deployment of IPV6 will improve the internet support for organizations as well as individuals in terms of the number of devices that can directly access internet services, the security of transactions, the improved quality of applications and the wider range of applications possible due to the integrated support for mobility. The deployment of IPV6 will improve organizations' abilities to offer services with real-time requirements such as live broadcasts on all kinds of personal computing devices, improved video surveillances and remote processing of complex applications.

The Mauritius software industry can also obtain direct economic opportunities from the worldwide deployment of IPV6. The software industry can participate in converting the massive amount of IPV4 applications that will need to be ported to IPV6 network. In addition to simply porting the applications, they can be further improved to benefit from the additional security and QoS support of IPV6. Additionally IPV6 presents important opportunities in terms of new kinds of secure and QoS-based applications for portable devices. The Mauritian software industry can seize the opportunity to obtain its market share from these classes of applications.

To deploy IPV6, ISPs will have to provide the required support in the network backbones of the country. Each organization of the country will then need to come up with its own strategy of transition.

8.0 Conclusion

In this paper, we presented the different problems associated with the IPV4. These problems include exhaustion of address space. We then proposed how IPV6 addressed many of the issues of IPV4 and also improves on the older protocol. We discussed about opportunities provided by IPV6 like enhanced security and Flow Label to implement QoS for different types of traffic. We then discussed on the hurdles encountered in IPV6 deployment, among which are technological, financial and human capacity issues. We also discuss why IPV6 has not spread according to the initial predictions, when it was being proposed. We also analyse the IPV6 deployment status around the world, noting that IPV6 accounts for limited Internet traffic. We also propose that IPV6 provides a unique opportunity for African countries, since most of these countries are not tied up with legacy hardware and technology and can invest in IPV6 ready equipment from the beginning.

Mauritius IT industry is booming nowadays and IPV6 deployment can contribute to a large extent to the industry. New applications, involving mobility or that can make us of specific features of IPV6 can be developed.

9.0 References

- 6DISS (IPv6 Dissemination and Exploitation) (2007). IPv6 Deployment and Associated Risks (for Strategists). Retrieved on 15th December 2009 from http://www.6diss.org/

- AfriNIC (2001): http://www.afrinic.net/about.htm (last accessed 13 Dec 2009)

- AfriNIC (2002): http://www.afrinic.net/projects/cvl.htm (last accessed 14 Dec 2009)

- AfriNIC (2003): http://www.afrinic.net/training/index.htm (last accessed 14 Dec 2009)

- AINA, A. (2005). Retrieved on 14th December from http://www.afrinic.net/docs/policies/AFPUB-2006-GEN-002.htm

- AKPLOGAN, A. (2004). Retrieved on 14th December 2009 from http://www.afrinic.net/docs/billing/afadm-fee200405.htm

- AKPLOGAN, A. (2007). Retrieved on 14th December 2009 from http://www.afrinic.net/docs/billing/afcorp-fee200703.htm

- BAKER, F. (2009). IPv4/IPv6 Coexistence and Transition. IEFT Journal 4 (3).

- BOUND J (2002), Dual Stack Transition Mechanism. Retrieved on 10th December 2009 from http://go6.net/ipv6-6bone/ngtrans/IETF-54-Yokohama/dstm.pdf

- BOUND, J. (2001). Internet Society: IPv6 Deployment.

- BOUND, J. (2007). The New New Internet: IPv6 Conference, Hyatt Regency Crystal City, May 10, 2007, "IPv6 Deployment Gaps to be Completed”.

- BOURAS CH., GKAMAS A., PRIMPAS D. AND STAMOS K., “Porting and performance aspects from IPv4 to IPv6: The case of OpenH323”, International Journal of Communication Systems, 2005, pp 847-866.

- BOURAS CH., GKAMAS A., PRIMPAS D. AND STAMOS K.,”Quality of Service Aspects in an IPv6 Domain”, ICON 2004, 12th IEEE conference on Network, 2004.

- BRADNER, S. AND MANKIN, A (1995). The Recommendation for the IP Next Generation Protocol, RFC 1752. Botterman, M. (2009). IPv6 Deployment Survey: Based on responses from the RIPE community during June 2009.

- CHILDRESS, B., CATHEY, B., AND DIXON, S. 2003. The Adoption of IPv6. *J. Comput. Small Coll.* 18, 4 (Apr. 2003), 153-158.

- CHRISTMAN, C. (2005). The move on to IPv6: If you've not done so already, it's time to get ready for the next generation of IP. Retrieved on 15th Decmber 2009 from http://features.techworld.com/networking/1109/the-move-on-to-ipv6/

- CXOTODAY (2009). India Readying for IPv6. Retrieved on 14th December 2009 from http://www.cxotoday.com/India/News/India_Readying_for_IPv6/551-108056-912.html

- DAS K (2008a) IPv6 and the 2008 Beijing Olympics. Retrieved on 14 December 2009 from http://ipv6.com/articles/general/IPv6-Olympics-2008.htm

- DAS K (2008b) IPv6 Deployment Around the World. Retrieved on 14th December 2009 from http://ipv6.com/articles/deployment/IPv6-Deployment-Status.htm

- DAVIES J. (2008) "Understanding IPV6", Second Edition- ISBN-10: 0-7356-2446-1, Microsoft Press.

- DOYLE J (2003) Transitioning to IPV6: Mechanisms and Issues. Retrieved on 10th December 2009 from http://www.6journal.org/archive/00000025/01/Jeff_Doyle.pdf

- DUNMORE M., "6NET- An IPV6 Deployment Guide", The 6NET consortium, September 2005.

- EDDY W., ISHAC J., "Comparison of IPV6 and IPV4 features", Internet draft, May 2006.

- European IPv6 Task Force (2004) IPv6 Task Force Steering Committee. Retrieved on 12th December 2009 from http://www.ipv6.eu/admin/bildbank/uploads/Documents/Deliverables/ipv6tf-sc_pu_d2_1_1_v1_25.pdf

- European IPv6 Task Force (2004) IPv6 task Force Steering Committee. Retrieved on 12th December 2009 from http://www.ipv6.eu/admin/bildbank/uploads/Documents/Deliverables/ipv6tf-sc_pu_d4_3_1_v3.pdf

- EUSTACE, G. (2009). Infrastructure Support Section, Information Technology Services, Massey University.

- Google (2008) Global IPv6 Statistics. Retrieved on 15 December 2009 from http://www.ripe.net/ripe/meetings/ripe-

57/presentations/Colitti-Global_IPv6_statistics_Measuring_the_current_state_of_IPv6_for_ordinary_users_.7gzD.pdf

- HAGEN S., "The IPV6 case: Questions and Answers", Sunny Paper, Sunny Connection AG., 2004, available at www.sunny.ch.

- HINDEN, R. M. (1996). IP Next Generation Overview, Communications of the ACM. ACM NewYork, USA pp 61-71.

- HUSTON, G. (2009). The ISP Column: Is the Transition to IPv6 a "Market Failure?".

- IEEE-USA White Paper (2009). Next Generation Internet: IPv4 Address Exhaustion, Mitigation Strategies and Implications for the U.S.

- ILITSCH, V. B (2008). Researchers: IPv6 traffic a mere 0.0026 percent of total. Retrieved on 14th December 2009 from http://arstechnica.com/old/content/2008/08/researchers-ipv6-traffic-a-mere-0-0026-percent-of-total.ars

- Internet Society (2009) Frequently Asked Questions on IPv6 adoption and IPv4 exhaustion.Retrieved on 10th December 2009 from http://www.isoc.org/educpillar/resources/ipv6.shtml

- IPv6 Canada (2006). Retrieved on 14 December 2009 from http://ipv6canada.ca/index.html

- IPv6 Forum India (2009) IPv6 Forum. Retrieved on 16th December 2009 from http://www.ipv6forum.in/

- IPv6 Forum Taiwan (2009) Developing IPv6 Technology. Retrieved on 16th December 2009 from http://www.ipv6.org.tw/newe.html

- JANET (2009) UK's Education and Research Network. Retrieved on 15th December 2009 from http://www.ja.net/services/connections/janet-sites/mans

- JORDI (2004) Telefonica to link Europe and Latin America with IPv6 Technology. Retrieved on 15th December 2009 from http://www.ipv6tf.org/index.php?page=news/newsroom&id=317

- KIRK, J. (2009). IDG News Service: Europe Moving Slow on IPv6 Deployment. Retrieved on 15th December 2009 from http://www.pcworld.com/businesscenter/article/174655/europe_moving_slow_on_ipv6_deployment.html

- MELFORD B. (1997) – "TCP/IP Limitations undone", Sunworld, January 1997.

- MW (2008) Phones Ring Earthquake Warnings. Retrieved on 13th December 2009 from http://www.letsjapan.markmode.com/index.php/2008/12/04/phones-ring-earthquake-warnings/

- National Advanced IPv6 Centre (2008) IPv6 Status in Malaysia. Retrieved on 12th December 2009 from http://www.nav6.org/content_resource.php

- PRAKASH B., "Using The 20 Bit Flow Label Field In The IPV6 Header To Indicate Desirable Quality Of Service On The Internet", Master of Science Thesis, University of Colorado,2004.

- RAJAHALME J., CONTA A., CARPENTER B. AND DEERING S., RFC 3697, "IPv6 Flow Label Specification", March 2004.

- TANTAYAKUL, K., KAMOLPHIWONG, S., AND ANGCHUAN, T. 2008. IPv6@HOME. In *Proceedings of the international*

Conference on Mobile Technology, Applications, and Systems (Yilan, Taiwan, September 10 - 12, 2008)

- The 6Net Consortium (2005) An IPv6 Deployment Guide. Retrieved on 11th December 2009 from http://www.6net.org/book/deployment-guide.pdf

- The TCP Guide (2009). IP Network Address Translation (NAT) Protocol. Retrieve on 15th Decmber 2009 from http://www.tcpipguide.co/free/t_IPNATOverviewMotivationAdvantagesandDisadvantages.htm

- Wiki (2001): http://en.wikipedia.org/wiki/AfriNIC (last accessed 14th Dec 2009)

- Wikipedia (2009) IPv6 Deployment. Retrieved on 16th December 2009 from http://en.wikipedia.org/wiki/IPv6_deployment

- WORTHEN B (2006) Internet Strategy: China's Next Generation Internet. Retrieved on 16th December 2009 from http://www.cio.com/article/22985/Internet_Strategy_China_s_Next_Generation_Internet